CHAPTER 8

Working with Alerts

March 23, 2010

About Alerts

The system generates alert messages to notify administrator when a predefined condition is met, such as when an activated service goes from up to down. Alerts can be sent out as email/epage.

RTMT, which supports alert defining, setting, and viewing, contains preconfigured and user-defined alerts. Although you can perform configuration tasks for both types, you cannot delete preconfigured alerts (whereas you can add and delete user-defined alerts).

The Alert menu comprises the following menu options:

- Alert Central—This option comprises the history and current status of every alert in the system.

Note You can also access Alert Central by clicking the Alert Central icon in the hierarchy tree in the system drawer.

- Set Alert/Properties—This menu option allows you to set alerts and alert properties.
- Remove Alert—This menu category allows you to remove an alert.
- Enable Alert—With this menu category, you can enable alerts.
- Disable Alert—You can disable an alert with this category.
- Suspend cluster/node Alerts—This menu category allows you to temporarily suspend alerts on a particular Cisco Unified Presence node or on the entire cluster.

- Clear Alerts—This menu category allows you to reset an alert (change the color of an alert item from to black) to signal that an alert has been taken care of. After an alert has been raised, its color will automatically change to in RTMT and will stay that way until you manually clear the alert.
- Clear All Alerts—This menu category allows you to clear all alerts.
- Alert Detail—This menu category provides detailed information on alert events.
- Config Email Server—In this category, you can configure your email server to enable alerts.
- Config Alert Action—This category allows you to set actions to take for specific alerts; you can configure the actions to send the alerts to desired email recipients.

In RTMT, you configure alert notification for perfmon counter value thresholds and set alert properties for the alert, such as the threshold, duration, frequency, and so on.

You can locate Alert Central under the Tools hierarchy tree in the quick launch. Alert Central provides both the current status and the history of all the alerts in the system.

- Preconfigured Alerts, page 8-2
- Alert Fields, page 8-3
- Alert Logs, page 8-4

Preconfigured Alerts

You can enable or disable preconfigured and custom alerts in Alert Central; however, you cannot delete preconfigured alerts.

The following list comprises the preconfigured alerts for the system:

- AuthenticationFailed
- CiscoDRFFailure
- CoreDumpFileFound
- CpuPegging
- CriticalServiceDown

Note The CriticalServiceDown alert only generates when the service status equals down (not for other states).

- HardwareFailure
- LogFileSearchStringFound
- LogPartitionHighWaterMarkExceeded
- LogPartitionLowWaterMarkExceeded
- LowActivePartitionAvailableDiskSpace
- LowAvailableVirtualMemory
- LowInactivePartitionAvailableDiskSpace
- LowSwapPartitionAvailableDiskSpace
- ServerDown

Note The ServerDown alert generates when the currently “active” AMC (primary AMC or the backup AMC, when the primary is not available) cannot reach another node in a cluster. This alert identifies network connectivity issues in addition to a server down condition.

- SparePartitionLowWaterMarkExceeded
- SparePartitionHighWaterMarkExceeded
- SyslogSeverityMatchFound
- SyslogStringMatchFound
- SystemVersionMismatched
- TotalProcessesAndThreadExceededThreshold

Alert Fields

You can configure both preconfigured and user-defined alerts in RTMT. You can also disable both preconfigured and user-defined alerts in RTMT. You can add and delete user-defined alerts in the performance-monitoring window; however, you cannot delete preconfigured alerts.

Table 8-1 provides a list of fields that you may use to configure each alert; users can configure preconfigured fields, unless otherwise noted.

Table 8-1 Alert Customization

Field	Description	Comment
Alert Name	High-level name of the monitoring item with which RTMT associates an alert	Descriptive name. For preconfigured alerts, you cannot change this field. For a list of preconfigured alerts, see Preconfigured Alerts, page 8-2.
Description	Description of the alert	You cannot edit this field for preconfigured alerts. For a list of preconfigured alerts, see Preconfigured Alerts, page 8-2.
Performance Counter(s)	Source of the performance counter	You cannot change this field.
Threshold	Condition to raise alert (value is...)	Specify up < - > down, less than #, %, rate greater than #, %, rate.
Value Calculated As	Method used to check the threshold condition	Specify value to be evaluated as absolute, delta (present - previous), or % delta.
Duration	Condition to raise alert (how long value threshold has to persist before raising alert)	Options include the system sending the alert immediately or after a specified time that the alert has persisted.
Alert Action ID	ID of alert action to take (System always logs alerts no matter what the alert action.)	Alert action is defined first If this field is blank, that indicates that email is disabled.
Enable Alerts	Enable or disable alerts.	Options include enabled or disabled.

Table 8-1 Alert Customization (continued)

Field	Description	Comment
Clear Alert	Resets alert (change the color of an alert item from to black) to signal that the alert has been resolved	After an alert has been raised, its color will automatically change to and stay that way until you manually clear the alert. Use Clear All to clear all alerts.
Alert Generation Rate	How often to generate alert when alert condition persists	Specify every X minutes. (Raise alert once every X minutes if condition persists.) Specify every X minutes up to Y times. (Raise alert Y times every X minutes if condition persists.)
User Provide Text	Administrator to append text on top of predefined alert text	N/A
Severity	For viewing purposes (for example, show only Sev. 1 alerts)	Specify defaults that are provided for predefined (for example, Error, Warning, Information) alerts.

Alert Logs

The alert log stores the alert, which is also stored in memory. The memory is cleared at a constant interval, leaving the last 30 minutes of data in the memory. When the service starts/restarts, the last 30 minutes of the alert data load into the memory by the system reading from the alert logs that exist in all servers in the cluster.The alert data in the memory is sent to the RTMT clients on request.

Upon RTMT startup, RTMT shows all logs that occurred in the last 30 minutes in the Alert Central log history. The alert log periodically updates, and new logs are inserted into the log history window. After the number of logs reaches 100, RTMT removes the oldest 40 logs.

The following file name format for the alert log applies: AlertLog_MM_DD_YYYY_hh_mm.csv.

The alert log includes the following attributes:

- Time Stamp—Time when RTMT logs the data
- Alert Name—Descriptive name of the alert
- Node—Node name for where RTMT raised the alert
- Alert Message—Detailed description about the alert
- Description—Description of the monitored object
- Severity—Severity of the alert
- PollValue—Value of the monitored object where the alert condition occurred
- Action—Alert action taken
- Group ID—Identifies the source of the alert

The first line of each log file comprises the header. Details of each alert get written in a single line, separated by a comma.

Working in Alert Central

You can access Alert Central and perform the following tasks:

- sort alert information
- enable, disable, or remove an alert
- clear an alert
- view alert details

Before You Begin

Review the information about alerts.

Procedure

Step 1 Perform one of the following actions:

a. On the Quick Launch Channel:

- Click **System.**
- In the tree hierarchy, double-click **Tools**.
- Click the Alert Central icon.

b. Select **System > Tools > Alert > Alert Central**.

Step 2 Perform one or more of the following actions:.

If you want to:	Action
Set alert properties	See Setting Alert Properties, page 8-7.
Suspend alerts on Cisco Unified Presence nodes	See Suspending Alerts on Cisco Unified Presence Nodes or the Cluster, page 8-12.
Configure emails for alert notification	See Configuring Emails for Alert Notification, page 8-11.
Configure alert actions	See Configuring Alert Actions, page 8-10.
Sort alert information in the Alert Status pane	**a.** Click the up/down arrow that displays in the column heading. For example, click the up/down arrow that displays in the Enabled or InSafeRange column
Sort alert history information	**a.** Click the up/down arrow in the columns in the Alert History pane. **b.** Use the scroll bar on the right side of the Alert History pane to see alert history that is out of view in the pane.
Enable, disable, or remove an alert	Perform one of the following actions: **a.** From the Alert Status window, right-click the alert and select **Disable/Enable Alert** (option toggles) or **Remove Alert**, depending on what you want to accomplish. **b.** Highlight the alert in the Alert Status window and select **System > Tools > Alert > Disable/Enable** (or **Remove**) **Alert**.
Clear either individual or collective alerts after they get resolved	Perform one of the following actions: **a.** After the Alert Status window displays, right-click the alert and select **Clear Alert** (or **Clear All Alerts**). **b.** Highlight the alert in the Alert Status window and select **System > Tools > Alert > Clear Alert** (or **Clear All Alerts**).
View alert details	**a.** Perform one of the following actions – After the Alert Status window displays, right-click the alert and select **Alert Details**. – Highlight the alert in the Alert Status window and select **System > Tools > Alert > Alert Details**. **b.** After you have finished viewing the alert details, click **OK**.

Troubleshooting Tips

You can only remove user-defined alerts from RTMT. The Remove Alert option appears grayed out when you select a preconfigured alert.

Related Topics

About Alerts, page 8-1

Setting Alert Properties

Using the alert notification feature, the application notifies you of system problems. The following configuration setup is required to activate alert notifications for a system performance counter:

From the RTMT Perfmon Monitoring pane, you can select the system perfmon counter and:

- Set up an email or a message popup window for alert notification.
- Determine the threshold for the alert.
- Determine the frequency of the alert notification (for example, the alert occurs once or every hour)
- Determine the schedule for when the alert activates (for example, on a daily basis or at certain times of the day).

Procedure

Step 1 Perform one of the following actions:

If you want to:	Action
Set alert properties for a performance counter	**a.** Display the performance counter. **b.** From the counter chart or table, right-click the counter for which you want to configure the alert notification, and select **Set Alert/Properties**. **c.** Check **Enable Alert**.
Set alert properties from Alert Central	**a.** Access Alert Central. **b.** Click the alert for which you want to set alert properties. **c.** Perform one of the following actions: • Right-click the alert and select **Set Alert/Properties**. • Select **System > Tools > Alert > Set Alert/Properties**. – Check **Enable Alert**.

Step 2 Select the severity level at which you want to be notified in the Severity list box.

Step 3 Enter a description of the alert in the Description pane.

Step 4 Click **Next**.

Step 5 Configure the settings in the Threshold, Value Calculated As, Duration, Frequency, and Schedule panes.

Table 8-2 Counter Alert Configuration Parameters

Setting	Description
Threshold Pane	
Trigger alert when following conditions met (Over, Under)	Check and enter the value that applies. • Over—Check to configure a maximum threshold that must be met before an alert notification is activated. In the Over value field, enter a value. For example, enter a value that equals the number of calls in progress. • Under—Check to configure a minimum threshold that must be met before an alert notification is activated. In the Under value field, enter a value. For example, enter a value that equals the number of calls in progress. **Tip** Use these check boxes in conjunction with the Frequency and Schedule configuration parameters.
Value Calculated As Pane	
Absolute, Delta, Delta Percentage	Click the radio button that applies. • Absolute—Because some counter values are accumulative, select Absolute to display the data at its current status. • Delta—Select Delta to display the difference between the current counter value and the previous counter value. • Delta Percentage—Select Delta Percentage to display the counter performance changes in percentage.
Duration Pane	
Trigger alert only when value constantly...; Trigger alert immediately	• Trigger alert only when value constantly...—If you want the alert notification only when the value is constantly below or over threshold for a desired number of seconds, click this radio button and enter seconds after which you want the alert to be sent. • Trigger alert immediately—If you want the alert notification to be sent immediately, click this radio button.
Frequency Pane	
Trigger alert on every poll; trigger up to...	Select the radio button that applies. • Trigger alert on every poll—If you want the alert notification to activate on every poll when the threshold is met, click this radio button. • Trigger up to...—If you want the alert notification to activate at certain intervals, click this radio button and enter the number of alerts that you want sent and the number of minutes within which you want them sent.

Setting	Description
Schedule Pane	
24-hours daily; start/stop	Select the radio button that applies: • 24-hours daily—If you want the alert to be triggered 24 hours a day, click this radio button. • Start/Stop—If you want the alert notification activated within a specific time frame, click the radio button and enter a start time and a stop time. If checked, enter the start and stop times of the daily task. For example, you can configure the counter to be checked every day from 9:00 am to 5:00 pm or from 9:00 pm to 9:00 am.

Troubleshooting Tips

For Cisco Unified Presence clusterwide alerts, the Enable/Disable this alert on following server(s) does not display in the Alert Properties window. Clusterwide alerts include number of registered phones, gateways, media devices, route list exhausted, media list exhausted, MGCP D-channel out of service, malicious call trace, and excessive quality reports.

What To Do Next

Configuring Alert Actions, page 8-10

Related Topics

- Viewing Performance Counters, page 7-2
- Working in Alert Central, page 8-5

How To Configure Alert Actions

In RTMT, you can configure alert actions for every alert that is generated and have the alert action sent to email recipients that you specify in the alert action list.

Table 8-3 provides a list of fields that you will use to configure alert actions. Users can configure all fields, unless otherwise marked.

Table 8-3 Alert Action Configuration

Field	Description	Comment
Alert Action ID	ID of alert action to take	Specify descriptive name.
Mail Recipients	List of email addresses. You can selectively enable/disable an individual email in the list.	N/A

- Configuring Alert Actions, page 8-10
- Configuring Emails for Alert Notification, page 8-11

Configuring Alert Actions

Before You Begin

Set alert properties.

Procedure

Step 1 Complete one or more of the following actions in the Alert Properties: Frequency and Schedule window:

If you want to:	Action
Trigger an alert action with this alert	Select the alert action that you want to send from the list box.
Add a new alert action	**a.** Click **Configure.** **b.** Click **Add** in the Alert Action window. **c.** Enter a name for the alert action in the Name field. **d.** Enter a description of the alert action in the Description field.
Edit an existing alert action	**a.** Click **Configure.** **b.** Highlight the alert action. **c.** Click **Edit**. **d.** Update the configuration. **e.** Click **OK**.
Delete an alert action	**a.** Click **Configure.** **b.** Highlight the alert action. **c.** Click **Delete.**
Add an email recipient to receive the alert action	**a.** Click **Configure.** **a.** Click **Add** in the Alert Action window. **b.** Click **Add** again inthe Recipients frame of the Action Configuration window. **c.** Enter an email or epage address of the recipient in the Enter email/epage address field. **d.** Click **OK.**
Enable email for a named email recipient	Check **Enable Email**.
Disable or delete an email recipient	Perform one of the following actions: – Highlight the recipient and uncheck **Enable**. – Highlight the recipient and click **Delete**.

Step 2 Enter the text that you want to display in the email message in the User-defined email text box.

Step 3 Click **Save** after you finish configuring the alert action.

What To Do Next

Enabling Trace Downloads, page 8-11

Related Topics

- Setting Alert Properties, page 8-7
- Configuring Emails for Alert Notification, page 8-11

Configuring Emails for Alert Notification

Procedure

Step 1 Select **System > Tools > Alert > Config Email Server**.

Step 2 Enter the email recipient information in the Mail Server field.

Step 3 Enter the port number of the mail server in the Port field. The default port is 25.

Step 4 Click **Add** in the Recipients frame of the Mail Server Configuration window.

Step 5 Enter an email or epage address of the recipient in the Enter email/epage address field.

Step 6 Enter the text that you want to display in the email message in the Default Message text box.

Step 7 Click **OK**.

Enabling Trace Downloads

Some preconfigured alerts will allow you to initiate a trace download based on the occurrence of an event. You can automatically capture traces when a particular event occurs by checking Enable Trace Download in Set Alert/Properties for the following alerts:

- CriticalServiceDown
- CoreDumpFileFound

⚠ **Caution** Enabling Trace Download may affect services on the server. Configuring a high number of downloads will adversely impact the quality of services on the server.

Before You Begin

Configure alert actions.

Procedure

Step 1 Click **Activate** in the Alert Properties: Email Notification window for alerts that do not allow trace download.

Step 2 Perform the following actions for alerts, such as CriticalServiceDown, that allow trace download:

a. Click **Next.**

b. Check **Enable TCT Download** in the Alert Properties: TCT Download window.

c. Enter the IP address, a user name, password, port and download directory path where the trace will be saved.

d. Click **Test Connection** to ensure that you have connectivity with the SFTP server. **If the connection test fails, your settings will not be saved.**

e. Click **OK.**

f. Enter the number and frequency of downloads in the TCT Download Parameters window. Setting the number and frequency of download will help you to limit the number of trace files that will be downloaded. The setting for polling provides the basis for the default setting for the frequency.

Troubleshooting Tips

Enabling TCT Download may affect services on the server. Configuring a high number of downloads will adversely impact the quality of services on the server.

Related Topics

- Configuring Alert Actions, page 8-10

Suspending Alerts on Cisco Unified Presence Nodes or the Cluster

You may want to temporarily suspend some or all alerts, either on a particular Cisco Unified Presence node or the entire cluster. For example, if you are upgrading the Cisco Unified Presence to a newer release, you would probably want to suspend all alerts until the upgrade completes, to ensure you do not receive emails or epages during the upgrade.

Procedure

Step 1 Select **System > Tools > Alert > Suspend Cluster/Node Alerts**.

Step 2 Perform one of the following actions:

If you want to:	Action
Suspend all alerts in the cluster	a. Click **Cluster Wide**. b. Check **Suspend all alerts**. c. Click **OK**.
Suspend alerts per server	a. Click **Per Server**. b. Check **Suspend** for each server on which you want alerts to be suspended. c. Click **OK**.
Resume alerts	a. Select **System > Tools > Alert > Suspend Cluster/Node Alerts.** b. Uncheck **Suspend** for each server on which you want alerts to resume. c. Click **OK**.

Troubleshooting Tips

Per server suspend states do not apply to Cisco Unified Presence clusterwide alerts.

Configuring Log Partition Monitoring

Log Partition Monitoring, which is installed automatically with the system, uses configurable thresholds to monitor the disk usage of the log partition on a server. The Cisco Log Partitioning Monitoring Tool service starts automatically after installation of Cisco Unified Presence. The Cisco Log Partitioning Monitoring Tool service starts automatically after installation of Cisco Unity.

Every 5 minutes, Log Partition Monitoring uses the following configured thresholds to monitor the disk usage of the log partition on a server:

- LogPartitionLowWaterMarkExceeded (% disk space)—When the disk usage is above the percentage that you specify, LPM sends out an alarm message to syslog and an alert to RTMT Alert central. To save the log files and regain disk space, you can use trace and log central option in RTMT.
- LogPartitionHighWaterMarkExceeded (% disk space)—When the disk usage is above the percentage that you specify, LPM sends a n alarm message to syslog and an alert to RTMT Alert central.

In addition, Cisco Log Partitioning Monitoring Tool service checks the server every 5 seconds for newly created core dump files. If there are new core dump files, Cisco Log Partitioning Monitoring Tool service sends a CoreDumpFileFound alarm and an alert to Alert Central with information on each new core file.

When the log partition monitoring services starts at system startup, the service checks the current disk space utilization. If the percentage of disk usage is above the low water mark, but less than the high water mark, the service sends a alarm message to syslog and generates a corresponding alert in RTMT Alert central.

To configure Log Partitioning Monitoring, set the alert properties for the LogPartitionLowWaterMarkExceeded and LogPartitionHighWaterMarkExceeded alerts in Alert Central.

To offload the log files and regain disk space on the server, you should collect the traces that you are interested in saving by using the Real-Time Monitoring tool.

If the percentage of disk usage is above the high water mark that you configured, the system sends an alarm message to syslog, generates a corresponding alert in RTMT Alert Central, and automatically purges log files until the value reaches the low water mark.

Note Log Partition Monitoring automatically identifies the common partition that contains an active directory and inactive directory. The active directory contains the log files for the current version of Cisco Unified Presence, and the inactive directory contains the log files for the previous installed version of Cisco Unified Presence. The active directory contains the log files for the current version of Cisco Unity, and the inactive directory contains the log files for the previous installed version of Cisco Unity. If necessary, the service deletes log files in the inactive directory first. The service then deletes log files in the active directory, starting with the oldest log file for every application until the disk space percentage drops below the configured low water mark. The service does not send an email when log partition monitoring purges the log files.

After the system determines the disk usage and performs the necessary tasks (sending alarms, generating alerts, or purging logs), log partition monitoring occurs at regular 5 minute intervals.

Before You Begin

To utilize log partition monitor, verify that the Cisco Log Partitioning Monitoring Tool service, a network service, is running on the server on Cisco Unified Serviceability. Stopping the service causes a loss of feature functionality.

.Procedure

Step 1 Select **Tools > Control Center > Network Services**.

Step 2 Select the server where you want to monitor the disk usage from the Servers list box.

Step 3 Click **Go**.

Step 4 Verify the status of the Cisco Log Partition Monitoring Tool (LPM) under Performance and Monitoring Services.

Step 5 Click the radio button next to Cisco LPM If the LPM is not running.

Step 6 Click **Start**.

Related Topics

- Setting Alert Properties, page 8-7