CHAPTER 9

Understanding Alerts

This chapter contains information on the following topics:

Using RTMT for Alerts

The system generate alert messages to notify administrator when a predefined condition is met, such as when an activated service goes from up to down. The system can send alerts as e-mail/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 category 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 server or on an entire cluster (if applicable).
- Clear Alerts—This menu category allows you to reset an alert (change the color of an alert item to black) to signal that an alert has been handled. After an alert has been raised, its color will automatically change in RTMT and will stay that way until you manually clear the alert.

Note The manual clear alert action does not update the System cleared timestamp column in Alert Central. This column is updated only if alert condition is automatically cleared.

- Clear All Alerts—This menu category allows you to clear all alerts.
- Reset all Alerts to Default Config—This menu category allows you to reset all the alerts to the default configuration.
- Alert Detail—This menu category provides detailed information on alert events.
- Config Email Server—In this category, you can configure your e-mail server to enable alerts.

Note To configure RTMT to send alerts via e-mail, you must configure DNS. For information on configuring the primary and secondary DNS IP addresses and the domain name in Cisco Unified Communications Manager Server Configuration, see the "DHCP Server Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

- 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 e-mail 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. RTMT predefined alerts are configured for perfom counter value thresholds as wells as event (alarms) notifications.

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.

Additional Information

See the Related Topics, page 9-10.

Viewing Alerts

RTMT displays both preconfigured alerts and custom alerts in Alert Central. RTMT organizes the alerts under the applicable tabs—System, CallManager, Cisco Unity Connection, and Custom.

Stand-alone Cisco Unified CM installation will not include Cisco Unity Connection tab and vice- versa. However, Cisco Unified CM Business Edition 5000 will have all the above tabs.

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

System Alerts

Note For alert descriptions and default configurations, see "System Alert Descriptions and Default Configurations" section on page E-1.

The following list comprises the preconfigured system alerts.

- AuthenticationFailed
- CiscoDRFFailure
- CoreDumpFileFound
- CpuPegging
- CriticalAuditEventGenerated
- CriticalServiceDown
- HardwareFailure
- LogFileSearchStringFound
- LogPartitionHighWaterMarkExceeded
- LogPartitionLowWaterMarkExceeded
- LowActivePartitionAvailableDiskSpace
- LowAvailableVirtualMemory
- LowInactivePartitionAvailableDiskSpace
- LowSwapPartitionAvailableDiskSpace
- ServerDown (*Unified CM clusters only*)
- SparePartitionHighWaterMarkExceeded
- SparePartitionLowWaterMarkExceeded
- SyslogSeverityMatchFound
- SyslogStringMatchFound
- SystemVersionMismatched
- TotalProcessesAndThreadsExceededThreshold

Note Since none of the audit events are alert worthy, there is no way to trigger the CriticalAuditEventGenerated alert.

CallManager Alerts

The following list comprises the preconfigured CallManager alerts.

Note For alert descriptions and default configurations, see "CallManager Alert Descriptions and Default Configurations" section on page F-1.

- BeginThrottlingCallListBLFSubscriptions
- CallAttemptBlockedByPolicy
- CallProcessingNodeCpuPegging
- CARIDSEngineCritical
- CARIDSEngineFailure
- CARSchedulerJobFailed

- CDRAgentSendFileFailed
- CDRFileDeliveryFailed
- CDRHighWaterMarkExceeded
- CDRMaximumDiskSpaceExceeded
- CodeYellow
- DBChangeNotifyFailure
- DBReplicationFailure
- DBReplicationTableOutOfSync
- DDRBlockPrevention
- DDRDown
- EMCCFailedInLocalCluster
- EMCCFailedInRemoteCluster
- ExcessiveVoiceQualityReports
- IMEDistributedCacheInactive
- IMEOverQuota
- IMEQualityAlert
- InsufficientFallbackIdentifiers
- IMEServiceStatus
- InvalidCredentials
- LowTFTPServerHeartbeatRate
- MaliciousCallTrace
- MediaListExhausted
- MgcpDChannelOutOfService
- NumberOfRegisteredDevicesExceeded
- NumberOfRegisteredGatewaysDecreased
- NumberOfRegisteredGatewaysIncreased
- NumberOfRegisteredMediaDevicesDecreased
- NumberOfRegisteredMediaDevicesIncreased
- NumberOfRegisteredPhonesDropped
- RouteListExhausted
- SDLLinkOutOfService
- TCPSetupToIMEFailed
- TLSConnectionToIMEFailed
- UserInputFailure

Cisco Unity Connection Alerts

The following list comprises the preconfigured Cisco Unity Connection alerts. These alerts apply only to Cisco Unity Connection and Cisco Unified Communications Manager Business Edition 5000.

Note For alert descriptions and default configurations, see "Cisco Unity Connection Alert Descriptions and Default Configurations" section on page G-1.

- NoConnectionToPeer *(Cisco Unity Connection cluster configuration only)*
- AutoFailoverSucceeded *(Cisco Unity Connection cluster configuration only)*
- AutoFailoverFailed *(Cisco Unity Connection cluster configuration only)*
- AutoFailbackSucceeded *(Cisco Unity Connection cluster configuration only)*
- AutoFailbackFailed *(Cisco Unity Connection cluster configuration only)*
- SbrFailed (Split Brain Resolution Failed) *(Cisco Unity Connection cluster configuration only)*
- DiskConsumptionCloseToCapacityThreshold
- DiskConsumptionExceedsCapacityThreshold
- LicenseExpirationWarning
- LicenseExpired

Note The first six alerts apply to Cisco Unity Connection cluster configurations only. Cisco Unified Communications Manager Business Edition 5000 does not support a Cisco Unity Connection cluster configuration.

Additional Information

See the Related Topics, page 9-10.

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.

Note Severity levels for Syslog entries match the severity level for all RTMT alerts. If RTMT issues a critical alert, the corresponding Syslog entry also specifies critical.

Table 9-1 provides a list of fields that you may use to configure each alert; users can configure preconfigured fields, unless otherwise noted.

Table 9-1 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 the "Viewing Alerts" section on page 9-2.
Description	Description of the alert	You cannot edit this field for preconfigured alerts. For a list of preconfigured alerts, see the "Viewing Alerts" section on page 9-2.
Performance Counter(s)	Source of the performance counter	You cannot change this field. You can associate only one instance of the performance counter with an alert.
Threshold	Condition to raise alert (value is...)	Specify up < - > down, less than #, %, rate greater than #, %, rate. This field is applicable only for alerts based on performance counters.
Value Calculated As	Method used to check the threshold condition	Specify value to be evaluated as absolute, delta (present - previous), or % delta. This field is applicable only for alerts based on performance counters.
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. This field is applicable only for alerts based on performance counters.
Number of Events Threshold	Raise alert only when a configurable number of events exceeds a configurable time interval (in minutes).	For ExcessiveVoiceQualityReports, the default thresholds equal 10 to 60 minutes. For RouteListExhausted and MediaListExhausted, the defaults equal 0 to 60 minutes. This field is applicable only for event based alerts.
Node IDs *(Unified CM clusters only)*	Cluster or list of servers to monitor	Cisco Unified Communications Manager servers, Cisco TFTP server, or first server. This field is applicable only for non-clusterwide alerts. **Note** When you deactivate both the Cisco CallManager and Cisco TFTP services of a server, the system considers that server as removed from the currently monitored server list. When you reactivate both Cisco CallManager and Cisco TFTP services, that server is added back, and its settings are restored to default values.

Table 9-1 Alert Customization (continued)

Field	Description	Comment
Alert Action ID	ID of alert action to take (System always logs alerts no matter what the alert action.)	Alert action gets defined first (see the "Additional Information" section on page 9-7). If this field is blank, that indicates that e-mail is disabled.
Enable Alerts	Enable or disable alerts.	Options include enabled or disabled.
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 Details *(Unified CM clusters only)*	Displays the detail of an alert (not configurable)	For ExcessiveVoiceQualityReports, RouteListExhausted, and MediaListExhausted, up to 30 current event details display in the current monitoring interval if an alert has been raised in the current interval. Otherwise, the previous 30 event details in the previous interval displays. For DChannel OOS alert, the list of outstanding OOS devices at the time the alert was raised displays.
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.

Additional Information

See the Related Topics, page 9-10.

Alert Action Configuration

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

Table 9-2 provides a list of fields that you will use to configure alert actions. Users can configure all fields, unless otherwise marked.

Table 9-2 Alert Action Configuration

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

Additional Information

See the Related Topics, page 9-10.

Enabling Trace Download

Some preconfigured alerts 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 the Enable Trace Download check box in Set Alert/Properties for the following alerts:

- CriticalServiceDown - CriticalServiceDown alert gets generated when any service is down.

Note The RTMT backend service checks status (by default) every 30 seconds. If service goes down and comes back up within that period, CriticalServiceDown alert may not get generated.

Note CriticalServiceDown alert monitors only those services that are listed in RTMT Critical Services.

- CodeYellow - This alarm indicates that Cisco Unified Communications Manager initiated call throttling due to unacceptably high delay in handling calls.
- CoreDumpFileFound - CoreDumpFileFound alert gets generated when RTMT backend service detects a new Core Dump file.

Note You can configure both CriticalServiceDown and CoreDumpFileFound alerts to download corresponding trace files for troubleshooting purposes. This helps preserve trace files at the time of crash.

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.

Additional Information

See the Related Topics, page 9-10.

Understanding Alert Logs

The alert log stores the alert, which is also stored in memory. The memory gets 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 on the server or on all servers in the cluster (if applicable). The alert data in the memory gets 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. Alert log periodically gets updated, and new logs get 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—Server name for where RTMT raised the alert
- Alert Message—Detailed description about the alert
- Type—Type of 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.

Additional Information

See the Related Topics, page 9-10.

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 Partition Monitoring Tool service starts automatically after installation of the system.

Every 5 minutes, Log Partition Monitoring uses the following configured thresholds to monitor the disk usage of the log partition and the spare 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 an alarm message to syslog and an alert to RTMT Alert central.

- SparePartitionLowWaterMarkExceeded (% 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.
- SparePartitionHighWaterMarkExceeded (% 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 new core dump files exist, Cisco Log Partitioning Monitoring Tool service sends a CoreDumpFileFound alarm and an alert to Alert Central with information on each new core file.

To utilize log partition monitor, verify that the Cisco Log Partitioning Monitoring Tool service, a network service, is running on Cisco Unified Serviceability on the server or on each server in the cluster (if applicable). Stopping the service causes a loss of feature functionality.

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. For more information, see "Setting Alert Properties" section on page 10-3.

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 installed version of the software (Cisco Unified Communications Manager and/or Cisco Unity Connection), and the inactive directory contains the log files for the previous installed version of the software. 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 e-mail 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.

Where to Find More Information

Related Topics

- Using RTMT for Alerts, page 9-1
- Viewing Alerts, page 9-2
- Alert Fields, page 9-5
- Alert Action Configuration, page 9-7
- Enabling Trace Download, page 9-8

- Understanding Alert Logs, page 9-9
- Working with Alerts, page 10-1
- Setting Alert Properties, page 10-3
- Suspending Alerts, page 10-5
- Configuring E-mails for Alert Notification, page 10-6
- Configuring Alert Actions, page 10-6