Cisco Unified Real-Time Monitoring Tool Administration Guide

For Cisco Unified Contact Center Express and Cisco Unified IP IVR
Release 8.0(1)

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number: OL-20103-01

Preface

This preface describes the purpose, audience, organization, and conventions of this guide and provides information on how to obtain related documentation.

This document may not represent the latest Cisco product information that is available. You can obtain the most current documentation by accessing Cisco product documentation page at this URL:

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/tsd_products_support_series_home.html

The preface covers these topics:

Purpose

The *Cisco Unified Real-Time Monitoring Tool Administration Guide* provides information about the Cisco Unified Real-Time Monitoring Tool (RTMT).

Use this book with the following documents for configuring Unified CCX:

Cisco Unified Contact Center Express (Unified CCX)	*Cisco Unified Contact Center Express Administration Guide, Cisco Unified Serviceability Administration Guide., Cisco Unified Contact Center Express Serviceability Guide*

These documents provide the following information:

- Instructions for administering Unified CCX.
- Descriptions of procedural tasks that you complete by using the administration interface.

Audience

The *Cisco Unified Real-Time Monitoring Tool Administration Guide* provides information for network administrators who are responsible for managing and supporting Unified CCX. Network engineers, system administrators, or telecom engineers use this guide to learn about, and administer, remote serviceability features. This guide requires knowledge of telephony and IP networking technology.

Organization

The following table shows how this guide is organized:

Chapter	Description
Real-Time Monitoring Tool	
Chapter 1, "Understanding Cisco Unified Real-Time Monitoring Tool"	Provides a brief description of the Cisco Unified Real-Time Monitoring Tool (RTMT).
Chapter 2, "Installing and Configuring Cisco Unified Real-Time Monitoring Tool"	Provides procedures for installing, upgrading, and uninstalling RTMT. Also provides information on how to navigate within RTMT and how to configure profiles.
Performance Monitoring	
Chapter 3, "Understanding Performance Monitoring"	Provides an overview of performance counters.
Chapter 4, "Monitoring Predefined System Objects"	Provides information on working with predefined system objects.
Chapter 5, "Working with Performance Queries"	Provides procedures for working with performance monitors, including viewing performance counters and counter descriptions, and perfmon logs.
Chapter 6, "Viewing and Troubleshooting Perfmon Logs"	Provides information about how to download perfmon logs or view them locally.
Alerts	
Chapter 7, "Understanding Alerts"	Provides an overview of alerts, including a description of preconfigured alerts. Describes fields that you use to configure alerts and alert actions.
Chapter 8, "Working with Alerts"	Provides procedures for working with Alerts.
Tools for Traces, Logs, and Plug-Ins	
Chapter 9, "Working with Trace and Log Central"	Provides information on configuring on-demand trace collection and crash dump files for system services as well as on viewing the trace files in the appropriate viewer.
Chapter 10, "Using SysLog Viewer"	Provides information on using the SysLog Viewer.
Chapter 11, "Using Plug-ins"	Provides information on installing and using plug-ins in the Real-Time Monitoring tool.
Analysis Manager	

Chapter	Description
Chapter 12, "Understanding Cisco Unified Analysis Manager for Cisco Unified Contact Center Express"	Provides information on Cisco Unified Analysis Manager, how to install and configure Analysis Manager, and how to identify and add nodes and call record repositories that the Analysis Manager can diagnose.
Appendixes: Performance Counter and Alerts Descriptions	
Appendix A, "System Performance Objects and Counters"	Provides a list of performance objects and their associated counters for the system
Appendix B, "Performance Objects and Counters for Unified CCX"	Provides a complete list of performance objects and their associated counters. Provides tables with related information about Unified CCX perfmon counters, the Cisco Unified Real-Time Monitoring Tool, and CCM_SNMP_MIB.
Appendix C, "System Alert Descriptions and Default Configurations"	This appendix contains descriptions and default configurations of system alerts.
Appendix D, "Cisco Unified Contact Center Express Alert Descriptions and Default Configurations"	This appendix contains descriptions and default configurations of Unified CCX alerts.

Related Documentation

- For additional documentation on Unified CCX, visit the following URL: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/tsd_products_support_series_home.html
- For a complete list of terms used in Cisco Unified CCX and Cisco Unified IP IVR, see the following URL: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_technical_reference_list.html

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Convention	Description
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
⟶	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Timesavers use the following conventions:

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Tips use the following conventions:

Tip Means *the information contains useful tips.*

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following conventions:

Warning **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.**

Obtain Additional Support and Documentation

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Documentation Feedback

You can provide comments about this document by sending an email to the following address:

ccbu_docfeedback@cisco.com

We appreciate your comments.

CONTENTS

PART 1

Cisco Unified Real-Time Monitoring Tool Basics

CHAPTER 1

Understanding Cisco Unified Real-Time Monitoring Tool

Note This document uses the following abbreviations to identify administration differences for these Cisco products:
Unified CM refers to Cisco Unified Communications Manager
Unified CCX refers to Cisco Unified Contact Center Express

The Cisco Unified Real-Time Monitoring Tool (RTMT), which runs as a client-side application, uses HTTPS and TCP to monitor system performance. RTMT can connect directly to devices via HTTPS to troubleshoot system problems.

Note Even when RTMT is not running as an application on your desktop, tasks such as alarm and performance monitoring updates continue to take place on the server in the background.

RTMT allows you to perform the following tasks:

- Monitor a set of predefined management objects that monitor the health of the system.
- Generate various alerts, in the form of e-mails, for objects when values go over/below user-configured thresholds.
- Collect and view traces in various default viewers that exist in RTMT.
- View syslog messages in SysLog Viewer.
- Work with performance-monitoring counters.

This chapter contains information on the following topics:

Services, Servlets, and Service Parameters on the Server

To support the RTMT client, several services need to be active and running on the server. RTMT uses the following services/servlets:

- Cisco AMC service—This service starts up automatically after the installation and allows RTMT to retrieve real-time information from the server or from a server in a cluster (if applicable).

Caution You must configure a second server as the failover collector in Cisco Unified Contact Center Express Administration, so RTMT can continue to retrieve information if the primary collector fails. Otherwise, RTMT cannot retrieve information if the primary collector has failed.

  The following list comprises some Cisco AMC service parameters that are associated with RTMT:

  - Primary Collector
  - Failover Collector
  - Data Collection Enabled
  - Data Collection Polling Rate
  - Server Synchronization Period
  - RMI Registry Port Number
  - RMI Object Port Number
  - AlertMgr Enabled
  - Logger Enabled

Note For the latest list of parameters, go to the Service Parameters window of the Cisco Unified CCX Serviceability interface; then, choose Cisco AMC service.

Note For information on these service parameters, see the service parameter Help.

- Cisco RIS Data Collector (in the Control Center—Network Services window in Cisco Unified Serviceability)—The Real-time Information Server (RIS) maintains real-time information such as performance counter statistics, critical alarms generated, and so on. The Cisco RIS Data Collector service provides an interface for applications, such as Cisco Unified Real-Time Monitoring Tool (RTMT), SOAP applications, and AlertMgrCollector (AMC) to retrieve the information that is stored on the server.
- Cisco Tomcat Stats Servlet (in the Control Center—Network Services window in Cisco Unified Serviceability)—The Cisco Tomcat Stats Servlet allows you to monitor the Tomcat perfmon counters by using RTMT or the Command Line Interface. Do not stop this service unless you suspect that this service is using too many resources, such as CPU time.
- Cisco Trace Collection Servlet (in the Control Center—Network Services window in Cisco Unified Serviceability)—The Cisco Trace Collection Servlet, along with the Cisco Trace Collection Service, supports trace collection and allows users to view traces by using the RTMT client. If you stop this service on a server, you cannot collect or view traces on that server.

- Cisco Trace Collection Service (in the Control Center—Network Services window in Cisco Unified Serviceability)—The Cisco Trace Collection Service, along with the Cisco Trace Collection Servlet, supports trace collection and allows users to view traces by using the RTMT client. If you stop this service on a server, you cannot collect or view traces on that server.
- Cisco Log Partition Monitoring Tool (in the Control Center—Network Services window in Cisco Unified Serviceability)—This service, which starts up automatically after the installation, monitors the disk usage of the log partition on a server.
- Cisco SOAP-Real-Time Service APIs (in the Control Center—Network Services window in Cisco Unified Serviceability)—The Cisco SOAP-Real-Time Service APIs, which start up automatically after the installation, allow you to collect real-time information for the system.
- Cisco SOAP-Performance Monitoring APIs (in the Control Center—Network Services window in Cisco Unified Serviceability)—This service, which starts up automatically after the installation, allows you to use performance monitoring counters for various applications through SOAP APIs.
- Cisco RTMT Reporter servlet (in the Control Center—Network Services window in Cisco Unified Serviceability)—This service, which starts up automatically after the installation, allows you to publish reports for RTMT.
- Cisco Serviceability Reporter (in the Control Center—Feature Services window in Cisco Unified Serviceability)—The Cisco Serviceability Reporter service allows you to publish reports for RTMT.

Additional Information

See the "Related Topics" section on page 1-4.

Nonconfigurable Components on the Server (RTMT Collector, Alert Manager, and RTMT Reporter)

RTMT Collector, a component that automatically gets installed with the application, logs preconfigured monitoring objects information while Alert Manager, also automatically installed, logs alert histories into log files. Each preconfigured object belongs to one of several categories: servers and alerts. Each category uses a separate log file, and alert details also get logged in a separate file.

The system also records important perfmon object values in performance log files.

Tip Although they require no configuration tasks to run, RTMT Collector and Alert Manager support redundancy. If the primary collector or manager fails for any reason, the secondary collector and manager perform the tasks until primary support becomes available. RTMT Collector, Alert Manager, and RTMT Reporter run on the first server to minimize call-processing interruptions.

The locally written log files appear in the primary collector server at cm/log/amc. For Unified CCX clusters, the log files can exist on more than one server in the cluster because the primary collector changes in failover and fallback scenarios.

You can display log files, except an alert log file, by using the Performance log viewer in RTMT or by using the native Microsoft Performance viewer. For more information on using the Performance log viewer in RTMT, refer to "Where to Find More Information" section on page 5-11. You can view an alert log file by using any text editor.

To download log files to a local machine, you can use the collect files option in Trace and Log Central in RTMT. For more information on downloading log files by using the collect files option, refer to "Collecting Trace Files" section on page 9-3.

Alternatively, from the command line interface (CLI), you can use the file list command to display a list of files and the file get command to download files by SFTP. For more information on using CLI commands, see the *Command Line Interface Reference Guide for Cisco Unified Contact Center Express*. available here:

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_maintenance_guides_list.html

Log files exist in csv format. New log files get created every day at 00:00 hours on the local system. The first column of all these logs comprises the time zone information and the number of minutes from the Greenwich Meridian Time (GMT). RTMT Reporter uses these log files as a data source to generate daily summary reports. The report, which is based on the default monitoring objects, generates every 24 hours for the following information:

- Server Status—% CPU load,% memory used,% disk space used per server.
- Alert Status—Number of alerts per server. For Unified CCX clusters, number of alerts per severity level for the cluster, including the top 10 alerts in the cluster.

Tip The RTMT reports display in English only.

The following service parameters apply to RTMT report generation: RTMT Reporter Designated server, RTMT Report Generation Time, and RTMT Report Deletion Age. For information on these parameters, go to the service parameter Help for your configuration by choosing a service in the Service drop-down list box of the Service Parameters window and then clicking **Help > This Page**.

For more information on the Serviceability reports, see the "Serviceability Reports" chapter in *Cisco Unified Serviceability Administration Guide* available here:
http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Additional Information

See the "Related Topics" section on page 1-4.

Where to Find More Information

Related Topics

- Services, Servlets, and Service Parameters on the Server, page 1-2
- Nonconfigurable Components on the Server (RTMT Collector, Alert Manager, and RTMT Reporter), page 1-3

CHAPTER 2

Installing and Configuring Cisco Unified Real-Time Monitoring Tool

You can install Cisco Unified Real-Time Monitoring Tool (RTMT), which works for resolutions 800*600 and above, on a computer that is running Windows 98, Windows XP, Windows 2000, Windows Vista, or Linux with KDE and/or Gnome client.

Note RTMT requires at least 128 MB in memory to run on a Windows OS platform.

This chapter contains information on the following topics:

Installing RTMT

A single copy of RTMT that is installed on your computer lets you monitor one server or one cluster at a time. For example, you can monitor either of the following entities:

- A Unified CCX product on one server.
- A server on a cluster to monitor the health of the cluster.

To monitor a product on a different server, you must first log off the server before you can log on to the other server.

Note For accessing Unified Analysis Manager, install the RTMT Client from Cisco Unified Communications Manager on a separate Client box.

Before you install RTMT, consider the following limitations:

- On a client machine, you can install RTMT client downloaded from only one product type - Unified CCX or say, Unified CM. Installing RTMT client from different product types on the same client machine is not supported.
- Using one instance or a multiple instances of the single RTMT installed on the same client machine you won't be able to monitor different products. For example, the RTMT Client installed from the Unified CCX server cannot be used to monitor either Unified CM, CUP, or Unity Connection. Similarly, RTMT installed from the Unified CM cannot be used to monitor Unified CCX or other products.
  To monitor different products, install RTMT from the respective servers on different client machines.
- The current RTMT download may not support earlier releases of Unified CCX. Some releases of Unified CCX may require different versions of RTMT to be installed on your computer (one version per Unified CCX release). Verify that the RTMT version that you install is compatible with the Unified CCX that you are monitoring. If the RTMT version that you are using is not compatible with the server that you want to monitor, the system prompts you to download the compatible version.
- Your computer stores the user preferences, such as the IP address and RTMT frame size, from the RTMT client that last exits.

To install the tool, perform the following procedure:

Note While installing RTMT on a Windows Vista platform, you will see a User Account Control pop-up message that says, "An unidentified program wants to access your computer." Click **Allow** to continue working with RTMT.

Procedure

Step 1 Go to the Plug-ins window of the administration interface for your configuration by choosing **Applications** or **System Settings > Plugins** from the Cisco Unified Contact Center Express Administration Web interface:

Step 2 Click the **Find** button.

Step 3 To install the RTMT tool on a client that is running the Microsoft Windows operating system, click the **Download** link for the Cisco Unified CCX Real-Time Monitoring Tool-Windows.

To install the RTMT tool on a client that is running the Linux operating system, click the **Download** link for the Cisco Unified CCX Real-Time Monitoring Tool-Linux.

Step 4 Download the executable to the preferred location on your client.

Step 5 To install the Windows version, double-click the RTMT icon that displays on the desktop or locate the directory where you downloaded the file and run the RTMT installation file.

The extraction process begins.

Step 6 To install the Linux version, ensure that the file has execute privileges; for example, enter the following command, which is case sensitive: **chmod +x CcmServRtmtPlugin.bin**

Step 7 After the RTMT welcome window displays, click **Next**.

Step 8 To accept the license agreement, click **I accept the terms of the license agreement**; then, click **Next**.

Step 9 Choose the location where you want to install RTMT. If you do not want to use the default location, click **Browse** and navigate to a different location. Click **Next**.

Default installation paths are:

- Windows—C:\Program Files\Cisco\Unified Serviceability\JRtmt
- Linux—/opt/ Cisco/Unified Serviceability/JRtmt

Step 10 To begin the installation, click **Next**.

The Setup Status window displays. Do not click Cancel.

Step 11 To complete the installation, click **Finish**.

Additional Information

See the "Related Topics" section on page 2-7.

Uninstalling RTMT

Tip When you use RTMT, it saves user preferences and the module jar files (the cache) locally on the client machine. When you uninstall RTMT, you choose whether to delete or save the cache.

On a Windows client, you uninstall RTMT through **Add/Remove Programs** under the Control Panel. (Choose **Start > Settings > Control Panel >Add/Remove Programs**.)

To uninstall RTMT on a Red Hat Linux with KDE and/or Gnome client, choose **Start > Accessories > Uninstall Real-time Monitoring tool** from the task bar.

Note While uninstalling RTMT on a Windows Vista machine, you will a see a User Account Control pop-up message that says, "An unidentified program wants to access your computer." Click **Allow** to continue working with RTMT.

Additional Information

See the "Related Topics" section on page 2-7.

Launching RTMT

Caution You must configure a second server as the failover collector in Cisco Unified Contact Center Express Administration, so RTMT can continue to retrieve information if the primary collector fails. Otherwise, RTMT cannot retrieve information if the primary collector has failed.

Note While using RTMT on a Windows Vista machine, you will a see a User Account Control pop-up message that says, "An unidentified program wants to access your computer." Click **Allow** to continue working with RTMT.

Procedure

Step 1 After you install the plug-in, perform one of the following tasks:

- From your Windows desktop, double-click the **Real-Time Monitoring Tool** icon.
- Choose **Start > All Programs > Cisco > Unified Serviceability > Real-Time Monitoring Tool**.

The Real-Time Monitoring Tool Login window displays.

Step 2 In the Host IP Address field, enter either the IP address or host name of the server or (if applicable) first server in a cluster.

Step 3 In the User Name field, enter the Application Username for the application.

Note Use the Application User credentials (provided during the Unified CCX installation) for logging in to RTMT. In case you forget the Application User credentials, reset it using the CLI commands provided in the "Gathering Configuration Information for Installation" section of the *Installation Guide for Cisco Unified Contact Center Express and Cisco Unified IP IVR* available here:
http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html

Step 4 In the Password field, enter the Administrator user password that you established for the username.

Note If the authentication fails or if the server is unreachable, the tool prompts you to reenter the server and authentication details, or you can click the Cancel button to exit the application. After the authentication succeeds, RTMT launches the monitoring module from local cache or from a remote server, when the local cache does not contain a monitoring module that matches the backend version.

Step 5 Enter the port that the application will use to listen to the server. The default setting equals 8443.

Note The Trace and Log Central tool in RTMT uses the port number that you specify to communicate with all the nodes in a cluster. If your system uses port mapping and all Unified CCX nodes do not map to the same port number, then some RTMT tools can not connect to those nodes. The tools that will fail to connect include Trace and Log Central, Job Status, SyslogViewer, Perfmon Log Viewer, and FTP/SFTP Configuration.

Step 6 Check the **Secure Connection** check box.

Step 7 Click **OK**.

Step 8 When prompted, add the certificate store by clicking **Yes**.

RTMT starts.

Additional Information

See the "Related Topics" section on page 2-7.

Navigating RTMT

The RTMT window comprises the following main components:

- Menu Bar, which includes some or all of the following menu options, depending on your configuration:
  - File—Allows you to save, restore, and delete existing RTMT profiles, monitor Java Heap Memory Usage, go to the Serviceability Report Archive window in Cisco Unified Serviceability, log off, or exit RTMT.
  - System—Allows you to monitor system summary, monitor server resources, work with performance counters, work with alerts, collect traces, and view syslog messages.
  - Edit—Allows you to configure categories (for table format view), set the polling rate for devices and performance monitoring counters, hide the quick launch channel, and edit the trace setting for RTMT.
  - Window—Allows you to close a single RTMT window or all RTMT windows.
  - Application—Allows you to browse the applicable web pages for Cisco Unified Serviceability.
  - Help—Allows you to access RTMT documentation online help or to view the RTMT version.
- Quick Launch Channel—Pane on the left side of RTMT window with tabs that you can click to display information on the server or information on the applications. The tab contains groups of icons that you can click to monitor various objects.
- Monitor pane—Pane where monitoring results display.

Additional Information

See the "Related Topics" section on page 2-7.

Working with Configuration Profiles

You can use RTMT to connect to a server or to any server in a Unified CCX cluster (if applicable). After you log in to a server, RTMT launches the monitoring module from the local cache or from a remote server when the local cache does not contain a monitoring module that matches the backend version.

RTMT includes a default configuration that is called Default. The first time that you use RTMT, it uses the Default profile and displays the system summary page in the monitor pane.

You can configure RTMT to display the information that interests you, such as different performance counters for different features, in the monitor pane of RTMT and save the framework of your configuration in a profile. You can then restore the profile at a later time during the same session or the next time that you log in to RTMT. By creating multiple profiles, so each profile displays unique information, you can quickly display different information by switching profiles.

Note If you are running the RTMT client and monitoring performance counters during a Unified CCX upgrade, the performance counters will not update during and after the upgrade. To continue monitoring performance counters accurately after the Unified CCX upgrade completes, you must either reload the RTMT profile or restart the RTMT client.

This section provides information on the following topics:

Using the Default Configuration Profile

When you initially load RTMT, the system includes a default profile that is called Default. The first time that you use RTMT, it will use the Default profile and display the system summary page in the monitor pane.

Adding Configuration Profiles

With RTMT, you can customize your monitoring window by monitoring different performance counters, then create your own configuration profiles, so you can restore these monitoring windows in a single step rather than opening each window again. You can switch between different profiles during the same RTMT session or use the configuration profile in subsequent RTMT sessions.

The following procedure describes how to create a profile.

Procedure

Step 1 Choose **System > Profile**.

The Preferences dialog box displays.

Step 2 Click **Save**.

The Save Current Configuration dialog box displays.

Step 3 In the Configuration name field, enter a name for this particular configuration profile.

Step 4 In the Configuration description field, enter a description of this particular configuration profile.

Note You can enter whatever you want for the configuration profile name and description.

Note Profiles apply to all servers within a cluster, but the profile cannot be saved and applied to a different cluster.

The system creates the new configuration profile.

Restoring Profiles

Perform the following procedure to restore a profile that you configured:

Procedure

Step 1 Choose **System > Profile**.

The Preferences dialog box displays.

Step 2 Click the profile that you want to restore.

Step 3 Click **Restore**.

All windows with precanned settings and/or performance monitoring counters for the restored configuration open.

Deleting Configuration Profiles

Perform the following procedure to delete a profile that you configured:

Procedure

Step 1 Choose **System > Profile**.

The Preferences dialog box displays.

Step 2 Click the profile that you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Close**.

Additional Information

See the "Related Topics" section on page 2-7.

Where to Find More Information

Related Topics

- Installing RTMT, page 2-1
- Uninstalling RTMT, page 2-3
- Launching RTMT, page 2-3
- Navigating RTMT, page 2-5
- Working with Configuration Profiles, page 2-5

PART 2

Performance Monitoring

CHAPTER 3

Understanding Performance Monitoring

Unified CCX provides Performance counters (called PerfMon counters) for application performance monitoring. The PerfMon counters help expose critical performance values, making it possible to track application performance in real time.

The PerfMon counters contain counter-based information, such as the name and index of the counter, the scale, the type, sub-counters to set when setting a counter, the current values, and a map containing counter instance data. Each performance counter instance object contains instance-based data, like the instance ID and current values.

You can monitor the performance of the components of the system and the components for the application on the system by choosing the counters for any object by using RTMT. The counters for each object display when the folder expands.

You can log perfmon counters locally on the computer and use the performance log viewer in RTMT to display the perfmon CSV log files that you collected or the Realtime Information Server Data Collection (RISDC) perfmon logs.

This chapter contains information on the following topics:

Using RTMT for Performance Monitoring

RTMT displays performance information for all the Unified CCX components, along with all the System Components.

RTMT provides alert notifications for troubleshooting performance. It also periodically polls performance counter to display data for that counter. Refer to "Displaying a Counter Description" section on page 5-8 for examples on displaying perfmon counters in a chart or table format.

Performance monitoring allows you to perform the following tasks:

- Continuously monitor a set of preconfigured objects AND receive notification in the form of an e-mail message.
- Associate counter threshold settings to alert notification. An e-mail or popup message provides notification to the administrator.

- Save and restore settings, such as counters being monitored, threshold settings, and alert notifications, for customized troubleshooting tasks.
- Display up to six perfmon counters in one chart for performance comparisons.
- Use performance queries to add a counter to monitor. See "Working with Performance Queries" section on page 5-1 for more information.

Understanding the Performance Counter Interface

RTMT contains ready-to-view, predefined performance counters. You can also select and add counters to monitor in RTMT.

- To view predefined system counters, see "Monitoring Predefined System Objects" section on page 4-1.
- To view predefined Unified CCX counters, see "Predefined Cisco Unified Contact Center Express Objects Overview" section on page 5-1.
- To add a counter to monitor, see "Working with Performance Queries" section on page 5-1.

RTMT displays performance counters in chart or table format. Chart format looks like a miniature window of information. You can display a particular counter by double clicking the counter in the perfmon monitoring pane.

Attributes for predefined performance counters, such as format and category, remain fixed. You can define attributes for counters that you configure in RTMT. Because chart view represents the default, you configure the performance counters to display in table format when you create a category.

This section contains the following topics:

Category Tabs

A category comprises a group of monitored performance counters. A tab in the RTMT monitoring pane contains the category name. All performance counters that are monitored in this tab belong to a category. RTMT displays any categories that you access during a RTMT session in the bottom toolbar.

The system polls the performance counters in the tab at the same rate, with each category configured to have its own polling rate.

You can create custom categories in the RTMT monitoring pane to view information that helps you troubleshoot specific performance, system, or device problems. If your system is experiencing performance problems with specific objects, create custom categories to monitor the performance of the counters within the object. In addition, you can create alert notifications for counters in these custom categories. To create custom categories, you add a new category tab. When the tab is created, you specify the specific performance counters, devices, and alerts within that tab and then save your custom category by using Profile.

Sample Rate

The application polls the counters to gather status information.

The polling rate in each precanned monitoring window remains fixed, and the default value specifies 30 seconds. If the collecting rate for the AMC (Alert Manager and Collector) service parameter changes, the polling rate in the precanned window also updates. In addition, the local time of the RTMT client application and not the backend server time, provides the basis for the time stamp in each chart. For more information on Service Parameters, refer to *Cisco Unified Contact Center Express Serviceability Administration Guide*.

In the RTMT monitoring pane, you configure the polling intervals for the applicable performance counters for each category tab that you create.

Note High-frequency polling rate affects the performance on the server. The minimum polling rate for monitoring a performance counter in chart view equals 5 seconds; the minimum rate for monitoring a performance counter in table view equals 1 second. The default for both specifies 10 seconds.

Zoom Feature

To get a closer look at perfmon counters, you can zoom a perfmon monitor counter in the RTMT. See also Highlight Feature, page 3-4.

Procedure

Step 1 To zoom in a counter, perform one of the following tasks:

- To zoom predefined objects, such as System Summary, perform one of the following tasks:
  - Drag the mouse over the plot area in the counter to frame the data and release the mouse button. The counter zooms in the chart.
  - Click the counter. The counter zooms in.
- To zoom counters in the Performance pane, perform one of the following tasks (and resize the window, if necessary):
  - Double-click the counter that you want to zoom. The box with the counter appears highlighted and the Zoom window launches. The minimum, maximum, average, and last fields show the values for the counter since the monitoring began for the counter.
  - Click the counter to select the counter to zoom. The box with the counter appears highlighted. Right-click the counter and select **Zoom Chart** or choose **System > Performance > Zoom Chart**. The Zoom window launches. The minimum, maximum, average, and last fields show the values for the counter since the monitoring began for the counter.

Step 2 To zoom out a counter, perform one of the following tasks:

- To zoom out predefined objects, such as System Summary, click the counter and press **Z** in the active counter to return the counter to original size.
- To zoom out counters in the Performance pane, click **OK** to close the Zoom window.

Highlight Feature

The highlight feature helps to distinguish hosts and counters when multiple nodes or counters display on color-coded graphs. This feature is active in the System Summary, CPU and Memory, Disk Usage, and Performance Log Viewer windows. See also "Zoom Feature" section on page 3-3.

Procedure

Step 1 To highlight charts and graphs, perform one of the following tasks:

- To highlight charts and graphs for predefined objects, such as System Summary, right-click in a plot area to highlight the nearest data series or point.
- To highlight charts and graphs in the performance log viewer, perform one of the following tasks
  - Right-click on any color code in the table below the chart in the Performance Log Viewer and choose **Highlight** to highlight the data series for that counter.
  - Right-click on any color code in the table below the chart in the Performance Log Viewer and choose **Change Color** to select a different color for the counter.

Step 2 To return a highlighted item to its original appearance in the Performance Log Viewer, select another item to highlight.

Counter Properties

Counter properties allow you to display a description of the counter and configure data-sampling parameters.

The Counter Property window contains the option to configure data samples for a counter. The performance counters that display in the RTMT performance monitoring pane contain green dots that represent samples of data over time. You can configure the number of data samples to collect and the number of data points to show in the chart. After the data sample is configured, view the information by using the View All Data/View Current Data menu option to view all the data that a perfmon counter collected.

Additional Information

See the "Related Topics" section on page 3-9.

Alert Notification for Counters

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

- From the RTMT Perfmon Monitoring pane, choose the system perfmon counter.
- Set up an e-mail or a message popup window for alert notification.
- Determine the threshold for the alert (for example, an alert activates when calls in progress exceed the threshold of over 100 calls or under 50 calls).
- 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).

Understanding Perfmon Logs

You can log perfmon counters locally on the computer and use the performance log viewer in RTMT to display the perfmon CSV log files that you collected or the Realtime Information Server Data Collection (RISDC) perfmon logs.

RTMT allows you to choose different perfmon counters to log locally. You can then view the data from the perfmon CSV log by using the performance log viewer.

See "Viewing Perfmon Log Files" section on page 6-1 for more information.

Understanding Troubleshooting Perfmon Data Logging

The troubleshooting perfmon data logging feature assists Cisco TAC in identifying system problems. When you enable troubleshooting perfmon data logging, you initiate the collection of a set of the applicable Unified CCX and operating system performance statistics on the selected server. The statistics that are collected include comprehensive information that can be used for system diagnosis.

The system automatically enables troubleshooting perfmon data logging to collect statistics from a set of perfmon counters that provides comprehensive information on the system state. When Troubleshooting Perfmon Data Logging is enabled, Cisco estimates that the system experiences a less than 5-percent increase in CPU utilization and an insignificant increase in the amount of memory that is being used, and it writes approximately 50 MB of information to the log files daily.

You can perform the following administrative tasks with the troubleshooting perfmon data logging feature:

- Enable and disable the trace filter for Troubleshooting perfmon data logging.
- Monitor the applicable set of predefined System, Unified CCX performance objects and counters on each server.
- Log the monitored performance data in CSV file format on the server in the active log partition in the var/log/active/cm/log/ris/csv directory. The log file uses the following naming convention: PerfMon_<server>_<month>_<day>_<year>_<hour>_<minute>.csv; for example, PerfMon_172.19.240.80_06_15_2005_11_25.csv. Specify the polling rate. This rate specifies the rate at which performance data gets gathered and logged. You can configure the polling rate down to 5 seconds. Default polling rate equals 15 seconds.
- View the log file in graphical format by using the Microsoft Windows performance tool or by using the Performance Log viewer in the RTMT.
- Specify the maximum number of log files that will be stored on disk. Log files exceeding this limit get purged automatically by removal of the oldest log file. The default specifies 50 files.
- Specify the rollover criteria of the log file based on the maximum size of the file in megabytes. The default value specifies 5 MB.
- Collect the Cisco RIS Data Collector PerfMonLog log file by using the Trace & Log Central feature of the RTMT or Command Line Interface.

For more information on configuring Troubleshooting Perfmon Data Logging, see "Configuring Troubleshooting Perfmon Data Logging" section on page 6-4.

The troubleshooting perfmon data-logging feature collects information from the following counters within the following perfmon objects.

Refer to the System Performance Objects and Counters for a description of the system counters:

- Database Change Notification Server Object
  - Clients
  - QueueDelay
  - QueuedRequestsInDB
  - QueuedRequestsInMemory
- Database Local DSN Object
  - CNDbSpace_Used
  - SharedMemory_Free
  - SharedMemory_Used
- Enterprise Replication DBSpace Monitors Object
  - ERDbSpace_Used
  - ERSBDbSpace_Used
- IP Object
  - In Receives
  - In HdrErrors
  - In UnknownProtos
  - In Discards
  - In Delivers
  - Out Requests
  - Out Discards
  - Reasm Reqds
  - Reasm Oks
  - Reasm Fails
  - Frag OKs
  - Frag Fails
  - Frag Creates
  - InOut Requests
- Memory Object
  - % Page Usage
  - % VM Used
  - % Mem Used
  - Buffers Kbytes
  - Cached Kbytes
  - Free Kbytes
  - Free Swap Kbytes

  - Low Total
  - Low Free
  - Pages
  - Pages Input
  - Pages Output
  - Shared Kbytes
  - Total Kbytes
  - Total Swap Kbytes
  - Total VM Kbytes
  - Used Kbytes
  - Used Swap Kbytes
  - Used VM Kbytes
- Network Interface Object
  - Rx Bytes
  - Rx Packets
  - Rx Errors
  - Rx Dropped
  - Rx Multicast
  - Tx Bytes
  - Tx Packets
  - Tx Errors
  - Tx Dropped
  - Total Bytes
  - Total Packets
  - Tx QueueLen
- Number of Replicates Created and State of Replication Object
  - Replicate_State
- Partition Object
  - %Used
  - Read Bytes Per Sec
  - Total Mbytes
  - Used Mbytes
  - Write Bytes Per Sec
- Process Object
  - PID
  - STime
  - % CPU Time
  - Page Fault Count

  - Process Status
  - VmData
  - VmRSS
  - VmSize
  - Thread Count
- Processor Object
  - Irq Percentage
  - Softirq Percentage
  - IOwait Percentage
  - User Percentage
  - Nice Percentage
  - System Percentage
  - Idle Percentage
  - %CPU Time
- System Object
  - Allocated FDs
  - Freed FDs
  - Being Used FDs
  - Max FDs
  - Total Processes
  - Total Threads
  - Total CPU Time
- TCP Object
  - Active Opens
  - Passive Opens
  - Attempt Fails
  - Estab Resets
  - Curr Estab
  - In Segs
  - Out Segs
  - Retrans Segs
  - InOut Segs
- Thread Object—This object is currently not supported on Unifed CCX.
  - %CPU Time

Refer to the Performance Objects and Counters for Unified CCX for a description of the Unified CCX counters.

Where to Find More Information

Related Topics

- Using RTMT for Performance Monitoring, page 3-1
- Configuring Troubleshooting Perfmon Data Logging, page 6-4
- Viewing Alerts, page 7-2
- Working with Performance Queries, page 5-1
- System Performance Objects and Counters, page A-1
- Performance Objects and Counters for Unified CCX, page B-1

CHAPTER 4

Monitoring Predefined System Objects

RTMT provides a set of default monitoring objects that assist you in monitoring the health of the system. Default objects include performance counters or critical event status for the system and other supported services.

The system logs data every 5 minutes for predefined system counters.

This chapter contains information on the following topics:

Predefined System Objects Overview

RTMT displays information on predefined system objects in the monitoring pane.

Tip The polling rate in each precanned monitoring window remains fixed, and the default value specifies 30 seconds. If the collecting rate for the AMC (Alert Manager and Collector) service parameter changes, the polling rate in the precanned window also updates. In addition, the local time of the RTMT client application and not the backend server time, provides the basis for the time stamp in each chart.

For more information on service parameters, refer to *Cisco Unified Contact Center Express Serviceability Administration Guide*.

Table 4-1 provides information on the predefined objects that RTMT monitors.

Tip To zoom in on the monitor of a predefined object, click and drag the left mouse button over the area of the chart in which you are interested. Release the left mouse button when you have the selected area. RTMT updates the monitored view. To zoom out and reset the monitor to the initial default view, press the "**R**" key.

Table 4-1 System Categories

Category	Description
System Summary	Displays information on Virtual Memory usage, CPU usage, Common Partition Usage, and the alert history log. To display information on predefined system objects, choose **System > System Summary.**
Server	• CPU and Memory—Displays information on CPU usage and Virtual memory usage for the server. To display information on CPU and Virtual memory usage, choose **System > Server > CPU and Memory**.To monitor CPU and memory usage for specific server, choose the server from the host drop-down list box. • Process—Displays information on the processes that are running on the server. To display information on processes running on the system, choose **System > Server > Process**. To monitor process usage for specific server, choose the server from the Host drop-down list box. • Disk Usage—Displays information on disk usage on the server. To display information on disk usage on the system, choose **System > Server > Disk Usage**. To monitor disk usage for specific server, choose the server from the host drop-down list box. • Critical Services—Displays the name of the critical service, the status (whether the service is up, down, activated, stopped by the administrator, starting, stopping, or in an unknown state), and the elapsed time during which the services have existed in a particular state for the server or for a particular server in a cluster (if applicable). To display information on critical services, choose **System > Server > Critical Services**, then click the applicable tab: – To display system critical services, click the System tab. – To display Unified CCX critical services, click the Unified CCX tab. – To monitor critical services for specific server on the tab, choose the server from the host drop-down list box and click the critical services tab in which you are interested. If the critical service status indicates that the administrator stopped the service, the administrator performed a task that intentionally stopped the service; for example, the service stopped because the administrator backed up or restored Unified CCX, performed an upgrade, stopped the service in Unified CCX Serviceability or the Command Line Interface (CLI), and so on. If the critical service status displays as unknown state, the system cannot determine the state of the service. **Note** RTMT will not support showing the partial running status of a service in the initial release of Unified CCX 8.0(1). This means that a service will show as up (running) under “Critical Services” even if some of its subsystems are down. The partial status of the Unified CCX services will only be viewable from the Unified CCX Serviceability Administration interface. For more information on the critical service status, refer to Monitoring Server Status, page 4-3.

Additional Information

See the "Related Topics" section on page 4-5.

Viewing the System Summary

The system summary in RTMT allows you to monitor important common information in a single monitoring pane. In system summary, you can view information on the following predefined object:

- Virtual Memory usage
- CPU usage
- Common Partition Usage
- Alert History Log

For more information about the data these monitors provide, see "Monitoring Server Status" section on page 4-3.

For more information about the Alert History Log, see Understanding Alerts, page 7-1.

Additional Information

See the "Related Topics" section on page 4-5.

Monitoring Server Status

The Servers category monitors CPU and memory usage, processes, disk space usage, and critical services for the different applications on the server.

The CPU and Memory monitor provide information about the CPU usage and Virtual memory usage on each server. For each CPU on a server, the information includes the percentage of time that each processor spends executing processes in different modes and operations (User, Nice, System, Idle, IRQ, SoftIRQ, and IOWait). The percentage of CPU equals the total time that is spent executing in all the different modes and operations excluding the Idle time. For memory, the information includes the Total, Used, Free, Shared, Buffers, Cached, Total Swap, Used Swap, and Free Swap memory in Kbytes, and the percentage of Virtual Memory in Use.

The Processes monitor provides information about the processes that are running on the system. RTMT displays the following information for each process—process ID (PID), CPU percentage, Status, Shared Memory (KB), Nice (level), VmRSS (KB), VmSize (KB), VmData (KB), Thread Count, Page Fault Count, and Data Stack Size (KB).

The disk usage monitoring category charts the percentage of disk usage for the common and swap partitions. It also displays the percentage of disk usage for each partition (Active, Boot, Common, Inactive, Swap, SharedMemory, Spare) in each host.

Note If more than one logical disk drive is available in your system, RTMT can monitor the disk usage for the 'spare' partition in the Disk Usage window.

The Critical Services monitoring category provides the name of the critical service, the status (whether the service is up, down, activated, stopped by the administrator, starting, stopping, or in an unknown state), and the elapsed time during which the services are up and running on the system.

For a specific description of each state, see Table 4-2.

Table 4-2 Status of Critical Services

Status of Critical Service	Description
starting	The service currently exists in start mode, as indicated in the Critical Services pane and in Control Center in Unified CCX Serviceability
up	The service currently runs, as indicated in the Critical Services pane and in Control Center in Unified CCX Serviceability.
stopping	The service currently remains stopped, as indicated in the Critical Services pane and in Control Center in Unified CCX Serviceability.
down	The service stopped running unexpectedly; that is, you did not perform a task that stopped the service. The Critical Services pane indicates that the service is down. The CriticalServiceDown alert gets generated when the service status equals down.
stopped by Admin	You performed a task that intentionally stopped the service; for example, the service stopped because you backed up or restored Unified CCX, performed an upgrade, stopped the service in Unified CCX Serviceability or the Command Line Interface (CLI), and so on. The Critical Services pane indicates the status.
not activated	The service does not exist in a currently activated status, as indicated in the Critical Services pane and in Service Activation in Unified CCX Serviceability.
unknown state	The system cannot determine the state of the service, as indicated in the Critical Services pane.

Additional Information

See the "Related Topics" section on page 4-5.

Understanding Server Logs

Every 5 minutes, the server data gets logged into the file as a single record. The system logs the data every 5 minutes for the following counters, based on the following calculation:

- cpuUsage—Average of all the values that were collected in the last 5 minutes
- MemoryInUse—Average of all the values that were collected in the last 5 minutes
- DiskSpaceInUse—Average of all the values that were collected in the last 5 minutes for the active partition

The Cisco AMC service logs the server data in csv format. The header of the log comprises the time zone information and a set of columns with the previous counters for a server. These sets of columns repeat for every server in a cluster, if applicable.

The following file name format of the server log applies: ServerLog_MM_DD_YYYY_hh_mm.csv. The first line of each log file comprises the header.

To download the server logs for viewing on your local computer, refer to Working with Trace and Log Central, page 9-1.

Additional Information

See the "Where to Find More Information" section on page 4-5.

Where to Find More Information

Related Topics

- Predefined System Objects Overview, page 4-1
- Viewing the System Summary, page 4-3
- Monitoring Server Status, page 4-3
- Understanding Server Logs, page 4-4

CHAPTER 5

Working with Performance Queries

To troubleshoot system performance problems, you add a counter (query) that is associated with the perfmon object to the Performance monitor, which displays a chart for the counter.

This chapter contains information on the following topics:

Working with Categories

Categories allow you to organize objects in RTMT, such as performance monitoring counters and devices. For example, the default category under performance monitoring, RTMT allows you to monitor six performance monitoring counters in graph format. If you want to monitor more counters, you can configure a new category and display the data in table format.

If you perform various searches, you can create a category for each search and save the results in the category.

Adding a Category

To add a category, perform the following procedure:

Procedure

Step 1 Choose **System** > **Performance** > **Open Performance Monitoring**.

Step 2 Choose **Edit > Add New Category**.

Step 3 Enter the name of the category; click **OK**.

The category tab displays at the bottom of the window.

Additional Information

See the "Where to Find More Information" section on page 5-11.

Renaming a Category

To rename a category, perform the following procedure:

Procedure

Step 1 Perform one of the following tasks:

- Right-click the category tab that you want to rename and choose **Rename Category**.
- Click the category tab that you want to rename and choose **Edit > Rename Category**.

Step 2 Enter the new name and click **OK**.

The renamed category displays at the bottom of the window.

Additional Information

See the "Where to Find More Information" section on page 5-11.

Deleting a Category

To delete a category, perform one of the following tasks:

- Right-click the category tab that you want to delete and choose **Remove Category**.
- Click the category tab that you want to delete and choose **Edit > Remove Category**.

Additional Information

See the "Where to Find More Information" section on page 5-11.

Using Performance Queries to Add a Counter

You can use queries to select and display perfmon counters. You can organize the perfmon counters to display a set of feature-based counters and save it in a category. See "Working with Categories" section on page 5-1 for more information. After you save your RTMT profile, you can quickly access the counters in which you are interested.

RTMT displays perfmon counters in chart or table format. The chart format displays the perfmon counter information by using line charts. For each category tab that you create, you can display up to six charts in the RTMT Perfmon Monitoring pane with up to three counters in one chart. After you create a category, you cannot change the display from a chart format to a table format, or vice versa.

Tip You can display up to three counters in one chart in the RTMT Perfmon Monitoring pane. To add another counter in a chart, click the counter and drag it to the RTMT Perfmon Monitoring pane. Repeat again to add up to three counters.

By default, RTMT displays perfmon counters in a chart format. You can also choose to display the perfmon counters in a table format. To display the perfmon counters in table format, you need to check the **Present Data in Table View** check box when you create a new category.

Before you add counters, see the "Category Tabs" section on page 3-2. To zoom a counter, see "Zoom Feature" section on page 3-3.

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel
  - Click **System**.
  - In the tree hierarchy, double-click **Performance**.
  - Click the **Performance** icon.
- Choose **System > Performance > Open Performance Monitoring**.

Step 2 Click the name of the server where you want to add a counter to monitor.

The tree hierarchy expands and displays all the perfmon objects.

Step 3 To monitor a counter in table format, continue to Step 4. To monitor a counter in chart format, skip to Step 9.

Step 4 Choose **Edit > New Category**.

Step 5 In the Enter Name field, enter a name for the tab.

Step 6 To display the perfmon counters in table format, check the **Present Data in Table View** check box.

Step 7 Click **OK**.

A new tab with the name that you entered displays at the bottom of the pane.

Step 8 Perform one of the following tasks to select one or more counters with one or more instances for monitoring in table format (skip the remaining step in this procedure):

- Double click a single counter and select a single instance from the pop-up window; then, click **Add**.
- Double click a single counter and select multiple instances from the pop-up window; then, click **Add**.

- Drag a single counter to the monitoring window and select a single instance from the pop-up window; then click **Add**.
- Drag a single counter to the monitoring window and select multiple instances from the pop-up window; then, click **Add**.
- Select multiple counters and drag them onto the monitoring window. Select a single instance from the pop-up window; then, click **Add**.
- Select multiple counters and drag them onto the monitoring window. Select multiple instances from the pop-up window; then, click **Add**.

Tip To display the counter in chart format after you display it in table format, right-click the category tab and choose **Remove Category**. The counter displays in chart format.

Step 9 To monitor a counter in chart format, perform the following tasks:

- Click the file icon next to the object name that lists the counters that you want to monitor.

  A list of counters displays.
- To display the counter information, either right-click the counter and click **Counter Monitoring**, double-click the counter, or drag and drop the counter into the RTMT Perfmon Monitoring pane.

The counter chart displays in the RTMT Perfmon Monitoring pane.

Additional Information

See the Related Topics, page 5-11.

Removing a Counter from the Performance Monitoring Pane

You can remove a counter chart (table entry) with the Remove Chart/TableEntry menu item in the Perfmon menu in the menu bar.

You can remove counters from the RTMT Perfmon Monitoring pane when you no longer need them. This section describes how to remove a counter from the pane.

Perform one of the following tasks:

- Right-click the counter that you want to remove and choose **Remove**.
- Click the counter that you want to remove and choose **Perfmon > Remove Chart/Table Entry**.

The counter no longer displays in the RTMT Perfmon Monitoring pane.

Additional Information

See the Related Topics, page 5-11.

Adding a Counter Instance

To add a counter instance, perform the following procedure:

Procedure

Step 1 Display the performance monitoring counter, as described in the "Using RTMT for Performance Monitoring" section on page 3-1.

Step 2 Perform one of the following tasks:

- Double-click the performance monitoring counter in the performance monitoring tree hierarchy.
- Click the performance monitoring counter in the performance monitoring tree hierarchy and choose **System > Performance > Counter Instances**.
- Right-click the performance monitoring counter in the performance monitoring tree hierarchy and choose **Counter Instances**.

Step 3 In the Select Instance window, click the instance; then, click **Add**.

The counter displays.

Additional Information

See the Related Topics, page 5-11.

Configuring Alert Notification for a Counter

The following procedure describes how to configure alert notification for a counter.

Tip To remove the alert for the counter, right-click the counter and choose Remove Alert. The option appears gray after you remove the alert.

Procedure

Step 1 Display the performance counter, as described in the "Using RTMT for Performance Monitoring" section on page 3-1.

Step 2 From the counter chart or table, right-click the counter for which you want to configure the alert notification, and choose **Set Alert/Properties**.

Step 3 Check the **Enable Alert** check box.

Step 4 In the Severity drop-down list box, choose the severity level at which you want to be notified.

Step 5 In the Description pane, enter a description of the alert.

Step 6 Click **Next**.

Step 7 Use Table 5-1 to configure the settings in the Threshold, Value Calculated As, Duration, Frequency, and Schedule panes. After you enter the settings in the window, click **Next** to proceed to the next panes.

Table 5-1 Counter Alert Configuration Parameters

Setting	Description
Threshold Pane	
Trigger alert when following conditions met (Over, Under)	Check the check box and enter the value that applies. • Over—Check this check box 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 this check box 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—Choose Absolute to display the data at its current status. These counter values are cumulative. • Delta—Choose Delta to display the difference between the current counter value and the previous counter value. • Delta Percentage—Choose 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.

Table 5-1 Counter Alert Configuration Parameters (continued)

Setting	Description
Frequency Pane	
Trigger alert on every poll; trigger up to...	Click 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. For example, if the calls in progress continue to go over or under the threshold, the system does not send another alert notification. When the threshold is normal (between 50 and 100 calls in progress), the system deactivates the alert notification; however, if the threshold goes over or under the threshold value again, the system reactivates alert notification. • 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.
Schedule Pane	
24-hours daily; start/stop	Click 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 the check box is 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.

Step 8 If you want the system to send an e-mail message for the alert, check the **Enable Email** check box.

Step 9 If you want to trigger an alert action that is already configured, choose the alert action that you want from the Trigger Alert Action drop-down list box.

Step 10 If you want to configure a new alert action for the alert, click **Configure**.

Note Whenever the specified alert is triggered, the system sends the alert action.

The Alert Action dialog box displays.

Step 11 To add a new alert action, click **Add**.

The Action Configuration dialog box displays.

Step 12 In the Name field, enter a name for the alert action.

Step 13 In the Description field, enter a description for the alert action.

Step 14 To add a new e-mail recipient for the alert action, click **Add**.

The Input dialog box displays.

Step 15 Enter either the e-mail or e-page address of the recipient that you want to receive the alert action notification.

Step 16 Click **OK**.

The recipient address displays in the Recipient list. The Enable check box gets checked.

Tip To disable the recipient address, uncheck the Enable check box. To delete a recipient address from the Recipient list, highlight the address and click **Delete**.

Step 17 Click **OK**.

Step 18 The alert action that you added displays in Action List.

Tip To delete an alert action from the action list, highlight the alert action and click **Delete**. You can also edit an existing alert action by clicking **Edit**.

Step 19 Click **Close**.

Step 20 In the User-defined email text box, enter the text that you want to display in the e-mail message.

Step 21 Click **Activate**.

Additional Information

See the Related Topics, page 5-11.

Displaying a Counter Description

Use one of two methods to obtain a description of the counter:

Procedure

Step 1 Perform one of the following tasks:

- In the Perfmon tree hierarchy, right-click the counter for which you want property information and choose **Counter Description**.
- In the RTMT Performance Monitoring pane, click the counter and choose **System > Performance > Counter Description** from the menu bar.

Tip To display the counter description and to configure data-sampling parameters, see the "Configuring a Data Sample" section on page 5-9.

The Counter Property window displays the description of the counter. The description includes the host address, the object to which the counter belongs, the counter name, and a brief overview of what the counter does.

Step 2 To close the Counter Property window, click **OK**.

Additional Information

See the Related Topics, page 5-11.

Configuring a Data Sample

The Counter Property window contains the option to configure data samples for a counter. The perfmon counters that display in the RTMT Perfmon Monitoring pane contain green dots that represent samples of data over time. You can configure the number of data samples to collect and the number of data points to show in the chart. After the data sample is configured, view the information by using the View All Data/View Current Data menu option. See the "Viewing Counter Data" section on page 5-10.

This section describes how to configure the number of data samples to collect for a counter.

Procedure

Step 1 Display the counter, as described in the "Using RTMT for Performance Monitoring" section on page 3-1.

Step 2 Perform one of the following tasks:

- Right-click the counter for which you want data sample information and choose **Monitoring Properties** if you are using chart format and **Properties** if you are using table format.
- Click the counter for which you want data sample information and choose **System > Performance > Monitoring Properties**.

The Counter Property window displays the description of the counter, as well as the tab for configuring data samples. The description includes the host address, the object to which the counter belongs, the counter name, and a brief overview of what the counter does.

Step 3 To configure the number of data samples for the counter, click the **Data Sample** tab.

Step 4 From the No. of data samples drop-down list box, choose the number of samples (between 100 and 1000). The default specifies 100.

Step 5 From the No. of data points shown on chart drop-down list box, choose the number of data points to display on the chart (between 10 and 50). The default specifies 20.

Step 6 Click one parameter, as described in Table 5-2.

Table 5-2 Data Sample Parameters

Parameter	Description
Absolute	Because some counter values are accumulative, choose Absolute to display the data at its current status.
Delta	Choose Delta to display the difference between the current counter value and the previous counter value.
Delta Percentage	Choose Delta Percentage to display the counter performance changes in percentage.

Step 7 To close the Counter Property window and return to the RTMT Perfmon Monitoring pane, click the **OK** button.

Additional Information

See the Related Topics, page 5-11.

Viewing Counter Data

Perform the following procedure to view the data that is collected for a performance counter.

Procedure

Step 1 In the RTMT Perfmon Monitoring pane, right-click the counter chart for the counter for which you want to view data samples and choose **View All Data**.

The counter chart displays all data that has been sampled. The green dots display close together, almost forming a solid line.

Step 2 Right-click the counter that currently displays and choose **View Current**.

The counter chart displays the last configured data samples that were collected. See the "Configuring a Data Sample" section on page 5-9 procedure for configuring data samples.

Additional Information

See the Related Topics, page 5-11.

Local Logging of Perfmon Counters Data

RTMT allows you to choose different perfmon counters to log locally. You can then view the data from the perfmon CSV log by using the performance log viewer. See "Viewing Perfmon Log Files" section on page 6-1.

Starting the Counter Logs

To start logging perfmon counter data into a CSV log file, perform the following procedure:

Procedure

Step 1 Display the performance monitoring counters, as described in the "Using RTMT for Performance Monitoring" section on page 3-1.

Step 2 If you are displaying perfmon counters in the chart format, right-click the graph for which you want data sample information and choose **Start Counter(s) Logging**. If you want to log all counters in a screen (both chart and table view format), you can right-click the category name tab at the bottom of the window and choose **Start Counter(s) Logging**.

The Counter Logging Configuration dialog box displays.

Step 3 In the Logger File Name field, enter a file name and click **OK**.

RTMT saves the CSV log files in the log folder in the .jrtmt directory under the user home directory. For example, in Windows, the path specifies D:\Documents and Settings\userA\.jrtmt\log, or in Linux, the path specifies /users/home/.jrtmt/log.

To limit the number and size of the files, configure the maximum file size and maximum number of files parameter in the trace output setting for the specific service in the Trace Configuration window of Cisco Unified Serviceability. See *Cisco Unified Serviceability Administration Guide* available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Stopping the Counter Logs

To stop logging perfmon counter data, perform the following procedure:

Procedure

Step 1 Display the performance monitoring counters, as described in the "Using RTMT for Performance Monitoring" section on page 3-1.

Step 2 If you are displaying perfmon counters in the chart format, right-click the graph for which counter logging is started and choose **Stop Counter(s) Logging.** If you want to stop logging of all counters in a screen (both chart and table view format), you can right-click the category name tab at the bottom of the window and choose **Stop Counter(s) Logging**.

Additional Information

See the Related Topics, page 5-11.

Where to Find More Information

Related Topics

- Working with Categories, page 5-1
- Using Performance Queries to Add a Counter, page 5-3
- Removing a Counter from the Performance Monitoring Pane, page 5-4
- Adding a Counter Instance, page 5-4
- Configuring Alert Notification for a Counter, page 5-5
- Displaying a Counter Description, page 5-8
- Configuring a Data Sample, page 5-9
- Viewing Counter Data, page 5-10
- Local Logging of Perfmon Counters Data, page 5-10
- Viewing Perfmon Log Files, page 6-1

- Understanding Performance Monitoring, page 3-1
- System Performance Objects and Counters, page A-1
- Performance Objects and Counters for Unified CCX, page B-1

CHAPTER 6

Viewing and Troubleshooting Perfmon Logs

To view perfmon logs, you can download the logs or view them locally.

This chapter contains information on the following topics:

Viewing Perfmon Log Files

You can view data from the perfmon CSV log by using the Performance Log Viewer in RTMT or by using the Microsoft Performance tool.

Viewing Log Files on the Performance Log Viewer

The Performance Log Viewer displays data for counters from perfmon CSV log files in a graphical format. You can use the performance log viewer to display data from the local perfmon logs that you collected, or you can display the data from the Realtime Information Server Data Collection (RISDC) perfmon logs.

The local perfmon logs comprise data from counters that you choose and store locally on your computer. For more information on how to choose the counters and how to start and stop local logging, see "Local Logging of Perfmon Counters Data" section on page 5-10.

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel
  - Click **System.**
  - In the tree hierarchy, double-click **Performance**.
  - Click the **Performance Log Viewer** icon.
- Choose **System > Performance > Open Performance Log Viewer**.

Step 2 Choose the type of perfmon logs that you want to view:

- For RISDC Perfmon Logs, perform the following steps:
  - **a.** Click on RISDC Perfmon Logs and choose a server from the Select a node drop-down box.
  - **b.** Click **Open**.

    The File Selection Dialog Box displays.
  - **c.** Choose the file and click **Open File**.

    The Select Counters Dialog Box displays.
  - **d.** Choose the counters that you want to display by checking the check box next to the counter.
  - **e.** Click **OK**.
- For locally stored data, perform the following steps:
  - **a.** Click Local Perfmon Logs.
  - **b.** Click **Open**.

    The File Selection Dialog Box displays. RTMT saves the perfmon CSV log files in the log folder in the .jrtmt directory under the user home directory. In Windows, the path specifies D:\Documents and Settings\userA\.jrtmt\log, or in Linux, the path specifies /users/home/.jrtmt/log.
  - **c.** Browse to the file directory.
  - **d.** Choose the file that you are interested in viewing or enter the file name in the filename field.
  - **e.** Click **Open**.

    The Select Counters Dialog Box displays.
  - **f.** Choose the counters that you want to display by checking the check box next to the counter.
  - **g.** Click **OK**.

The performance log viewer displays a chart with the data from the selected counters. The bottom pane displays the selected counters, a color legend for those counters, display option, mean value, minimum value, and the maximum value.

Table 6-1 describes the functions of different buttons that are available on the performance log viewer.

Table 6-1 Performance Log Viewer

Button	Function
Select Counters	Allows you to add counters that you want to display in the performance log viewer. To not display a counter, uncheck the Display column next to the counter.
Reset View	Resets the performance log viewer to the initial default view.
Save Downloaded File	Allows you to save the log file to your local computer.

Tip You can order each column by clicking on a column heading. The first time that you click on a column heading, the records display in ascending order. A small triangle pointing up indicates ascending order. If you click the column heading again, the records display in descending order. A small triangle pointing down indicates descending order. If you click the column heading one more time, the records displays in the unsorted state.

Additional Information

See the Related Topics, page 6-5.

Zooming In and Out

The performance Log viewer includes a zoom feature that allows you to zoom in on an area in the chart. To zoom in, click and drag the left button of the mouse until you have the selected desired area.

To reset the chart to the initial default view, click **Reset View** or right-mouse click the chart and choose **Reset**.

Additional Information

See the Related Topics, page 6-5.

Viewing the Perfmon Log Files with the Microsoft Performance Tool

To view the log files by using the Microsoft Performance tool, follow these steps:

Procedure

Step 1 Choose **Start > Settings > Control Panel > Administrative Tools > Performance**.

Step 2 In the application window, click the right mouse button and choose **Properties**.

Step 3 Click the Source tab in the System Monitor Properties dialog box.

Step 4 Browse to the directory where you downloaded the perfmon log file and choose the perfmon csv file. The log file includes the following naming convention: PerfMon_<server>_<month>_<day>_<year>_<hour>_<minute>.csv; for example, PerfMon_172.19.240.80_06_15_2005_11_25.csv.

Step 5 Click **Apply.**

Step 6 Click the **Time Range** button. To specify the time range in the perfmon log file that you want to view, drag the bar to the appropriate starting and ending times.

Step 7 To open the Add Counters dialog box, click the Data tab and click **Add**.

Step 8 From the Performance Object drop-down box, choose the perfmon object. If an object has multiple instances, you may choose **All instances** or select only the instances that you are interested in viewing.

Step 9 You can choose **All Counters** or select only the counters that you are interested in viewing.

Step 10 To add the selected counters, click **Add**.

Step 11 When you finish selecting counters, click **Close**.

Additional Information

See the Related Topics, page 6-5.

Working with Troubleshooting Perfmon Data Logging

When you enable RISDC perfmon logs, information gets collected for the system in logs that are written on the server. You can enable or disable RISDC perfmon logs from the Service Parameter window of the Unified CCX Serviceability interface by choosing **Tools > Service Parameters**.

By default, RISDC perfmon logging remains enabled. Be aware that RISDC perfmon logging is also known as Troubleshooting Perfmon Data logging. When you enable RISDC perfmon logging, the server collects performance data that are used to troubleshoot problems.

You can collect the log files for Cisco RIS Data Collector service on the server by using RTMT to download the log files. If you want to download the log files by using the CLI, refer to *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*. After you collect the log files, you can view the log file by using the Performance Log Viewer in RTMT or by using the Microsoft Windows performance tool. See "Viewing Log Files on the Performance Log Viewer" section on page 6-1 or "Viewing the Perfmon Log Files with the Microsoft Performance Tool" section on page 6-3.

Configuring Troubleshooting Perfmon Data Logging

The following procedure describes how to configure the troubleshooting perfmon data logging feature.

Procedure

Step 1 Go to the Service Parameters window of the Unified CCX Serviceability interface for your configuration by choosing **Tools > Service Parameters**.

Step 2 From the Server drop-down list box, choose the server.

Step 3 From the Service drop-down list box, choose Cisco RIS Data Collector.

Step 4 Enter the appropriate settings as described in Table 6-2.

Step 5 Click **Save**.

Troubleshooting Perfmon Data-Logging Configuration Settings

Table 6-2 describes the available settings to enable and disable troubleshooting perfmon data logging.

Table 6-2 Troubleshooting Perfmon Data-Logging Parameters

Field	Description
Enable Logging	From the drop-down box, choose **True** to enable or **False** to disable troubleshooting perfmon data logging. The default value specifies True.
Polling Rate	Enter the polling rate interval (in seconds). You can enter a value from 5 (minimum) to 300 (maximum). The default value specifies 15.
Maximum No. of Files	Enter the maximum number of Troubleshooting Perfmon Data Logging files that you want to store on disk. You can enter a value from 1 (minimum) up to 100 (maximum). The default value specifies 50. Consider your storage capacity in configuring the Maximum No. of Files and Maximum File Size Parameters. Cisco recommends that you do not exceed a value of 100 MB when you multiply the Maximum Number of Files value by the Maximum File Size value. When the number of files exceeds the maximum number of files that you specified in this field, the system will delete log files with the oldest timestamp. **Caution** If you do not save the log files on another machine before you change this parameter, you risk losing the log files.
Maximum File Size	Enter the maximum file size (in megabytes) that you want to store in a perfmon log file before a new file is started. You can enter a value from 1 (minimum) to 500 (maximum). The default value specifies 5 MB. Consider your storage capacity in configuring the Maximum No. of Files and Maximum File Size Parameters. Cisco recommends that you do not exceed a value of 100 MB when you multiply the Maximum Number of Files value by the Maximum File Size value.

Where to Find More Information

Related Topics

- Using RTMT for Performance Monitoring, page 3-1
- Working with Troubleshooting Perfmon Data Logging, page 6-4
- Working with Performance Queries, page 5-1
- System Performance Objects and Counters, page A-1
- Performance Objects and Counters for Unified CCX, page B-1

PART 3

Alerts

CHAPTER 7

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.
- 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 7-8.

Viewing Alerts

RTMT displays both preconfigured alerts and custom alerts in Alert Central. RTMT organizes the alerts under the applicable tabs—System, Unified CCX, and Custom.

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

- System Alerts, page 7-2
- Unified CCX Alerts, page 7-3

System Alerts

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

The following list comprises the preconfigured system alerts.

- AuthenticationFailed
- CiscoDRFFailure
- CoreDumpFileFound
- CpuPegging
- CriticalServiceDown
- HardwareFailure

- LogFileSearchStringFound
- LogPartitionHighWaterMarkExceeded
- LogPartitionLowWaterMarkExceeded
- LowActivePartitionAvailableDiskSpace
- LowAvailableVirtualMemory
- LowInactivePartitionAvailableDiskSpace
- LowSwapPartitionAvailableDiskSpace
- ServerDown
- SparePartitionHighWaterMarkExceeded
- SparePartitionLowWaterMarkExceeded
- SyslogSeverityMatchFound
- SyslogStringMatchFound
- SystemVersionMismatched
- TotalProcessesAndThreadsExceededThreshold

Unified CCX Alerts

The following list comprises the preconfigured Unified CCX alerts.

Note For alert descriptions and default configurations, see "Cisco Unified Contact Center Express Alert Descriptions and Default Configurations" section on page D-1.

- DB CRA % Space Used
- DBReplicationStopped
- HistoricalDataWrittenToFiles
- PurgeInvoked
- UnifiedCCXEngineMemoryUsageHigh

Additional Information

See the Related Topics, page 7-8.

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 7-1 provides a list of fields that you may use to configure each alert; users can configure preconfigured fields, unless otherwise noted.

Table 7-1 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 7-2.
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 7-2.
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).	This field is applicable only for event based alerts.
Node IDs	Cluster or list of servers to monitor	
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 7-5). 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	Displays the detail of an alert (not configurable)	

Table 7-1 Alert Customization (continued)

Field	Description	Comment
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 7-8.

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 7-2 provides a list of fields that you will use to configure alert actions. Users can configure all fields, unless otherwise marked.

Table 7-2 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 7-8.

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.

- 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 7-8.

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 7-8.

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 8-3.

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 (Unified CCX), 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 7-1
- Viewing Alerts, page 7-2
- Alert Fields, page 7-3
- Alert Action Configuration, page 7-5
- Enabling Trace Download, page 7-5
- Understanding Alert Logs, page 7-6
- Working with Alerts, page 8-1
- Setting Alert Properties, page 8-3
- Suspending Alerts, page 8-5
- Configuring E-mails for Alert Notification, page 8-6
- Configuring Alert Actions, page 8-6

CHAPTER 8

Working with Alerts

This chapter contains information on the following topics:

Working with Alerts

By using the following procedure, you can perform tasks, such as access Alert Central, sort alert information, enable, disable, or remove an alert, clear an alert, or view alert details.

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel
  - Click **System**.
  - In the tree hierarchy, double-click **Tools**.
  - Click the Alert Central icon.
- Choose **System > Tools > Alert > Alert Central**.

The Alert Central monitoring window displays and shows the alert status and alert history of the alerts that the system has generated.

Step 2 Perform one of the following tasks:

- To set alert properties, see the "Setting Alert Properties" section on page 8-3.
- To suspend alerts, see the "Suspending Alerts" section on page 8-5.
- To configure e-mails for alert notification, see the "Configuring E-mails for Alert Notification" section on page 8-6.
- To configure alert actions, see the "Configuring Alert Actions" section on page 8-6.

- To sort alert information in the Alert Status pane, click the up/down arrow that displays in the column heading. For example, click the up/down arrow that displays in the Enabled or In Safe Range column.

  You can sort alert history information by clicking the up/down arrow in the columns in the Alert History pane. To see alert history that is out of view in the pane, use the scroll bar on the right side of the Alert History pane.
- To enable, disable, or remove an alert, perform one of the following tasks:
  - From the Alert Status window, right-click the alert and choose **Disable/Enable Alert** (option toggles) or **Remove Alert**, depending on what you want to accomplish.
  - Highlight the alert in the Alert Status window and choose **System > Tools > Alert > Disable/Enable** (or **Remove**) **Alert**.

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

- To clear either individual or collective alerts after they get resolved, perform one of the following tasks:
  - After the Alert Status window displays, right-click the alert and choose **Clear Alert** (or **Clear All Alerts**).
  - Highlight the alert in the Alert Status window and choose **System > Tools > Alert > Clear Alert** (or **Clear All Alerts)**.

  After you clear an alert, it changes from red to black.
- To reset alerts to default configuration, perform one of the following tasks:
  - After the Alert Status window displays, right-click the alert and choose **Reset Alert to Default Config,** to reset that alert to the default configuration.
  - Choose **System > Tools > Alert > Reset all Alerts to Default Config,** to reset all the alerts to the default configuration.
- To view alert details, perform one of the following tasks:
  - After the Alert Status window displays, right-click the alert and choose **Alert Details**.
  - Highlight the alert in the Alert Status window and choose **System > Tools > Alert > Alert Details**.

Tip After you have finished viewing the alert details, click **OK**.

Additional Information

See the "Related Topics" section on page 8-8.

Setting Alert Properties

The following procedure describes how to set alert properties.

Procedure

Step 1 Display Alert Central, as described in the "Working with Alerts" section on page 8-1.

Step 2 From the Alert Status window, click the alert for which you want to set alert properties.

Step 3 Perform one of the following tasks:

- Right-click the alert and choose **Set Alert/Properties**.
- Choose **System > Tools > Alert > Set Alert/Properties**.

Step 4 To enable the alert, check the **Enable Alert** check box.

Step 5 From the Severity drop-down list box, choose the severity of the alert.

Step 6 From the Enable/Disable this alert on following server(s) pane, check the Enable check box of the servers on which you want this alert to be enabled.

For preconfigured alerts, the Description information pane displays a description of the alert.

Step 7 Click **Next**.

Step 8 In the Threshold pane, enter the conditions in which the system triggers the alert.

Step 9 In the Duration pane, click one of the following radio buttons:

- Trigger alert only when below or over.... radio button—If you want the alert to be triggered only when the value is constantly below or over the threshold for a specific number of seconds; then, enter the seconds.
- Trigger alert immediately—If you want the system to trigger an alert immediately.

Step 10 Click **Next**.

Step 11 In the Frequency pane, click one of the following radio buttons:

- Trigger alert on every poll—If you want the alert to be triggered on every poll.
- Trigger up to <numbers> of alerts within <number> of minutes—If you want a specific number of alerts to be triggered within a specific number of minutes. Enter the number of alerts and number of minutes.

Step 12 In the Schedule pane, click one of the following radio buttons:

- 24-hours daily—If you want the alert to be triggered 24 hours a day.
- Start time/Stop time—If you want the alert to be triggered within a specific start and stop time. Enter the start and stop times.

Step 13 Click **Next**.

Step 14 If you want to enable e-mail for this alert, check the Enable Email check box.

Step 15 To trigger an alert action with this alert, choose the alert action that you want to send from the drop-down list box.

Step 16 To configure a new alert action, or edit an existing one, click **Configure**.

Step 17 To add a new alert action, continue to Step 18. To edit an existing alert action, skip to Step 25.

Step 18 Click **Add**.

Step 19 In the Name field, enter a name for the alert action.

Step 20 In the Description field, enter a description of the alert action.

Step 21 To add an e-mail recipient, click **Add**.

Step 22 In the Enter email/epage address field, enter an e-mail or e-page address of the recipient that you want to receive the alert action.

Step 23 Click **OK**.

The Action Configuration window shows the recipient(s) that you added, and the Enable check box appears checked.

Tip To delete an e-mail recipient, highlight the recipient and click **Delete**. The recipient that you chose disappears from the recipient list.

Step 24 When you finish adding all the recipients, click **OK**. Skip to Step 27.

Step 25 To edit an existing alert action, highlight the alert action and click **Edit**.

The Action Configuration window of the alert action that you chose displays.

Step 26 Update the configuration and click **OK**. Continue to Step 27.

Step 27 After you finish alert action configuration, click **Close**.

For alerts, such as CriticalServiceDown and CodeYellow, that allow trace download, perform the following procedure:

a. Click **Next**.

b. In the Alert Properties: Trace Download window, check the Enable Trace Download check box.

c. The SFTP Parameters Dialog window displays. Enter the IP address, a user name, password, port and download directory path where the trace will be saved. To ensure that you have connectivity with the SFTP server, click **Test Connection**. If the connection test fails, your settings will not get saved.

d. To save your configuration, click **OK**.

e. In the Trace Download Parameters window, enter the number and frequency of downloads. 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.

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.

Note To delete an alert action, highlight the action, click **Delete**, and click **Close**.

Additional Information

See the "Related Topics" section on page 8-8.

Suspending Alerts

You may want to temporarily suspend some or all alerts, on a particular server or on an entire cluster (if applicable). For example, if you are upgrading the Unified CCX to a newer release, you would probably want to suspend all alerts until the upgrade completes, so you do not receive e-mails and/or e-pages during the upgrade. The following procedure describes how to suspend alerts in Alert Central.

Procedure

Step 1 Choose **System > Tools > Alert > Suspend cluster/node Alerts**.

Note Per server suspend states do not apply to Unified CCX.

Step 2 Do one of the following:

To suspend all alerts in the cluster	Choose the Cluster Wide radio button and check the suspend all alerts check box.
To suspend alerts per server	Choose the Per Server radio button and check the Suspend check box of each server on which you want alerts to be suspended.

Step 3 Click **OK**.

Note To resume alerts, choose **Alert > Suspend cluster/node Alerts** again and uncheck the suspend check boxes.

Additional Information

See the "Related Topics" section on page 8-8.

Configuring E-mails for Alert Notification

Perform the following procedure to configure e-mail information for alert notification.

Note Because Unified CCX generates the e-mail notifications, you can verify that the mail server that you configure can be reached from the Unified CCX platform with the CLI command: **utils network ping** <mail server>

Procedure

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

The Mail Server Configuration window displays.

Step 2 Enter the address of the mail server in the Mail Server field.

Step 3 Enter the port number of the mail server in the Port field.

Step 4 Enter the address of the intended recipient in the Enter e-mail/epage address field.

Repeat Step 4 as necessary to enter all intended e-mail recipients.

By default, RTMT_Admin@domain will be used, where domain is the domain of the host server.

Step 5 Click **OK**.

Additional Information

See the "Related Topics" section on page 8-8.

Configuring Alert Actions

The following procedure describes how to configure new alert actions.

Procedure

Step 1 Display Alert Central, as described in the "Working with Alerts" section on page 8-1.

Step 2 Choose **System >Tools > Alert > Config Alert Action**.

Step 3 Perform Step 17 through in the "Setting Alert Properties" section on page 8-3 to add, edit, or delete alert actions.

Additional Information

See the "Related Topics" section on page 8-8

Configuring a Global E-Mail List for Alert Notifications

The following procedure describes how to configure all precanned alerts at once for sending to one or more e-mail destinations. This procedure uses the initial "Default" alert action setting that is assigned to all alerts by default at installation.

Follow this procedure to configure a recipient list for all precanned alerts without having to set an alert action for each alert. When you add e-mail destinations to the Default alert action list, all pre-canned alerts get sent to those recipients, as long as all alerts continue to use the Default alert action.

Note To configure a new alert action for a specific alert, you can use the Set Alerts/Properties option,which displays when you right-click an alert. You can also reconfigure existing alert actions with this option.

Any time you update an alert action, the changes apply to all alerts that are configured with that alert action. For example, if all alerts use the "Default" alert action, updating the alert action "Default" will impact all alerts.

You cannot remove the "Default" alert action. For all other alert actions, the system allows you to delete an alert action only when it is not associated with other alerts. If an alert action is associated with multiple alerts, you must reassign a new alert action to those alerts before you can delete the alert action.

Procedure

Step 1 Click **Alert Central** in the QuickLaunch Channel.

The Alert Central window displays.

Step 2 Click **System > Tools > Alert > Config Alert Action**.

The Alert Action box displays.

Step 3 Select Default (highlight the item) in the Alert Action list and click **Edit**.

The Action Configuration box displays.

Step 4 (Optional) Enter the description of the default list.

Step 5 Click **Add** to add a recipient. The Input box displays.

Step 6 Enter an e-mail destination that is to receive all alerts. Click **OK**.

The e-mail address displays in the Recipients list in the Action Configuration box; the destination is enabled by default.

Note You can disable an e-mail destination at any time by clicking the check box next to the destination to disable it. To completely remove a recipient from the list, highlight the recipient in the list and click **Delete**.

Step 7 Return to Step 5 to add additional e-mail destinations, as required.

Note You can disable e-mails for an alert at any time by highlighting the alert in the Alert Central window, right-clicking the alert, and using the Set Alert/Properties selections to deselect Enable Email.

Additional Information

See the "Related Topics" section on page 8-8.

Where to Find More Information

Related Topics

- Working with Alerts, page 8-1
- Setting Alert Properties, page 8-3
- Suspending Alerts, page 8-5
- Configuring E-mails for Alert Notification, page 8-6
- Configuring Alert Actions, page 8-6
- Configuring a Global E-Mail List for Alert Notifications, page 8-7
- Configuring Alert Notification for a Counter, page 5-5
- Understanding Alerts, page 7-1

PART 4

Tools for Traces, Logs, and Plug-Ins

CHAPTER 9

Working with Trace and Log Central

The trace and log central feature in the Cisco Unified Real-Time Monitoring Tool (RTMT) allows you to configure on-demand trace collection for a specific date range or an absolute time. You can collect trace files that contain search criteria that you specify and save the trace collection criteria for later use, schedule one recurring trace collection and download the trace files to a SFTP or FTP server on your network, or collect a crash dump file.

After you collect the files, you can view them in the appropriate viewer within the real-time monitoring tool. You can also view traces on the server without downloading the trace files by using the remote browse feature. You can open the trace files by either selecting the internal viewer that is provided with RTMT or choosing an appropriate program as an external viewer.

Note From RTMT, you can also edit the trace setting for the traces on the server that you have specified. Enabling trace settings decreases system performance; therefore, enable Trace only for troubleshooting purposes.

Note To use the trace and log central feature in the RTMT, make sure that RTMT can directly access the server or all of the servers in a cluster without Network Access Translation (NAT). If you have set up a NAT to access devices, configure the server(s) with a hostname instead of an IP address and make sure that the host names and their routable IP address are in the DNS server or host file.

Note For devices that support encryption, the SRTP keying material does not display in the trace file.

This chapter contains information on the following topics:

Importing Certificates

You can import the server authentication certificate that the certificate authority provides for the server or for each server in the cluster. Cisco recommends that you import the certificates before using the trace and log central option. If you do not import the certificates, the trace and log central option displays a security certificate for the server(s) each time that you log in to RTMT and access the trace and log central option. You cannot change any data that displays for the certificate.

To import the certificate, choose **Tools > Trace > Import Certificate**.

A messages displays that states that the system completed the importing of server certificates. Click **OK**.

Additional Information

See the Related Topics, page 9-27.

Displaying Trace and Log Central Options in RTMT

Before you begin, make sure that you have imported the security certificates as described in the "Importing Certificates" section on page 9-2.

To display the Trace & Log Central tree hierarchy, perform one of the following tasks:

- In the Quick Launch Channel, click **System**; then, click the **Trace & Log Central** icon.
- Choose **Tools > Trace & Log Central**.

Tip From any option that displays in the tree hierarchy, you can specify the services/applications for which you want traces, specify the logs and servers that you want to use, schedule a collection time and date, configure the ability to download the files, configure zip files, and delete collected trace files.

After you display the Trace and Log Central options in the real-time monitoring tool, perform one of the following tasks:

- Collect traces for services, applications, and system logs on the server or on one or more servers in the cluster. See "Collecting Trace Files" section on page 9-3
- Collect and download trace files that contain search criteria that you specify as well as save trace collection criteria for later use. See "Using the Query Wizard" section on page 9-6
- Schedule a recurring trace collection and download the trace files to a SFTP or FTP server on your network. See "Scheduling Trace Collection" section on page 9-11
- Collect a crash dump file for one or more servers on your network. See "Collecting a Crash Dump" section on page 9-14.
- Collect audit log files and download the audit logs to a SFTP or FTP server on your network. See "Collecting Audit Logs" section on page 9-17.

- View the trace files that you have collected. See the "Using Local Browse" section on page 9-20.
- View all of the trace files on the server. See the "Using Remote Browse" section on page 9-21.
- View the current trace file that is being written on the server for each application. You can perform a specified action when a search string appears in the trace file. See "Using Real-Time Trace" section on page 9-24.

Additional Information

- See Related Topics, page 9-27.

Collecting Trace Files

Use the Collect Files option in Trace and Log Central to collect traces for services, applications, and system logs on the server or on one or more servers in the cluster. You specify date/time range for which you want to collect traces, the directory in which to download the trace files, whether to delete the collected files from the server, and so on. The following procedure describes how to collect traces by using the trace and log central feature.

Note The services that you have not activated also display, so you can collect traces for those services.

If you want to collect trace files that contain search criteria that you specify or you want to use trace collection criteria that you saved for later use, see the "Using the Query Wizard" section on page 9-6.

RTMT Trace and Log Central Disk IO and CPU Throttling

RTMT supports the throttling of critical Trace and Log Central operations and jobs, whether they are running on demand, scheduled, or automatic. The throttling slows the operations when IO utilization is in high demand for call processing, so call processing can take precedence.

When you make a request for an on-demand operation when the call processing node is running under high IO conditions, the system displays a warning that gives you the opportunity to abort the operation. You can configure the IO rate threshold values that control when the warning displays with the following service parameters (in Cisco RIS Data Collector service):

- TLC Throttling CPU Goal
- TLC Throttling IOWait Goal

The system compares the values of these parameters against the actual system CPU and IOWait values. If the goal (the value of the service parameter) is lower than the actual value, the system displays the warning.

Before You Begin

Perform one or more of the following tasks:

- Configure the information that you want to include in the trace files for the various services from the Trace Configuration window in Cisco Unified Serviceability. For more information on configuring service parameters, see the *Cisco Unified Serviceability Administration Guide* available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html
- If you want alarms to be sent to a trace file, choose an SDI or SDL trace file as the alarm destination in the Alarm Configuration window in Cisco Unified Serviceability.
- Configure the throttling of critical Trace and Log Central operations and jobs by setting the values of the TLC Throttling CPU Goal and TLC Throttling IOWait Goal service parameters (Cisco RIS Data Collector service).

Procedure

Step 1 Display the Trace and Log Central options, as described in the "Displaying Trace and Log Central Options in RTMT" section on page 9-2.

Step 2 In the Trace & Log Central tree hierarchy, double-click **Collect Files**.

The Trace Collection wizard displays.

Note The services that you have not activated also display, so you can collect traces for those services.

Note If any server in the cluster is not available, a dialog box displays with a message that indicates which server is not available. The unavailable server will not display in the Trace and Log Central windows.

Step 3 In the Select UCCX Services/Application tab, perform one of the following tasks:

- To collect all system logs for the server, check the **Select All Services on all Servers** check box or check the check box next to the server and click **Next**.
- To collect traces for particular system logs on the server, check the check boxes that apply and click **Next**.
- To go to the next tab without collecting traces for system logs, click **Next**.

Step 4 In the Select System Services/Application tab, perform one of the following tasks:

- To collect all system logs for all servers in a cluster, check the **Select All Services on all Servers** check box and click **Next**.

Note If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects traces for your standalone server.

- To collect traces for all system logs on a particular server, check the check box next to the server and click **Next**.
- To collect traces for particular system logs on particular servers, check the check boxes that apply and click **Next**.

- To continue the trace collection wizard without collecting traces for system logs, click **Next**.

Step 5 In the Collection Time pane, specify the time range for which you want to collect traces. Choose one of the following options:

- **Absolute Range**—Specify the server time zone and the time range (start and end date and time) for which you want to collect traces.

  The time zone of the client machine provides the default setting for the Select Reference Server Time Zone field. All the standard time zones, along with a separate set of entries for all time zones that have Daylight Saving settings, display in the Select Time Zone drop-down list box.

  Trace and Log Central downloads the file with a time range that is based on your Selected Reference Server Time Zone field. If you have servers in a cluster in a different time zone, TLC will adjust for the time change and get files for the same period of time. For example, if you specify files from 9:00 AM to 10:00 AM and you have a second server (server x) that is in a time zone that is one hour ahead, TLC will download files from 10:00 AM to 11:00 AM from server x.

  To set the date range for which you want to collect traces, choose the drop-down list box in the From Date/Time and To Date/Time fields.

- **Relative Range**—Specify the time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect traces.

Step 6 In the Download File option group box, specify the options that you want for downloading traces. From the Select Partition drop-down list box, choose the partition that contains the logs for which you want to collect traces.

Cisco Unified Serviceability stores the logs for the version of application that you are logged in to in the active partition and stores the logs for the other version (if installed) in the inactive directory.

This means that when you upgrade from one version of Unified CCX that is running on an appliance server to another version, and you restart the server with the new version, Cisco Unified Serviceability moves the logs of the previous version to the inactive partition and stores logs for the newer version in the active partition. If you log back in to the older version, Cisco Unified Serviceability moves the logs for the newer version to the inactive partition and stores the logs for the older version in the active directory.

Note Cisco Unified Serviceability does not retain logs from Unified CCX versions that ran on the Windows platform.

Step 7 To specify the directory in which you want to download the trace files, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies <rtmt_install_directory>\<server name or server IP address>\<download time> where <rtmt_install_directory> specifies the directory where RTMT is installed.

Step 8 To create a zip file of the trace files that you collect, choose the **Zip File** radio button. To download the trace files without zipping the files, choose the **Do Not Zip Files** radio button.

Step 9 To delete collected log files from the server, check the **Delete Collected Log Files from the server** check box.

Step 10 Click **Finish** or, to abort the settings**,** click **Cancel**.

If you clicked Finish, the window shows the progress of the trace collection.

When the trace collection process is complete, the message "Completed downloading for node <Server name or IP address>" displays at the bottom of the window.

Step 11 To view the trace files that you collected, you can use the Local Browse option of the trace collection feature. For more information, see the "Using Local Browse" section on page 9-20.

Note You will see a message if the service parameter values are exceeded or if the system is in code yellow.

Additional Information

- For information about setting the values of service parameters, see the "Service Parameters Configuration" chapter in the *Cisco Unified Contact Center Express Administration Guide*.
- Also see Related Topics, page 9-27.

Collecting Installation Logs

The following procedure describes how to collect installation and upgrade logs in trace and log central.

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel
  - Click **System**.
  - Click the **Trace & Log Central** icon.
- Choose **Tools > Trace >Trace & Log Central**.

The Trace & Log Central window displays.

Step 2 In the Trace & Log Central tree hierarchy, double-click **Collect Install Logs**.

The Collect Install Logs wizard displays

Step 3 In the Select Servers Options box, specify from which server you would like to collect the install logs. To collect the install logs for a particular server, check the check box next to the server. To collect the install logs for all servers, check the Select All Servers check box.

Step 4 In the Download File Options, specify the directory where you want to download the log file. To specify the directory in which you want to download the log files, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies <rtmt_install_directory> where <rtmt_install_directory> specifies the directory where RTMT is installed.

Step 5 Click **Finish**.

Using the Query Wizard

The Trace Collection Query Wizard allows you to collect and download trace files that contain search criteria that you specify as well as to save trace collection criteria for later use. To use the Trace Collection Query Wizard, perform the following procedure.

Note You can open a maximum of five concurrent files for viewing within Trace and Log Central. This includes using the Query Wizard, Local Browse, and Remote Browse features.

Before You Begin

Perform one or more of the following tasks:

- From the Trace Configuration window in Cisco Unified Serviceability, configure the information that you want to include in the trace files for the various services. For more information, refer to *Cisco Unified Serviceability Administration Guide* available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html
- If you want alarms to be sent to a trace file, choose an SDI or SDL trace file as the alarm destination in the Alarm Configuration window. For more information, refer to *Cisco Unified Serviceability Administration Guide* available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Procedure

Step 1 Display the Trace and Log Central options, as described in the "Displaying Trace and Log Central Options in RTMT" section on page 9-2.

Step 2 In the Trace & Log Central tree hierarchy, double-click **Query Wizard**.

The Query wizard displays.

Step 3 In the Query Wizard Options window, click one of the following radio buttons:

- Saved Query

  Click the **Browse** button to navigate to the query that you want to use. Choose the query and click **Open**.

  If you chose a single-node, generic query, the server to which RTMT is connected displays with a checkmark next to the Browse button. You can run the query on additional servers in a cluster by placing a checkmark next to those servers.

  If you chose an all-node, generic query, all servers in the cluster display with a checkmark next to the Browse button. You can uncheck any server for which you do not want to run the query.

  If you chose a regular query, all of the servers that you selected when you saved the query display with a checkmark. You can check or uncheck any servers in the list. If you choose new servers, you must use the wizard to choose the services for that server.

  To run the query without any modifications, click **Run Query** and go to Step 20. To modify the query, go to Step 4.

- Create Query

Step 4 Click **Next**.

Step 5 If you clicked the Saved Query radio button and chose a query, the criteria that you specified for query display. If necessary, modify the list of services/applications for which you want to collect traces. If you clicked the Create Query radio button, you must choose all services/applications for which you want to collect traces.

Tip To collect traces for all services and applications on a particular server, check the check box next to the server name or server IP address. To collect traces for all services and applications for all servers in a Unified CCX cluster, check the **Select All Services on All Servers** check box. To collect traces for particular system logs on the server, check the check boxes that apply.

Note The services that you have not activated also display, so you can collect traces for those services.

Note If you have a cluster configuration, you can install some of the listed services/applications only on a particular server in the cluster. To collect traces for those services/applications, make sure that you collect traces from the server on which you have activated the service/application.

Step 6 In the Select UCCX Services/Application tab, choose the services and application logs in which you are interested by checking all check boxes that apply.

Step 7 Click **Next**.

Step 8 In the Select System Logs tab, choose the logs in which you are interested by checking all check boxes that apply.

Step 9 Click **Next**.

Step 10 In the Query Time Options box, specify the time range for which you want to collect traces. Choose one of the following options:

- **All Available Traces**—Choose this option to collect all the traces on the server for the service(s) that you chose.
- **Absolute Range**—Specify the server time zone and the time range (start and end date and time) for which you want to collect traces.

  The time zone of the client machine provides the default setting for the Select Reference Server Time Zone field. All the standard time zones, along with a separate set of entries for all time zones that have Daylight Saving settings, display in the Select Time Zone drop-down list box.

  Trace Log Central downloads the files with a time range that is based on your Selected Reference Server Time Zone field. If you have servers in a cluster in a different time zone, TLC will adjust for the time change and get files for the same period of time. For example, if you specify files from 9:00 AM to 10:00 AM and you have a second server (server x) that is in a time zone that is one hour ahead, TLC will download files from 10:00 AM to 11:00 AM from server x.

  To set the date range for which you want to collect traces, choose the drop-down list box in the From Date/Time and To Date/Time fields.
- **Relative Range**—Specify the time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect traces.

Step 11 To search by phrases or words that exist in the trace file, enter the word or phrase in the Search String field. If you want to search for an exact match to the word or phrase that you entered, check the Case Sensitive check box.

Step 12 In the Call Processing Impact Options box, specify the level of impact you want the string search activity to have on call processing. From the Select Impact Level drop down list box, select Low, Medium, or High. Low impact causes the least impact on call processing but yields slower results. High impact causes the most impact on call processing but yields faster results.

Step 13 Click **Next**.

Step 14 In the Action Options window, choose one of the following actions:

- Trace Browse
- On Demand Trace Collection
  - To specify the directory in which you want to download the trace files and the results file, click the **Browse** button next to the Download selected files field, navigate to the directory, and click **Open**. The default specifies <rtmt_install_directory>\<server name or server IP address>\<download time> where <rtmt_install_directory> specifies the directory where RTMT is installed.
  - To create a zip file of the trace files that you collect, check the **Zip File** check box.
  - To delete collected log files from the server, check the **Delete Collected Log Files from Server** check box.
- Schedule Download

  Included a start date and time and an end date and time. To configure the trace server, click the Configure Trace Server check box. The SFTP Parameters dialog box displays. In the dialog box, you can configure the following parameters:
  - Host IP Address
  - User Name
  - Password
  - Port
  - Download Directory Path

Step 15 Choose one of the following options:

- To execute the query, click **Run Query**. This option is only available if you selected Trace Browse from the Action Options window.

  The Query Results folder displays. When the query completes, a dialog box that indicates that the query execution completed displays. Click **Close** and continue with Step 20.
- To save the query, click the **Save Query** button and continue with Step 16.
- To download the trace, click the **Download Trace** button. This option is only available if you selected On Demand Trace Collection or Schedule Download from the Action Options window.

Tip After you have downloaded the trace files, you can view them by using the Local Browse option of the trace and log central feature. For more information, see the "Using Local Browse" section on page 9-20.

Step 16 Check the check box next to the type of query that you want to create.

- **Generic Query**—Choose this option if you want to create a query that you can run on servers other than the one on which it was created. You can create a generic query only if the services that you chose exist on that server. If you chose services on more than one server in a cluster, a message displays.

  Then, choose either the Single Node Query or All Node Query option. If you choose the Single Node Query, the trace collection tool by default chooses the server on which you created the query when you execute the query. If you choose the All Node Query option, the trace collection tool selects the following server by default:

- For Unified CCX, the trace collection tool chooses the server on which you created the query when you executed the query.

Note You can choose servers other than the default before running the query.

- **Regular Query**—Choose this option if you only want to run the query on that server or cluster (if applicable) on which you created the query.

Step 17 Click **Finish**.

Step 18 Browse to the location to store the query, enter a name for the query in the File Name field, and click **Save**.

Step 19 Do one of the following tasks:

- To run the query that you have just saved, click **Run Query** and continue with Step 20.
- To exit the query wizard without running the query that you created, click **Cancel**.

Step 20 After the query execution completes, perform one or more of the following tasks:

- To view a file that you collected, navigate to the file by double-clicking Query Results, double-clicking the <node> folder, where <node> equals the IP address or host name for the server that you specified in the wizard, and double-clicking the folder that contains the file that you want to view.

  After you have located the file, you can either right-click the mouse to select the type of program that you would like to use to view the file or double-click the file to display the file in the default viewer. The real-time monitoring tool displays the file in the appropriate viewer for the file type. If no other appropriate viewer applies, the real-time monitoring tool opens files in the Generic Log Viewer.

- Download the trace files and the result file that contains a list of the trace files that your query collected by choosing the files that you want to download, clicking the **Download** button, specifying the criteria for the download, and clicking **Finish**.
  - To specify the directory in which you want to download the trace files and the results file, click the **Browse** button next to the Download selected files field, navigate to the directory, and click **Open**. The default specifies <rtmt_install_directory>\<server name or server IP address>\<download time> where <rtmt_install_directory> specifies the directory where RTMT is installed.
  - To create a zip file of the trace files that you collect, check the **Zip File** check box.
  - To delete collected log files from the server, check the **Delete Collected Log Files from Server** check box.

Tip After you have downloaded the trace files, you can view them by using the Local Browse option of the trace and log central feature. For more information, see the "Using Local Browse" section on page 9-20.

- To save the query, click **Save Query** button and complete Step 16 through Step 18.

Note You will see a message if the service parameter values are exceeded or if the system is in code yellow.

Additional Information

See the Related Topics, page 9-27.

Scheduling Trace Collection

You can use the Schedule Collection option of the trace and log central feature to schedule up to six concurrent trace collections and to download the trace files to a SFTP or FTP server on your network, run another saved query, or generate a syslog file. To change a scheduled collection after you have entered it in the system, you must delete the scheduled collection and add a new collection event. To schedule trace collection, perform the following procedure.

Note You can schedule up 10 trace collection jobs, but only six trace collection can be concurrent. That is, only six jobs can be in a running state at the same time.

Before You Begin

Perform one or more of the following tasks:

- Configure the information that you want to include in the trace files for the various services from the Trace Configuration window of Cisco Unified Serviceability. For more information, refer to the *Cisco Unified Serviceability Administration Guide* available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html
- If you want alarms to be sent to a trace file, choose an SDI or SDL trace file as the alarm destination in the Alarm Configuration window. For more information, refer to the *Cisco Unified Serviceability Administration Guide* available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Procedure

Step 1 Display the Trace and Log Central options, as described in the "Displaying Trace and Log Central Options in RTMT" section on page 9-2.

Step 2 In the Trace & Log Central tree hierarchy, double-click **Schedule Collection**.

The Schedule Collection wizard displays.

Note The services that you have not activated also display, so you can collect traces for those services.

Note If any server in the cluster is not available, a dialog box displays with a message that indicates which server is not available. The unavailable server will not display in the Trace and Log Central windows.

Note If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects traces for all service and applications for your standalone server.

- To collect traces for all services and applications for all servers, check the **Select All Services on All Servers** check box and click **Next**.
- To collect traces for all services and applications on a particular server, check the check box next to the server and click **Next**.
- To collect traces for particular services or applications on particular servers, check the check boxes that apply and click **Next**.
- To continue the schedule collection wizard without collecting traces for services or applications, click **Next.**

Step 3 In the Select UCCX Services/Application tab, perform one of the following tasks:

- To collect all system logs for the server, check the **Select All Services on all Servers** check box or check the check box next to the server and click **Next**.
- To collect traces for particular system logs on the server, check the check boxes that apply and click **Next**.
- To continue the schedule collection wizard without collecting traces for system logs, click **Next**.

Step 4 In the Select System Services/Application tab, perform one of the following tasks:

Note If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects traces for your standalone server.

- To collect all system logs for all servers, check the **Select All Services on all Servers** check box and click **Next**.
- To collect traces for all system logs on a particular server, check the check box next to the server and click **Next**.
- To collect traces for particular system logs on particular servers, check the check boxes that apply and click **Next**.
- To continue the schedule collection wizard without collecting traces for system logs, click **Next**.

Step 5 Specify the server time zone and the time range for which you want to collect traces.

The time zone of the client machine provides the default setting for the Select Reference Server Time Zone field. All the standard time zones, along with a separate set of entries for all time zones that have Daylight Saving settings, display in the Select Time Zone drop-down list box.

Step 6 To specify the date and time that you want to start the trace collection, click the down arrow button next to the Schedule Start Date/Time field. From the Date tab, choose the appropriate date. From the Time tab, choose the appropriate time.

Step 7 To specify the date and time that you want to end the trace collection, click the down arrow button next to the Schedule End Date/Time field. From the Date tab, choose the appropriate date. From the Time tab, choose the appropriate time.

Note The trace collection completes, even if the collection goes beyond the configured end time; however, the trace and log central feature deletes this collection from the schedule.

Step 8 From the Scheduler Frequency drop-down list box, choose how often you want to run the configured trace collection.

Step 9 From the Collect Files that are generated in the last drop-down list boxes, specify the time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect traces.

Step 10 To search by phrases or words that exist in the trace file, enter the word or phrase in the Search String field. The tool searches for a match to the word or phrase that you enter and collects those files that match the search criteria. If you want to search for an exact match to the word or phrase that you entered, check the Case Sensitive check box

Step 11 To create a zip file of the trace files that you collect, check the **Zip File** check box.

Step 12 To delete collected log files from the server, check the **Delete Collected Log Files from the Server** check box.

Step 13 Choose one or more of the following actions:

- Download Files. If you chose Download Files or Run Another Query, continue with Step 14.
- Run Another Query
- Generate Syslog. If you chose Generate Syslog, go to Step 16.

Step 14 In the SFTP/FTP Server Parameters group box, enter the server credentials for the server where the trace and log central feature downloads the results and click **Test Connection**. After the trace and log central feature verifies the connection to the SFTP or FTP server, click **OK**.

Note The **Download Directory Path** field specifies the directory in which the trace and log central feature stores collected files. By default, the trace collection stores the files in the home directory of the user whose user ID you specify in the SFTP or FTP parameters fields: /home/<user>/Trace.

Step 15 If you chose the Run Another Query Option, click the **Browse** button to locate the query that you want to run, and click **OK**.

Note The trace and log central feature only executes the specified query if the first query generates results.

Step 16 Click **Finish**.

A message indicates that the system added the scheduled trace successfully.

Note If the real-time monitoring tool cannot access the SFTP or FTP server, a message displays. Verify that you entered the correct IP address, user name, and password

Step 17 Click **OK**.

Step 18 To view a list of scheduled collections, click the **Job Status** icon in the Trace portion of the Quick Launch Channel.

Tip To delete a scheduled collection, choose the collection event and click **Delete**. A confirmation message displays. Click **OK**.

Additional Information

See the Related Topics, page 9-27.

Viewing Trace Collection Status and Deleting Scheduled Collections

To view trace collection event status and to delete scheduled trace collections, use the following procedure:

Procedure

Step 1 Display the Trace & Log Central tree hierarchy, as described in "Displaying Trace and Log Central Options in RTMT" section on page 9-2.

Step 2 Double-click **Job Status**.

The Job Status Window displays.

Step 3 From the Select a Node drop-down list box, choose the server for which you want to view or delete trace collection events.

This list of scheduled trace collections displays.

Possible job types include Scheduled Job, OnDemand, RealTimeFileMon, and RealTimeFileSearch.

Possible statuses include Pending, Running, Cancel, and Terminated.

Step 4 To delete a scheduled collection, choose the event that you want to delete and click **Delete**.

Note You can delete jobs with a status of "Pending" or "Running" and a job type of "Schedule Task" or job type of "RealTimeFileSearch."

Additional Information

See the Related Topics, page 9-27.

Collecting a Crash Dump

Perform the following procedure to collect a core dump of trace files:

Procedure

Step 1 Display the Trace & Log Central tree hierarchy, as described in "Displaying Trace and Log Central Options in RTMT" section on page 9-2.

Step 2 Double-click **Collect Crash Dump**.

The Collect Crash Dump wizard displays.

Note The services that you have not activated also display, so you can collect traces for those services.

Note If any server in the cluster is not available, a dialog box displays with a message that indicates which server is not available. The unavailable server will not display in the Trace and Log Central windows.

Note If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects traces for all service and applications for your standalone server.

- To collect traces for all services and applications for all servers, check the **Select All Services on All Servers** check box and click **Next**.
- To collect traces for all services and applications on a particular server, check the check box next to the server and click **Next**.
- To collect traces for particular services or applications on particular servers, check the check boxes that apply and click **Next**.
- To continue the collect crash dump wizard without collecting traces for services or applications, click **Next**.

Step 3 In the Select UCCX Services/Application tab, perform one of the following tasks:

- To collect all system logs for the server, check the **Select All Services on all Servers** check box or check the check box next to the server and click **Next**.
- To collect traces for particular system logs on the servers, check the check boxes that apply and click **Next**.
- To continue the collect crash dump wizard without collecting traces for system logs, click **Next**.

Step 4 In the Select System Services/Application tab, perform one of the following tasks:

Note If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects traces for your standalone server.

- To collect all system logs for all servers, check the **Select All Services on all Servers** check box and click **Next**.
- To collect traces for all system logs on a particular server, check the check box next to the server and click **Next**.
- To collect traces for particular system logs on particular servers, check the check boxes that apply and click **Next**.
- To continue the collect crash dump wizard without collecting traces for system logs, click **Next**.

Step 5 In the Collection Time group box, specify the time range for which you want to collect traces. Choose one of the following options:

- **Absolute Range**—Specify the server time zone and the time range (start and end date and time) for which you want to collect traces.

  The time zone of the client machine provides the default setting for the Select Reference Server Time Zone field. All the standard time zones, along with a separate set of entries for all time zones that have Daylight Saving settings, display in the Select Time Zone drop-down list box.

Trace Log Central downloads the files with a time range that is based on your Selected Reference Server Time Zone field. If you have servers in a cluster in a different time zone, TLC will adjust for the time change and get files for the same period of time. For example, if you specify files from 9:00 AM to 10:00 AM and you have a second server (server x) that is in a time zone that is one hour ahead, TLC will download files from 10:00 AM to 11:00 AM from server x.

To set the date range for which you want to collect crash files, choose the drop-down list box in the From Date/Time and To Date/Time fields.

- **Relative Range**—Specify the length of time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect crash files.

Step 6 From the Select Partition drop-down list box, choose the partition that contains the logs for which you want to collect traces.

Cisco Unified Serviceability stores the logs for the version of application that you are logged in to in the active partition and stores the logs for the other version (if installed) in the inactive directory.

This means that when you upgrade from one version of Unified CCX that is running on the Linux platform to another version, and you restart the server with the new version, Cisco Unified Serviceability moves the logs of the previous version to the inactive partition and stores logs for the newer version in the active partition. If you log in to the older version, Cisco Unified Serviceability moves the logs for the newer version to the inactive partition and stores the logs for the older version in the active directory.

Note Cisco Unified Serviceability does not retain logs from Unified CCX versions that ran on the Windows platform.

Step 7 To specify the directory in which you want to download the trace files, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies <rtmt_install_directory>\<server name or server IP address>\<download time> where <rtmt_install_directory> specifies the directory where RTMT is installed.

Step 8 To create a zip file of the crash dump files that you collect, choose the **Zip File** radio button. To download the crash dump files without zipping the files, choose the **Do Not Zip Files** radio button.

Note You cannot download a zipped crash dump file that exceeds 2 gigabytes.

Step 9 To delete collected crash dump files from the server, check the **Delete Collected Log Files from Server** check box.

Step 10 Click **Finish**.

A message displays that states that you want to collect core dumps. To continue, click **Yes**.

Note If you chose the **Zip File** radio button and the crash dump files exceed 2 gigabytes, the system displays a message that indicates that you cannot collect the crash dump file of that size with the **Zip File** radio button that you chose. Choose the **Do Not Zip Files** radio button and try the collection again.

Additional Information

See the Related Topics, page 9-27.

Collecting Audit Logs

The audit user can collect, view, and delete the audit logs. The end user can view the audit logs.

Note Only a user with an audit role can delete the audit logs.

Perform the following procedure to collect audit logs:

Procedure

Step 1 Display the Trace & Log Central tree hierarchy, as described in "Displaying Trace and Log Central Options in RTMT" section on page 9-2.

Step 2 Double-click **Collect Audit Logs**.

The Collect Audit Logs Action Options wizard displays.

Step 3 *P*erform one of the following actions in the Action Options window:

- To browse audit logs, check the **Browse Audit Logs** check box.
- To download audit logs, check the **Download Audit Logs** check box.
- To schedule a download of audit logs, check the **Schedule Download of Audit Logs** check box.

Step 4 Click **Next**.

The Nodes Selection Options wizard displays.

Step 5 Perform one of the following actions in the Action Options window:

Note If you have a standalone server and check the **Select All Servers** check box, the system will browse, download, or schedule a download of all audit logs for your standalone server.

- To browse, download, or schedule a download of audit logs for all servers, check the **Select All Servers** check box.
- To browse, download, or schedule a download of audit logs on a particular server, check the check box next to the server.

Step 6 Click **Finish**.

Proceed with one of the following selections:

- Browse Audit Logs, go to Step 7.
- Download Audit Logs, go to Step 12.
- Schedule Download of Audit Logs, go to Step 17.

Step 7 The Remote Browse is Ready window displays. Click the **Close** button.

Step 8 The Nodes pane displays.

Step 9 On the left side of the Nodes pane, double-click on the **Nodes** folder. Navigate through the tree hierarchy until the Audit App folder displays.

Step 10 After the audit log file names display in the pane on the right side of the window, you can either right-click the mouse to select the type of program that you would like to use to view each file or double-click the selected file to display the file in the default viewer.

Step 11 Select an audit log file and perform one of the following actions:

- To download the selected audit log file, click the **Download** button.

  The Select Download Options wizard displays.

  a. To specify the directory in which you want to download the audit log file, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies <\Program Files\Cisco\CallManager Serviceability\JRtmt>.

  b. To create a zip file of the audit log files that you collect, choose the **Zip File** radio button.

  Note You cannot download a zipped audit log file that exceeds 2 gigabytes.

  c. To delete collected audit log files from the server, check the **Delete Files on Server** check box.

  d. Click **Finish**.

- To delete the selected audit log file, click the **Delete** button.
- To refresh the selected audit log file, click the **Refresh** button.
- To refresh all of the audit log files, click the **Refresh All** button.

  You have completed the steps for Browse Audit Logs.

Step 12 To download audit logs, click **Next**. The Download Audit Logs window displays.

Step 13 In the Nodes Selection Options pane, select one of the following:

- Check the **Select All Servers** checkbox.
- Check a specific node checkbox.

Step 14 In the Collection Time pane, select one of the following radio buttons:

- Absolute Range—Specify the server time zone and the time range (start and end date and time) for which you want to audit logs.

  The time zone of the client machine provides the default setting for the Select Reference Server Time Zone field. All the standard time zones, along with a separate set of entries for all time zones that have Daylight Saving settings, display in the Select Time Zone drop-down list box.

  Trace Log Central downloads the files with a time range that is based on your Selected Reference Server Time Zone field. If you have servers in a cluster in a different time zone, TLC will adjust for the time change and get files for the same period of time. For example, if you specify files from 9:00 AM to 10:00 AM and you have a second server (server x) that is in a time zone that is one hour ahead, TLC will download files from 10:00 AM to 11:00 AM from server x.

- Relative Range—Specify the length of time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect audit logs based on the values from the following table:

Period of Time	Range
Minutes	5 - 60
Hours	2 - 24
Days	1 - 31
Weeks	1 - 4
Months	1 -12

Step 15 In the Download File Options pane, select one of the following options:

a. To specify the directory in which you want to download the audit log file, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies <\Program Files\Cisco\CallManager Serviceability\JRtmt>.

b. To create a zip file of the audit log files that you collect, choose the **Zip File** radio button.

Note You cannot download a zipped audit log file that exceeds 2 gigabytes.

c. To delete collected audit log files from the server, check the **Delete Collected Log Files from Server** check box.

Step 16 Click **Finish**. You have completed the steps for the download of audit logs.

Step 17 The Schedule Download of Audit Logs window displays.

a. In the Nodes Selection Options pane, select one of the following options:
   - Check the **Select All Servers** checkbox.
   - Check a specific node checkbox.

b. In the Schedule Time pane, perform the following actions:
   - Highlight the **Select Reference Server Time Zone**.
   - Use the calendar and highlight a **Start Date/Time**.
   - Use the calendar and highlight an **End Date/Time**.
   - Select the Scheduler Frequency. You may choose Hourly, Daily, Weekly, or Monthly.
   - Check the **Zip All Files** checkbox if you want to zip the audit log files.
   - Check the **Delete Collected Log Files From Server** checkbox if you want to delete the collected audit log files from the server.

c. In the Action Options pane, check the **Download Files** checkbox.

   The SFTP/FTP Parameters Dialog window displays. Enter the following information:
   - Protocol—Select FTP (default) or SFTP.
   - Host IP Address—Enter the IP address of the host server.
   - User Name—Enter your user name.
   - Password—Enter your password.
   - Port—Enter the FTP or SFTP port information.
   - Download Directory Path—Enter the complete directory path where the files get downloaded.
   - Click on **Test Connection**. When the connection has been tested, the files are downloaded.

Additional Information

See the Related Topics, page 9-27.

Using Local Browse

After you have collected trace files and downloaded them to your PC, you can view them with a text editor that can handle UNIX variant line terminators such as WordPad on your PC, or you can view them by using the viewers within the real-time monitoring tool.

Note Do not use NotePad to view collected trace files.

Perform the following procedure to display the log files that you have collected with the trace and log central feature. If you zipped the trace files when you downloaded them to your PC, you will need to unzip them to view them by using the viewers within the real-time monitoring tool.

Note You can open a maximum of five concurrent files for viewing within Trace & Log Central. This includes using the Query Wizard, Local Browse, and Remote Browse features.

Before You Begin

Collect traces files as described in one of the following sections:

- "Collecting Trace Files" section on page 9-3
- "Using the Query Wizard" section on page 9-6
- "Scheduling Trace Collection" section on page 9-11

Procedure

Step 1 Display the Trace and Log Central options, as described in the "Displaying Trace and Log Central Options in RTMT" section on page 9-2.

Step 2 Double-click **Local Browse**.

Step 3 Browse to the directory where you stored the log file and choose the file that you want to view.

Step 4 To display the results, double-click the file.

Step 5 If the file type has a viewer that is already associated with it, the file opens in that viewer. Otherwise, the Open With dialog box displays. Click the program (viewer) that you would like to use to view the file. If your preferred program is not on the list, choose another program by clicking the **Other** button.

If you want to use this program as your default viewer, click the **Always use this program to open these files** check box

The real-time monitoring tool displays the file in the appropriate viewer for the file type. If no other appropriate viewer applies, the real-time monitoring tool opens files in the Generic Log Viewer.

Additional Information

See the Related Topics, page 9-27.

Using Remote Browse

After the system has generated trace files, you can view them on the server by using the viewers within the real-time monitoring tool. You can also use the remote browse feature to download the traces to your PC.

Perform the following procedure to display and/or download the log files on the server with the trace and log central feature.

Note You can open a maximum of five concurrent files for viewing within Trace and Log Central. This includes using the Query Wizard, Local Browse, and Remote Browse features.

Before You Begin

Collect traces files as described in one of the following sections:

- "Collecting Trace Files" section on page 9-3
- "Using the Query Wizard" section on page 9-6
- "Scheduling Trace Collection" section on page 9-11

Procedure

Step 1 Display the Trace and Log Central options, as described in the "Displaying Trace and Log Central Options in RTMT" section on page 9-2.

Step 2 Double-click **Remote Browse**.

Step 3 Choose the appropriate radio button, and click **Next**.

Note The services that you have not activated also display, so you can choose traces for those services.

Note If you choose Crash Dump, the wizard displays only the services that may cause a crash dump. If you do not see the service in which you are interested, click **Back** and choose Trace Files.

Note If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects traces for all service and applications for your standalone server.

- To collect traces for all services and applications for all servers, check the **Select All Services on All Servers** check box and click **Next**.
- To collect traces for all services and applications on a particular server, check the check box next to the server and click **Next**.
- To collect traces for particular services or applications on particular servers, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without collecting traces for services or applications, click **Next.**

Step 4 In the Select UCCX Services/Application tab, perform one of the following tasks:

- To collect all system logs for the server, check the **Select All Services on all Servers** check box or check the check box next to the server and click **Next**.
- To collect traces for particular system logs on the server, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without collecting traces for system logs, click **Next**.

Step 5 In the Select System Services/Application tab, perform one of the following tasks:

Note If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects system logs for your standalone server.

- To collect all system logs for all servers, check the **Select All Services on all Servers** check box and click **Next**.
- To collect traces for all system logs on a particular server, check the check box next to the server and click **Next**.
- To collect traces for particular system logs on particular servers, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without collecting traces for system logs, click **Next**.
- Go to Step Step 8.

Note If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects crash dump files for your standalone server.

- To choose crash dump files for all services and applications for all servers, check the **Select All Services on All Servers** check box and click **Next**.
- To choose crash dump files for all services and applications on a particular server, check the check box next to the server and click **Next**.
- To choose crash dump files for particular services or applications on particular servers, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without collecting crash dump files, click **Next**.

Step 6 In the Select UCCX Services/Application tab, perform one of the following tasks:

- To choose crash dump files for the server, check the **Select All Services on all Servers** check box or check the check box next to the server and click **Next**.
- To choose crash dump files for particular system logs on the server, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without collecting crash dump files, click **Next**.

Step 7 In the Select System Services/Application tab, perform one of the following tasks:

Note If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects crash dump files for your standalone server.

- To choose crash dump files for all servers, check the **Select All Services on all Servers** check box.
- To choose crash dump files for all system logs on a particular server, check the check box next to the server.

- To choose crash dump files for particular system logs on particular servers, check the check boxes that apply.
- To continue the Remote Browse wizard without collecting crash dump files, go to Step 8.

Step 8 Click **Finish**.

Step 9 After the traces become available, a message displays. Click **Close**.

Step 10 Perform one of the following tasks:

- To display the results, navigate to the file through the tree hierarchy. After the log file name displays in the pane on the right side of the window, you can either right-click the mouse to select the type of program that you would like to use to view the file or double-click the file to display the file in the default viewer.

Tip To sort the files that display in the pane, click a column header; for example, to sort the files by name, click the Name column header.

The real-time monitoring tool displays the file in the appropriate viewer for the file type. If no other appropriate viewer applies, the real-time monitoring tool opens files in the Generic Log Viewer.

- To download the trace files, choose the files that you want to download, click **Download**, specify the criteria for the download, and click **Finish**.
  - To specify the directory in which you want to download the trace files, click the **Browse** button next to the Download all files field, navigate to the directory, and click **Open**. The default specifies <rtmt_install_directory>\<server name or server IP address>\<download time> where <rtmt_install_directory> specifies the directory where RTMT is installed.
  - To create a zip file of the trace files that you collect, check the **Zip File** check box.
  - To delete collected log files from the server, check the **Delete Files on server** check box.
- To delete trace files from the server, click the file that displays in the pane on the right side of the window; then, click the **Delete** button.
- To refresh a specific service or a specific server in a cluster, click the service or server name; then, click the **Refresh** button. After a message states that the remote browse is ready, click **Close**.
- To refresh all services or all servers in a cluster that display in the tree hierarchy, click the **Refresh All** button. After a message states that the remote browse is ready, click **Close**.

Tip After you have downloaded the trace files, you can view them by using the Local Browse option of the trace and log central feature. For more information, see the "Using Local Browse" section on page 9-20.

Additional Information

See the Related Topics, page 9-27.

Using Real-Time Trace

The real-time trace option of the trace and log central feature in the RTMT allows you to view the current trace file that is being written on the server for each application. If the system has begun writing a trace file, the real-time trace starts reading the file from the point where you began monitoring rather than at the beginning of the trace file. You cannot read the previous content.

The real-time trace provides the following options:

- View Real-Time Data, page 9-24
- Monitor User Event, page 9-25

View Real-Time Data

The view real-time data option of the trace and log central feature allows you to view a trace file as the system writes data to that file. You can view real-time trace data in the generic log viewer for up to 10 services, with a limit of 3 concurrent sessions on a single server. The log viewer refreshes every 5 seconds. As the traces get rolled into a new file, the generic log viewer appends the content in the viewer.

Note Depending on the frequency of the traces that a service writes, the View Real Time Data option may experience a delay before being able to display the data in the generic log viewer.

Procedure

Step 1 Display the Trace & Log Central tree hierarchy, as described in "Displaying Trace and Log Central Options in RTMT" section on page 9-2.

Step 2 Double-click **Real Time Trace**.

Note If any server in the cluster is not available, a dialog box displays with a message that indicates which server is not available. The unavailable server will not display in the Trace and Log Central windows.

Step 3 Double-click **View Real Time Data**.

The View Real Time Data wizard displays.

Step 4 From the **Nodes** drop-down list box, choose the server for which you want to view real-time data and click **Next**.

Step 5 Choose the product, service, and the trace file type for which you want to view real-time data.

Note The services that you have not activated also display, so you can collect traces for those services.

Note The following message displays at the bottom of this window: If trace compression is enabled, the data seen in this window can be bursty due to buffering of data.

Step 6 Click **Finish**. The real-time data for the chosen service displays in the generic log viewer.

Step 7 Check the **Show New Data** check box to keep the cursor at the end of the window to display new traces as they appear. Uncheck the **Show New Data** check box if you do not want the cursor to move to the bottom of the window as new traces display.

Step 8 Repeat this procedure to view data for additional services. For Unified CCX, you can view data for 5 services only.

A message displays if you attempt to view data for too many services or too many services on a single server.

Step 9 When you are done viewing the real-time data, click **Close** on the generic log viewer.

Tip To search by phrases or words in the Log Viewer, enter the word or phrase in the Search String field. If you want to do a case-sensitive search for a word or phrase, check the Match Case check box.

Additional Information

See the Related Topics, page 9-27.

Monitor User Event

The monitor user event option of the trace and log central feature monitors real-time trace files and performs a specified action when a search string appears in the trace file. The system polls the trace file every 5 seconds. If the search string occurs more than once in one polling interval, the system performs the action only once. For Unified CCX, you can monitor only one service for each event.

Before you Begin

If you want to generate an alarm when the specified search string exists in a monitored trace file, enable the LogFileSearchStringFound alert. For more information on enabling alerts, see the "Setting Alert Properties" section on page 8-3.

Procedure

Step 1 Display the Trace & Log Central tree hierarchy, as described in "Displaying Trace and Log Central Options in RTMT" section on page 9-2.

Step 2 Double-click **Real Time Trace**.

Note If any server in the cluster is not available, a dialog box displays with a message that indicates which server is not available. The unavailable server will not display in the Trace and Log Central windows.

Step 3 Double-click **Monitor User Event**.

The Monitor User Event wizard displays.

Step 4 Perform one of the following tasks:

- To view the monitoring events that you have already set up, choose the **View Configured Events** radio button, choose a server from the drop-down list box, and click **Finish**.

The events that are configured for the server that you choose display.

Note To delete an event, choose the event and click **Delete**.

- To configure new monitoring events, choose the **Create Events** radio button, click **Next**, and continue with Step 5.

Step 5 Choose the server that you want the system to monitor from the **Nodes** drop-down list box and click **Next**.

Step 6 Choose the product, service, and the trace file type that you want the system to monitor and click **Next**.

Note The services that you have not activated also display, so you can collect traces for those services.

Step 7 In the **Search String** field, specify the phrases or words that you want the system to locate in the trace files. The tool searches for an exact match to the word or phrase that you enter.

Step 8 Specify the server time zone and the time range (start and end date and time) for which you want the system to monitor trace files.

The time zone of the client machine provides the default setting for the Select Reference Server Time Zone field. All the standard time zones, along with a separate set of entries for all time zones that have Daylight Saving settings, display in the Select Time Zone drop-down list box.

Trace and Log Central downloads the files with a time range that is based on your Selected Reference Server Time Zone field. If you have servers in a cluster in a different time zone, TLC will adjust for the time change and get files for the same period of time. For example, if you specify files from 9:00 AM to 10:00 AM and you have a second server (server x) that is in a time zone that is one hour ahead, TLC will download files from 10:00 AM to 11:00 AM from server x.

To set the date range for which you want to monitor traces, choose the drop-down list box in the From Date/Time and To Date/Time fields.

Step 9 Choose one or more of the following actions that you want the system to perform when it encounters the search string that you specified in the Search String field:

- Alert—Choose this option to generate an alarm when the system encounters the specified search string. For the system to generate the alarm, you must enable the enable the LogFileSearchStringFound alert. For more information on enabling alerts, see the "Setting Alert Properties" section on page 8-3.
- Local Syslog—Choose this option if you want the system to log the errors in the application logs area in the SysLog Viewer. The system provides a description of the alarm and a recommended action. You can access the SysLog Viewer from RTMT.
- Remote Syslog—Choose this option to enable the system to store the syslog messages on a syslog server. In the **Server Name** field, specify the syslog server name.
- Download File—Choose this option to download the trace files that contain the specified search string. In the SFTP/FTP Server Parameters group box, choose either FTP or SFTP, enter the server credentials for the server where you want to download the trace files, and click **Test Connection**. After the trace and log central feature verifies the connection to the SFTP or FTP server, click **OK**.

Note The Download Directory Path field specifies the directory in which the trace and log central feature stores collected files. By default, the trace collection stores the files in the home directory of the user whose user ID you specify in the SFTP/FTP parameters fields: /home/<user>/Trace.

Note The system polls the trace files every 5 seconds and performs the specified actions when it encounters the search string. If more than one occurrence of the search string occurs in a polling interval, the system performs the action only once.

Note The following message displays at the bottom of this window: If trace compression is enabled, there might be a delay in catching the event after it occurs, due to buffering of data.

Step 10 Click **Finish**.

Additional Information

See the Related Topics, page 9-27.

Updating the Trace Configuration Setting for RTMT

To edit trace settings for the Real-Time Monitoring plug-in, choose **Edit > Trace Settings**; then, click the radio button that applies. The system stores the rtmt.log file in the Documents and Settings directory for the user; for example, on a Windows machine, the log gets stored in C:\Documents and Settings\<userid>\.jrtmt\log.

Tip The Error radio button equals the default setting.

Additional Information

See the Related Topics, page 9-27.

Where to Find More Information

Related Topics

- Using the Query Wizard, page 9-6
- Using Local Browse, page 9-20
- Collecting Trace Files, page 9-3
- Scheduling Trace Collection, page 9-11
- Displaying Trace and Log Central Options in RTMT, page 9-2
- Collecting a Crash Dump, page 9-14
- Using Local Browse, page 9-20

Additional Cisco Documentation

Cisco Unified Serviceability Administration Guide available here:
http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

CHAPTER 10

Using SysLog Viewer

To display messages in SysLog Viewer, perform the following procedure:

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel
  - Click **System**.
  - In the tree hierarchy, double-click **Tools**.
  - Click the Syslog Viewer icon.
- Choose **System >Tools > SysLog Viewer> Open SysLog Viewer**.

Step 2 From the Select a Node drop-down list box, choose the server where the logs that you want to view are stored.

Step 3 Click the tab for the logs that you want to view.

Step 4 After the log displays, double-click the log icon to list the file names in the same window.

Tip If some syslog messages do not appear in the window, scrolling the mouse pointer over the missing syslog messages refreshes the display.

Step 5 To view the contents of the file at the bottom of the window, click the file name.

Step 6 Click the entry that you want to view.

Step 7 To view the complete syslog message, double-click the syslog message.

Tip CiscoSyslog messages also display the syslog definition, which includes recommended actions, in an adjacent pane when you double-click the syslog message. You do not have to access the Alarm Definitions in Cisco Unified Serviceability for this information.

You can also use the following buttons that are described in Table 10-1 to view the syslog messages:

Tip To make a column larger or smaller, drag the arrow that displays when your mouse hovers between two column headings.

Tip You can order the messages by clicking a column heading. The first time that you click a column heading, the records display in ascending order. A small triangle pointing up indicates ascending order. If you click the column heading again, the records display in descending order. A small triangle pointing down indicates descending order. If you click the column heading one more time, the records displays in the unsorted state.

Tip You can filter the results by choosing an option in the Filter By drop-down list box. To remove the filter, click Clear Filter. All logs display after you clear the filter.

Table 10-1 Syslog Viewer Buttons

Button	Function
Refresh	Updates the contents of the current log on the syslog viewer. **Tip** You can enable the syslog viewer to automatically update the syslog messages every 5 seconds by checking the Auto Refresh check box.
Clear	Clears the display of the current log.
Filter	Limits the messages that displayed base on the set of options that you select.
Clear Filter	Removes the filter that limits the type of messages that display.
Find	Allows you to search for a particular string in the current log.
Save	Saves the currently selected log on your PC

Additional Information

See the "Related Topics" section on page 10-2.

Where to Find More Information

Related Topics

- Installing and Configuring Cisco Unified Real-Time Monitoring Tool, page 2-1

CHAPTER 11

Using Plug-ins

You can expand the functionality of RTMT by installing an application plug-in. You can download the latest plug-ins for the RTMT viewer from Cisco.com. After installing the plug-in, you can access the application in the RTMT viewer.

To download the plug-in, perform the following procedure:

Procedure

Step 1 Choose **Application > CCO Voice Tools Download**.

Step 2 The Login Prompt displays. Enter your Cisco.com user name and password and click OK.

Step 3 Download the file to your PC.

Step 4 To begin the installation, double-click the download file.

Step 5 Follow the installation instruction.

To access the plug-in, perform the following procedure:

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel
  - Click **System**.
  - In the tree hierarchy, double-click **Tools**.
  - Click the icon of the application in which you are interested.
- Under **System > Tools > Plugin**, choose the plug-in that you want to launch.

The application displays in the plugin window.

Refer to the application document for usage information.

Note Currently, Unified CCX does not provide any application plug-ins for the RTMT.

PART 5

Analysis Manager

CHAPTER 12

Understanding Cisco Unified Analysis Manager for Cisco Unified Contact Center Express

The Cisco Unified Analysis Manager (Unified Analysis Manager), a tool included with the Cisco Unified Real-Time Monitoring Tool (RTMT), is used to perform troubleshooting operations. Unified Analysis Manager also allows you to monitor various aspects of the devices added to the tool. When the Unified Analysis Manager is launched, it can be used to collect troubleshooting information from your system and provide an analysis of that information. You can use this information to perform your own troubleshooting operation or to send the information to Cisco Technical Assistance for analysis for a Unified CM installation.

The Analysis Manager application is installed as an option when you install the RTMT software. The Analysis Manager interface is accessed from the RTMT main menu and quick launch channel.

Once it is installed, the application can identify the supported UC products and applications that you have in your system and troubleshoot call failures across these UC applications, collecting trace and log files, and other platform and configuration information.

The Unified Analysis Manager will support the following products:

- Cisco Unified Contact Center Express (Unified CCX) Release 8.0(1)
- Cisco Unified Communications Manager (Unified CM) Release 8.0 (1)
- Cisco Unified Contact Center Enterprise (Unified CCE) Release 8.0(1)
- Cisco IOS Voice Gateways (37xx, 28xx, 38xx, 5350XM, 5400XM) IOS Release PI 11
- Cisco Unity Connection (Unity Connection) Release 8.0(1)
- Cisco Unified Presence (Unified Presence) Release 8.0(2)

The three primary components of the Unified Analysis Manager interface are:

- Administration—The system component lets you import device and group configuration from an external file and provide a status of jobs run by the Unified Analysis Manager.
- Inventory —The inventory component is used to identify all of the devices in your system that can be accessed and analyzed by the Unified Analysis Manager.
- Tools —The tools component contains all of the functions that Unified Analysis Manager supports. This includes configuring traces settings, collecting logs and viewing configurations.

How the Unified Analysis Manager Works

The Unified Analysis Manager application is installed as part of the RTMT installation for a Unified CM server. So once you complete the RTMT installation, you have access to the Unified Analysis Manager features.

The Unified Analysis Manager application is not displayed when RTMT is connected to a Unified CCX server because this tool is dependent on the Unified CM database. Therefore, you need to install RTMT for a Unified CM server.

When you use RTMT to connect to a Unified CM or a Unified CM Business Edition server, you can add nodes to include Unified CCX servers (or any of the supported products) which form part of the Unified Communications solution in Unified Analysis Manager.

Installing Unified Analysis Manager for Unified CCX

To monitor and troubleshoot a Unified CCX based solution with the help of Unified Analysis Manager, you must install the RTMT for a Unified CM server and then add the Unified CCX nodes accordingly. Other supported products which form the solution should also be added as required.

Caution The Unified Analysis Manager is designed in such a way so that if you install RTMT for a Unified CCX server, you will be unable to find or view it from RTMT. This is because the Unified Analysis Manager is dependent on the Unified CM database for its functioning.

Adding a Unified CCX Node

The following procedure explains how to add a Unified CCX node or edit an existing configuration:

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory > Node**. The Node window displays.

Step 2 Click the **Add** button to add a node or select a node from the list or click the **Edit** button to edit an existing configuration. The **Add** or **Edit Node** screen displays.

Note Fields on this screen that are marked with an asterisk (*) are required fields.

Step 3 Use the **Node Type** drop-down list box to select the node as **Unified CCX**.

Step 4 In the **IP/Host Name** field, enter the host name or the IP address of the node you are adding or editing.

Step 5 In the **Transport Protocol** field, select the protocol you want to use. Options for this field depend on the **Product Type** you selected.

Note The **Transport Protocol** field is automatically populated with the default value specific to Unified CCX and is not editable.

Step 6 In the **Port Number** field, enter the port number on the node that you will be using.

Note The **Port Number** field is already populated with the default value and needs to be changed only if it has been changed explicitly on the Unified CCX nodes, which is rare.

Step 7 In the **User Name** and **Password** fields, enter the user name and password that gives you access to the node. Re-enter the password in the **Confirm Password** field.

Note For the **User Name** and **Password** fields, use the same Platform Administrator username and password that you use for Cisco Unified Operating System Administration on the Unified CCX server.

Step 8 In the **Description** field, you can optionally provide a brief description of the node you are adding.

Step 9 In the **Associated Call Record Server** and **Associated Trace File Server** fields, use the drop down list to select the respective servers you want to use for the node.

Step 10 Use the **Associated Group** checkboxes if you want to add the node to an existing group.

Step 11 If you have a NAT or Terminal Server configuration, use the **Advanced** button to display the **Add Node-Advanced** screen. Enter the appropriate information in the **Alternate IP/Hostname** and **Alternate Port** fields.

Step 12 Click the **Save** button to add the node. You can use the **Cancel** button to end the operation without adding the node.

Adding a Unified Contact Center Express Call Record Repository

The following procedure explains how to add a call record server or edit an existing configuration:

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory > Call Record Repositories**.

Step 2 The **Call Record Repository** window displays with a list of configured servers. Click the **Add** button to add a new server or highlight a server on the list or click the **Edit** button to edit an existing configuration.

Step 3 Use the **Repository Type** drop down list to select **Unified CCX**.

Step 4 In the **Hostname** field, enter the name of the server you are adding.

Step 5 In the **JDBC Port** field, enter the port number on the server that you will be using.

Note The **JDBC Port** field is automatically populated with the default port number if you have chosen Unified CCX as the repository type.

Step 6 In the **JDBC User Name** and **JDBC Password** fields, enter the user name and password that gives you access to the server. Re-enter the password in the **Confirm Password** field.

Note Enter 'uccxsct' in the **JDBC User Name** field. You can however reset the password for this user from the Password Management page of the Cisco Unified CCX Administration. The new password should be used to configure the Call Record Repository.

Step 7 In the **Description** field, you can optionally provide a brief description of the node you are adding.

Step 8 Use the **Nodes Available for Association** to select the nodes that will have access to the server.

Step 9 If you have a NAT or Terminal Server configuration, use the **Advanced** button to display the **Add Call Record Server-Advanced** screen. Enter the appropriate information in the **Alternate Hostname** and **Alternate Port** fields.

Step 10 Click the **Add** button to add the server or **Edit** to update the configuration. You can use the **Cancel** button to end the operation without adding the server.

After you are done with adding the node(s) and call record repository(s), click **Test Connectivity** from the Unified Ananlysis Manager screen to check the connectivity and confirm that the node(s) and call record repository(s) are up and working.

Where to Find More Information

For more information about RTMT and Unified CCX, refer to:

- Cisco Unified Communications Manager Release 8.0(1)
- Cisco Unified Contact Center Express Release 8.0(1)

PART 6

Appendixes: Performance Counters and Alerts

APPENDIX A

System Performance Objects and Counters

This appendix contains the following sections:

Cisco Tomcat Connector

The Tomcat Hypertext Transport Protocol (HTTP)/HTTP Secure (HTTPS) Connector object provides information about Tomcat connectors. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Unified CCX web pages get accessed. The Secure Socket Layer (SSL) status of web application URLs provides the basis for the instance name for each Tomcat HTTP Connector. For example, https://*<IP Address>*:8443 for SSL or http://*<IP Address>*:8080 for non-SSL. Table A-1 contains information on the Tomcat HTTP connector counters.

Table A-1 Cisco Tomcat Connector

Counters	Counter Description
Errors	This counter represents the total number of HTTP errors (for example, 401 Unauthorized) that the connector encountered. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Unified CCX-related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.
MBytesReceived	This counter represents the amount of data that the connector received. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Unified CCX-related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.
MBytesSent	This counter represents the amount of data that the connector sent. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Unified CCX-related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.
Requests	This counter represents the total number of request that the connector handled. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Unified CCX-related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.

Table A-1 Cisco Tomcat Connector (continued)

Counters	Counter Description
ThreadsTotal	This counter represents the current total number of request processing threads, including available and in-use threads, for the connector. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Unified CCX-related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.
ThreadsMax	This counter represents the maximum number of request processing threads for the connector. Each incoming request on a Unified CCX-related window requires a thread for the duration of that request. If more simultaneous requests are received than the currently available request processing threads can handle, additional threads will be created up to the configured maximum shown in this counter. If still more simultaneous requests are received, they accumulate within the server socket that the connector created, up to an internally specified maximum number. Any further simultaneous requests will receive connection refused messages until resources are available to process them. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Unified CCX-related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.
ThreadsBusy	This counter represents the current number of busy/in-use request processing threads for the connector. A Tomcat Connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when web pages that are related to Unified CCX are accessed. The Secure Sockets Layer (SSL) status of the URLs for the web application provides the basis for the instance name for each Tomcat connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.

Cisco Tomcat JVM

The Cisco Tomcat Java Virtual Machine (JVM) object provides information about the pool of common resource memory used by Unified CCX applications such as Cisco Unified CCX Administration and Cisco Unified Serviceability. Table A-2 contains information on the Tomcat JVM counters.

Table A-2 Tomcat JVM

Counters	Counter Description
KBytesMemoryFree	This counter represents the amount of free dynamic memory block (heap memory) in the Tomcat Java Virtual Machine. The dynamic memory block stores all objects that Tomcat and its web applications such as Cisco Unified CCX Administration and Cisco Unified Serviceability create. When the amount of free dynamic memory is low, more memory gets automatically allocated, and total memory size (represented by the KbytesMemoryTotal counter) increases but only up to the maximum (represented by the KbytesMemoryMax counter). You can determine the amount of memory in use by subtracting KBytesMemoryFree from KbytesMemoryTotal.
KBytesMemoryMax	This counter represents the amount of free dynamic memory block (heap memory) in the Tomcat Java Virtual Machine. The dynamic memory block stores all objects that Tomcat and its web applications such as Cisco Unified CCX Administration and Cisco Unified Serviceability create.
KBytesMemoryTotal	This counter represents the current total dynamic memory block size, including free and in-use memory, of Tomcat Java Virtual Machine. The dynamic memory block stores all objects that Tomcat and its web applications such as Cisco Unified CCX Administration and Cisco Unified Serviceability create.

Cisco Tomcat Web Application

The Cisco Tomcat Web Application object provides information about how to run Unified CCX web applications. The URLs for the web application provide basis for the instance name for each Tomcat Web Application. For example, Cisco Unified CCX Administration (https://<IP Address>:8443/appadmin) gets identified by appadmin, Cisco Unified Serviceability gets identified by ccmservice, Unified CCX Serviceability gets identified by uccxservice, and URLs that do not have an extension, such as https://<IP Address>:8443 or http://<IP Address>:8080), get identified by _root. Table A-3 contains information on the Tomcat Web Application counters.

Table A-3 Tomcat Web Application

Counters	Counter Description
Errors	This counter represents the total number of HTTP errors (for example, 401 Unauthorized) that a Unified CCX-related web application encountered. The URLs for the web application provide the basis instance name for each Tomcat Web Application. For example, Unified CCX Administration (https://<IP Address>:8443/appadmin) gets identified by appadmin, Cisco Unified Serviceability gets identified by ccmservice, Unified CCX Serviceability gets identified by uccxservice, and URLs that do not have an extension, such as https://<IP Address>:8443 or http://<IP Address>:8080), get identified by _root.
Requests	This counter represents the total number of requests that the web application handles. Each time that a web application is accessed, its Requests counter increments accordingly. The URLs for the web application provide the basis instance name for each Tomcat Web Application. For example, Unified CCX Administration (https://<IP Address>:8443/appadmin) gets identified by appadmin, Cisco Unified Serviceability gets identified by ccmservice, Unified CCX Serviceability gets identified by uccxservice, and URLs that do not have an extension, such as https://<IP Address>:8443 or http://<IP Address>:8080), get identified by _root.
SessionsActive	This counter represents the number of sessions that the web application currently has active (in use). The URLs for the web application provide the basis instance name for each Tomcat Web Application. For example, Unified CCX Administration (https://<IP Address>:8443/appadmin) gets identified by appadmin, Cisco Unified Serviceability gets identified by ccmservice, Unified CCX Serviceability gets identified by uccxservice, and URLs that do not have an extension, such as https://<IP Address>:8443 or http://<IP Address>:8080), get identified by _root.

Database Change Notification Client

The Database Change Notification Client object provides information on change notification clients. Table A-4 contains information on the Database Change Notification Client counters.

Table A-4 Database Change Notification Client

Counters	Counter Descriptions
MessagesProcessed	This counter represents the number of database change notifications that have been processed. This counter refreshes every 15 seconds.
MessagesProcessing	This counter represents the number of change notification messages that are currently being processed or are waiting to be processed in the change notification queue for this client. This counter refreshes every 15 seconds.
QueueHeadPointer	This counter represents the head pointer to the change notification queue. The head pointer acts as the starting point in the change notification queue. To determine the number of notifications in the queue, subtract the head pointer value from the tail pointer value. By default, this counter refreshes every 15 seconds.

Table A-4 Database Change Notification Client (continued)

Counters	Counter Descriptions
QueueMax	This counter represents the largest number of change notification messages that will be processed for this client. This counter remains cumulative since the last restart of the Cisco Database Layer Monitor service.
QueueTailPointer	This counter represents the tail pointer to the change notification queue. The tail pointer represents the ending point in the change notification queue. To determine the number of notifications in the queue, subtract the head pointer value from the tail pointer value. By default, this counter refreshes every 15 seconds
TablesSubscribed	This counter represents the number of tables in which this client has subscribed.

Database Change Notification Server

The Database Change Notification Server object provides information on different change-notification-related statistics. Table A-5 contains information on the Database Change Notification Server counters.

Table A-5 Database Change Notification Server

Counter	Counter Descriptions
Clients	This counter represents the number of change notification clients (services/servlets) that have subscribed for change notification.
Queue Delay	This counter provides the number of seconds that the change notification process has messages to process but is not processing them. This condition is true if: • either Change Notification Requests Queued in Database (QueuedRequestsInDB) and Change Notification Requests Queued in Memory (QueuedRequestsInMemory) are non-zero, or • the Latest Change Notification Messages Processed count is not changing. This condition gets checked every 15 seconds.
QueuedRequestsInDB	This counter represents the number of change notification records that are in the DBCNQueue (Database Change Notification Queue) table via direct TCP/IP connection (not queued in shared memory). This counter refreshes every 15 seconds.
QueuedRequestsInMemory	This counter represents the number of change notification requests that are queued in shared memory.

Database Change Notification Subscription

The Database Change Notification Subscription object displays the names of tables where the client will receive Change Notifications.

The SubscribedTable object displays the table with the service or servlet that will receive change notifications. Because the counter does not increment, this display occurs for informational purposes only.

Database Local DSN

The Database Local Data Source Name (DSN) object and LocalDSN counter provide the DSN information for the local machine. Table A-6 contains information on the Database local DSN.

Table A-6 Database Local Data Source Name

Counters	Counter Descriptions
CcmDbSpace_Used	This counter represents the amount of Ccm DbSpace that is being consumed
CcmtempDbSpace_Used	This counter represents the amount of Ccmtemp DbSpace that is being consumed.
CNDbSpace_Used	This counter represents the percentage of CN dbspace consumed.
LocalDSN	This counter represents the data source name (DSN) that is being referenced from the local machine.
SharedMemory_Free	This counter represents total shared memory that is free.
SharedMemory_Used	This counter total shared memory that is used.
RootDbSpace_Used	This counter represents the amount of RootDbSpace that is being consumed.

DB User Host Information Counters

The DB User Host Information object provides information on DB User Host.

The DB:User:Host Instance object displays the number of connections that are present for each instance of DB:User:Host.

Enterprise Replication DBSpace Monitors

The enterprise replication DBSpace monitors object displays the usage of various ER DbSpaces. Table A-7 contains information on the enterprise replication DB monitors.

Table A-7 Enterprise Replication DBSpace Monitors

Counters	Counter Descriptions
ERDbSpace_Used	This counter represents the amount of enterprise replication DbSpace that was consumed.
ERSBDbSpace_Used	This counter represents the amount of ERDbSpace that was consumed.

Enterprise Replication Perfmon Counters

The Enterprise Replication Perfmon Counter object provides information on the various replication counters.

The ServerName:ReplicationQueueDepth counter displays the server name followed by the replication queue depth.

IP

The IP object provides information on the IPv4-related statistics on your system. Table A-8 contains information on the IP counters.

Table A-8 IP

Counters	Counter Descriptions
Frag Creates	This counter represents the number of IP datagrams fragments that have been generated at this entity.
Frag Fails	This counter represents the number of IP datagrams that were discarded at this entity because the datagrams could not be fragmented, such as datagrams where the Do not Fragment flag was set.
Frag OKs	This counter represents the number of IP datagrams that were successfully fragmented at this entity.
In Delivers	This counter represents the number of input datagrams that were delivered to IP user protocols. This includes Internet Control Message Protocol (ICMP).
In Discards	This counter represents the number of input IP datagrams where no problems were encountered, but which were discarded. Lack of buffer space provides one possible reason. This counter does not include any datagrams that were discarded while awaiting reassembly.
In HdrErrors	This counter represents the number of input datagrams that were discarded with header errors. This includes bad checksums, version number mismatch, other format errors, time-to-live exceeded, and other errors that were discovered in processing their IP options.
In Receives	This counter represents the number of input datagrams that were received from all network interfaces. This counter includes datagrams that were received with errors
In UnknownProtos	This counter represents the number of locally addressed datagrams that were received successfully but discarded because of an unknown or unsupported protocol.
InOut Requests	This counter represents the number of incoming IP datagrams that were received and the number of outgoing IP datagrams that were sent.
Out Discards	This counter represents the number of output IP datagrams that were not transmitted and were discarded. Lack of buffer space provides one possible reason.
Out Requests	This counter represents the total number of IP datagrams that local IP user-protocols (including ICMP) supply to IP in requests transmission. This counter does not include any datagrams that were counted in ForwDatagrams.

Table A-8 IP (continued)

Counters	Counter Descriptions
Reasm Fails	This counter represents the number of IP reassembly failures that the IP reassembly algorithm detected, including time outs, errors, and so on. This counter does not represent the discarded IP fragments because some algorithms, such as the algorithm in RFC 815, can lose track of the number of fragments because it combines them as they are received.
Reasm OKs	This counter represents the number of IP datagrams that were successfully reassembled.
Reasm Reqds	This counter represents the number of IP fragments that were received that required reassembly at this entity.

IP6

The IP6 object, which supports Unified CCX, provides information on the IPv6-related statistics on your system. Table A-9 contains information on the IP counters.

Table A-9 IP6

Counters	Counter Descriptions
Frag Creates	This counter represents the number of IP datagrams fragments that have been generated as a result of fragmentation at this entity.
Frag Fails	This counter represents the number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not, for example because their Do not Fragment flag was set.
Frag OKs	This counter represents the number of IP datagrams that have been successfully fragmented at this entity.
In Delivers	This counter represents the total number of input datagrams successfully delivered to IP user-protocols (including Internet Control Message Protocol [ICMP]).
In Discards	This counter represents the number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). This counter does not include any datagrams that were discarded while awaiting reassembly.
In HdrErrors	This counter represents the number of input datagrams discarded due to errors in their IP header, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.
In Receives	This counter represents the number of input datagrams received from all network interfaces, including those received with errors.
In UnknownProtos	This counter represents the number of locally addressed datagrams that were received successfully but discarded because of an unknown or unsupported protocol.
InOut Requests	This counter represents the total number of IP datagrams received and the number of IP datagrams sent.

Table A-9 IP6 (continued)

Counters	Counter Descriptions
Out Discards	This counter represents the number of output IP datagrams that was not transmitted and was discarded. One reason may be a lack of buffer space.
Out Requests	This counter represents the total number of IP datagrams which local IP user-protocols (including Internet Control Message Protocol [ICMP]) supply to IP in requests transmission. This counter does not include any datagrams counted in ForwDatagrams.
Reasm Fails	This counter represents the number of failures detected by the IP reassembly algorithm (for various reasons, for example timed out, errors, and so on). This is not necessarily a count of discarded IP fragments since some algorithms, notably the algorithm in RFC 815, can lose track of the number of fragments by combining them as they are received.
Reasm OKs	This counter represents the number of IP datagrams that have been successfully reassembled.
Reasm Reqds	This counter represents the number of IP fragments received which needed to be reassembled at this entity.

Memory

The memory object provides information about the usage of physical memory and swap memory on the server. Table A-10 contains information on memory counters.

Table A-10 Memory

Counters	Counter Descriptions
% Mem Used	This counter displays the system physical memory utilization as a percentage. The value of this counter equals (Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes) / Total KBytes, which also corresponds to the Used KBytes/Total KBytes.
% Page Usage	This counter represents the percentage of active pages.
% VM Used	This counter displays the system virtual memory utilization as a percentage. The value of this counter equals (Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes + Used Swap KBytes) / (Total KBytes + Total Swap KBytes), which also corresponds to Used VM KBytes/Total VM KBytes.
Buffers KBytes	This counter represents the capacity of buffers in your system in kilobytes.
Cached KBytes	This counter represents the amount of cached memory in kilobytes.
Free KBytes	This counter represents the total amount of memory that is available in your system in kilobytes.
Free Swap KBytes	This counter represents the amount of free swap space that is available in your system in kilobytes.
Faults Per Sec	This counter represents the number of page faults (both major and minor) that the system made per second (post 2.5 kernels only). This does not necessarily represent a count of page faults that generate I/O because some page faults can get resolved without I/O.

Table A-10 Memory (continued)

Counters	Counter Descriptions
Low Total	This counter represents the total low (non-paged) memory for kernel.
Low Free	This counter represents the total free low (non-paged) memory for kernel.
Major Faults Per Sec	This counter represents the number of major faults that the system has made per second that have required loading a memory page from disk (post 2.5 kernels only).
Pages	This counter represents the number of pages that the system paged in from the disk plus the number of pages that the system paged out to the disk.
Pages Input	This counter represents the number of pages that the system paged in from the disk.
Pages Input Per Sec	This counter represents the total number of kilobytes that the system paged in from the disk per second.
Pages Output	This counter represents the number of pages that the system paged out to the disk.
Pages Output Per Sec	This counter represents the total number of kilobytes that the system paged out to the disk per second.
Shared KBytes	This counter represents the amount of shared memory in your system in kilobytes.
Total KBytes	This counter represents the total amount of memory in your system in kilobytes.
Total Swap KBytes	This counter represents the total amount of swap space in your system in kilobytes.
Total VM KBytes	This counter represents the total amount of system physical and memory and swap space (Total Kbytes + Total Swap Kbytes) that is in use in your system in kilobytes.
Used KBytes	This counter represents the amount of system physical memory that is in use on the system in kilobytes. The value of the Used KBytes counter equals Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes. The Used KBytes value differs from the Linux term that displays in the top or free command output. The Used value that displays in the top or free command output equals the difference in Total KBytes - Free KBytes and also includes the sum of Buffers KBytes and Cached KBytes.
Used Swap KBytes	This counter represents the amount of swap space that is in use on your system in kilobytes.
Used VM KBytes	This counter represents the system physical memory and the amount of swap space that is in use on your system in kilobytes. The value equals Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes + Used Swap KBytes. This corresponds to Used Mem KBytes + Used Swap KBytes.

Network Interface

The network interface object provides information about the network interfaces on the system. Table A-11 contains information on network interface counters.

Table A-11 Network Interface

Counters	Counter Descriptions
Rx Bytes	This counter represents the number of bytes, including framing characters, that were received on the interface.
Rx Dropped	This counter represents the number of inbound packets that were chosen to be discarded even though no errors had been detected. This prevents the packet from being delivered to a higher layer protocol. Discarding packets to free up buffer space provides one reason.
Rx Errors	This counter represents the number of inbound packets (packet-oriented interfaces) and the number of inbound transmission units (character-oriented or fixed-length interfaces) that contained errors that prevented them from being deliverable to a higher layer protocol.
Rx Multicast	This counter represents the number of multicast packets that were received on this interface.
Rx Packets	This counter represents the number of packets that this sublayer delivered to a higher sublayer. This does not include the packets that were addressed to a multicast or broadcast address at this sublayer.
Total Bytes	This counter represents the total number of received (Rx) bytes and transmitted (Tx) bytes.
Total Packets	This counter represents the total number of Rx packets and Tx packets.
Tx Bytes	This counter represents the total number of octets, including framing characters, that were transmitted out from the interface.
Tx Dropped	This counter represents the number of outbound packets that were chosen to be discarded even though no errors were detected. This action prevents the packet from being delivered to a higher layer protocol. Discarding a packet to free up buffer space represents one reason.
Tx Errors	This counter represents the number of outbound packets (packet-oriented interfaces) and the number of outbound transmission units (character-oriented or fixed-length interfaces) that could not be transmitted because of errors.
Tx Packets	This counter represents the total number of packets that the higher level protocols requested for transmission, including those that were discarded or not sent. This does not include packets that were addressed to a multicast or broadcast address at this sublayer.
Tx QueueLen	This counter represents the length of the output packet queue (in packets).

Number of Replicates Created and State of Replication

The Number of Replicates Created and State of Replication object provides real-time replication information for the system. Table A-12 contains information on replication counters.

Table A-12 Number of Replicates Created and State of Replication

Counters	Counter Descriptions
Number of Replicates Created	This counter displays the number of replicates that were created by Informix for the DB tables. This counter displays information during Replication Setup.
Replicate_State	This counter represents the state of replication. The following list provides possible values: • 0—Initializing. The counter equals 0 when the server is not defined *or* when the server is defined but realizes the template has not completed. • 1—Replication setup script fired from this node. Cisco recommends that you run utils dbreplication status on the CLI to determine the location and cause of the failure. • 2—Good Replication. • 3—Bad Replication. A counter value of 3 indicates replication in the cluster is bad. It does not mean that replication failed on a particular server in the cluster. Cisco recommends that you run utils dbreplication status on the CLI to determine the location and cause of the failure. • 4—Replication setup did not succeed.

Partition

The partition object provides information about the file system and its usage in the system. Table A-13 contains information on partition counters. These counters are also available for the spare partition, if present.

Table A-13 Partition

Counters	Counter Descriptions
% CPU Time	This counter represents the percentage of CPU time that is dedicated to handling I/O requests that were issued to the disk. This counter is no longer valid with the counter value -1.
% Used	This counter represents the percentage of disk space that is in use on this file system.
% Wait in Read	Not Used. The Await Read Time counter replaces this counter. This counter is no longer valid with the counter value -1.
% Wait in Write	Not Used. The Await Write Time counter replaces this counter. This counter is no longer valid with the counter value -1.
Await Read Time	This counter represents the average time, measured in milliseconds, for Read requests that are issued to the device to be served. This counter is no longer valid with the counter value -1.

Table A-13 Partition (continued)

Counters	Counter Descriptions
Await Time	This counter represents the average time, measured in milliseconds, for I/O requests that were issued to the device to be served. This includes the time that the requests spent in queue and the time that was spent servicing them.This counter is no longer valid with the counter value -1.
Await Write Time	This counter represents the average time, measured in milliseconds, for write requests that are issued to the device to be served. This counter is no longer valid with the counter value -1.
Queue Length	This counter represents the average queue length for the requests that were issued to the disk. This counter is no longer valid with the counter value -1.
Read Bytes Per Sec	This counter represents the amount of data in bytes per second that was read from the disk.
Total Mbytes	This counter represents the amount of total disk space in megabytes that is on this file system.
Used Mbytes	This counter represents the amount of disk space in megabytes that is in use on this file system.
Write Bytes Per Sec	This counter represents the amount of data that was written to the disk in bytes per second.

Process

The process object provides information about the processes that are running on the system. Table A-14 contains information on process counters.

Table A-14 Process

Counters	Counter Descriptions
% CPU Time	This counter, which is expressed as a percentage of total CPU time, represents the tasks share of the elapsed CPU time since the last update.
% MemoryUsage	This counter represents the percentage of physical memory that a task is currently using.
Data Stack Size	This counter represents the stack size for task memory status.
Nice	This counter represents the nice value of the task. A negative nice value indicates that the process has a higher priority while a positive nice value indicates that the process has a lower priority. If the nice value equals zero, do not adjust the priority when you are determining the dispatchability of a task.
Page Fault Count	This counter represents the number of major page faults that a task encountered that required the data to be loaded into memory.
PID	This counter displays the task-unique process ID. The ID periodically wraps, but the value will never equal zero.

Table A-14 Process (continued)

Counters	Counter Descriptions
Process Status	This counter displays the process status: • 0—Running • 1—Sleeping • 2—Uninterruptible disk sleep • 3—Zombie • 4—Stopped • 5— Paging • 6—Unknown
Shared Memory Size	This counter displays the amount of shared memory (KB) that a task is using. Other processes could potentially share the same memory.
STime	This counter displays the system time (STime), measured in jiffies, that this process has scheduled in kernel mode. A jiffy corresponds to a unit of CPU time and gets used as a base of measurement. One second comprises 100 jiffies.
Thread Count	This counter displays the number of threads that are currently grouped with a task. A negative value (-1) indicates that this counter is currently not available. This happens when thread statistics (which includes all performance counters in the Thread object as well as the Thread Count counter in the Process object) are turned off because the system total processes and threads exceeded the default threshold value.
Total CPU Time Used	This counter displays the total CPU time in jiffies that the task used in user mode and kernel mode since the start of the task. A jiffy corresponds to a unit of CPU time and gets used as a base of measurement. One second comprises 100 jiffies.
UTime	This counter displays the time, measured in jiffies, that a task has scheduled in user mode.
VmData	This counter displays the virtual memory usage of the heap for the task in kilobytes (KB).
VmRSS	This counter displays the virtual memory (Vm) resident set size (RSS) that is currently in physical memory in kilobytes (KB). This includes the code, data, and stack.
VmSize	This counter displays the total virtual memory usage for a task in kilobytes (KB). It includes all code, data, shared libraries, and pages that have been swapped out: Virtual Image = swapped size + resident size.
Wchan	This counter displays the channel (system call) in which the process is waiting.

Processor

The processor object provides information on different processor time usage in percentages. Table A-15 contains information on processor counters.

Table A-15 Processor

Counters	Counter Descriptions
% CPU Time	This counter displays the processors share of the elapsed CPU time, excluding idle time, since the last update. This share gets expressed as a percentage of total CPU time.
Idle Percentage	This counter displays the percentage of time that the processor is in the idle state and did not have an outstanding disk I/O request.
IOwait Percentage	This counter represents the percentage of time that the processor is in the idle state while the system had an outstanding disk I/O request.
Irq Percentage	This counter represents the percentage of time that the processor spends executing the interrupt request that is assigned to devices, including the time that the processor spends sending a signal to the computer.
Nice Percentage	This counter displays the percentage of time that the processor spends executing at the user level with nice priority.
Softirq Percentage	This counter represents the percentage of time that the processor spends executing the soft IRQ and deferring task switching to get better CPU performance.
System Percentage	This counter displays the percentage of time that the processor is executing processes in system (kernel) level.
User Percentage	This counter displays the percentage of time that the processor is executing normal processes in user (application) level.

System

The System object provides information on file descriptors on your system. Table A-16 contains information on system counters.

Table A-16 System

Counters	Counter Descriptions
Allocated FDs	This counter represents the total number of allocated file descriptors.
Being Used FDs	This counter represents the number of file descriptors that are currently in use in the system.
Freed FDs	This counter represents the total number of allocated file descriptors on the system that are freed.
Max FDs	This counter represents the maximum number of file descriptors that are allowed on the system.
Total CPU Time	This counter represents the total time in jiffies that the system has been up and running.

Table A-16 System (continued)

Counters	Counter Descriptions
Total Processes	This counter represents the total number of processes on the system.
Total Threads	This counter represents the total number of threads on the system.

TCP

The TCP object provides information on the TCP statistics on your system. Table A-17 contains information on the TCP counters.

Table A-17 TCP

Counters	Counter Description
Active Opens	This counter displays the number of times that the TCP connections made a direct transition to the SYN-SENT state from the CLOSED state.
Attempt Fails	This counter displays the number of times that the TCP connections have made a direct transition to the CLOSED state from either the SYN-RCVD state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYS-RCVD state.
Curr Estab	This counter displays the number of TCP connections where the current state is either ESTABLISHED or CLOSE- WAIT.
Estab Resets	This counter displays the number of times that the TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
In Segs	This counter displays the total number of segments that were received, including those received in error. This count only includes segments that are received on currently established connections.
InOut Segs	This counter displays the total number of segments that were sent and the total number of segments that were received.
Out Segs	This counter displays the total number of segments that were sent. This count only includes segments that are sent on currently established connections, but excludes retransmitted octets.
Passive Opens	This counter displays the number of times that TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
RetransSegs	This counter displays the total number of segments that were retransmitted because the segment contains one or more previously transmitted octets.

Thread

The Thread object provides a list of running threads on your system. Table A-18 contains information on the Thread counters.

Table A-18 Thread

Counters	Counter Description
% CPU Time	This counter displays the threads share of the elapsed CPU time since the last update. This counter expresses the share as a percentage of the total CPU time.
PID	This counter displays the threads leader process ID.

Where to Find More Information

- Understanding Performance Monitoring
- Working with Performance Queries

APPENDIX **B**

Performance Objects and Counters for Unified CCX

This appendix provides information on Unified CCX-related objects and counters. For information on specific counters, click the blue text in the following list to go to the object:

- Unified CCX DB Monitors, page B-2
- Unified CCX Engine JVM Heap, page B-2

Tip For the latest performance monitoring counters, objects, and counter descriptions that are available for Unified CCX, access the performance monitoring counters in the Cisco Unified Real-Time Monitoring Tool. In RTMT, you can review a counter description, as described in the "Using Performance Queries to Add a Counter" section on page 5-3.

Unified CCX DB Monitors

The Unified CCX DB Monitors object provides information about the space used by Unified CCX datastores. Table B-1 contains information about Unified CCX DB Monitors counters.

Table B-1 Unified CCX DB Monitors

Counters	Counter Description
DB CRA % Space Used	This counter represents the amount (%) of space used by Unified CCX Configuration Data.
DB CRA REPOSITORY % Space Used	This counter represents the amount (%) of space used by Unified CCX Repository.
FcrAsSvr % Space Used	This counter represents the amount (%) of space used by Unified CCX Frascal.

Unified CCX Engine JVM Heap

The Unified CCX Engine JVM Heap object provides information about heap usage of the Unified CCX Engine. Table B-2 contains information about Unified CCX Engine JVM Heap counters.

Table B-2 Unified CCX Engine JVM Heap

Counters	Counter Description
KBytesMemoryCommitted	This counter represents the amount of memory in Kbytes that is committed for the Engine JVM to use. This amount of memory is guaranteed for the JVM to use.
KBytesMemoryMax	This counter represents the amount of memory in bytes that can be used by Engine JVM. Based on the availability of System memory, the JVM may fail to allocate memory even if the amount of used memory does not exceed this maximum size.
KBytesMemoryUsed	This counter represents the amount of memory currently in use by the JVM.
PercentageMemoryUsedAfterGC	This counter represents the percentage of heap memory that is used by the application after the last full Garbage Collection cycle.

Where to Find More Information

Related Topics

- Understanding Performance Monitoring
- Working with Performance Queries

APPENDIX C

System Alert Descriptions and Default Configurations

The following list comprises the system alerts, their definitions, and default settings.

AuthenticationFailed

Authentication validates the user ID and password that are submitted during log in. An alarm gets raised when an invalid user ID and/or the password gets used.

Default Configuration

Table C-1 Default Configuration for the AuthenticationFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Number of AuthenticationFailed events exceeds: 1 time in the last 1 minute
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CiscoDRFFailure

This alert occurs when the DRF backup or restore process encounters errors.

Default Configuration

Table C-2 Default Configuration for the CiscoDRFFailure RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CiscoDRFFailure event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Table C-2 Default Configuration for the CiscoDRFFailure RTMT Alert (continued)

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

CoreDumpFileFound

This alert occurs when the CoreDumpFileFound event gets generated. This indicates that a core dump file exists in the system.

Default Configuration

Table C-3 Default Configuration for the CoreDumpFileFound RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CoreDumpFileFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Trace download Parameters	Not Selected
Enable Email	Selected
Trigger Alert Action	Default

CpuPegging

CPU usage gets monitored based on configured thresholds. If the usage goes above the configured threshold, this alert gets generated.

Default Configuration

Table C-4 Default Configuration for the CpuPegging RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: 99%
Duration	Trigger alert only when value constantly below or over threshold for 60 seconds
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CriticalServiceDown

The CriticalServiceDown alert gets generated when the service status equals down (not for other states).

Default Configuration

Table C-5 Default Configuration for the CriticalServiceDown RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Service status is DOWN
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Trace download Parameters	Enable Trace Download not selected
Enable Email	Selected
Trigger Alert Action	Default

HardwareFailure

This alert occurs when a hardware failure event (disk drive failure, power supply failure, and others) has occurred.

Default Configuration

Table C-6 Default Configuration for the HardwareFailure RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: HardwareFailure event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LogFileSearchStringFound

This alert occurs when the LogFileSearchStringFound event gets generated. This indicates that the search string was found in the log file.

Default Configuration

Table C-7 Default Configuration for the LogFileSearchStringFound RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: LogFileSearchStringFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Table C-7 Default Configuration for the LogFileSearchStringFound RTMT Alert (continued)

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

LogPartitionHighWaterMarkExceeded

This alert occurs when the percentage of used disk space in the log partition exceeds the configured high water mark. When this alert gets generated, LPM deletes files in the log partition (down to low water mark) to avoid running out of disk space.

Note LPM may delete files that you want to keep. You should act immediately when you receive the LogPartitionLowWaterMarkExceeded alert.

Default Configuration

Table C-8 Default Configuration for the LogPartitionHighWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Log Partition Used Disk Space Exceeds High Water Mark (95%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LogPartitionLowWaterMarkExceeded

This alert occurs when the LogPartitionLowWaterMarkExceeded event gets generated. This indicates that the percentage of used disk space in the log partition has exceeded the configured low water mark.

Note Be aware that this alert is an early warning. The administrator should start freeing up disk space. Using RTMT/TLC, you can collect trace/log files and delete them from the server. The administrator should adjust the number of trace files that are kept to avoid hitting the low water mark again.

Default Configuration

Table C-9 Default Configuration for the LogPartitionLowWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Log Partition Used Disk Space Exceeds Low Water Mark (95%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LowActivePartitionAvailableDiskSpace

This alert occurs when the percentage of available disk space on the active partition is lower than the configured value.

Default Configuration

Table C-10 Default Configuration for the LowActivePartitionAvailableDiskSpace RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Active Partition available diskspace below (4%)
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LowAvailableVirtualMemory

RTMT monitors virtual memory usage. When memory runs low, a LowAvailableVirtualMemory alert gets generated.

Default Configuration

Table C-11 Default Configuration for the LowAvailableVirtualMemory RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Available virtual memory below (30%)
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LowInactivePartitionAvailableDiskSpace

This alert occurs when the percentage of available disk space of the inactive partition equals less than the configured value.

Default Configuration

Table C-12 Default Configuration for the LowInactivePartitionAvailableDiskSpace RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Inactive Partition available disk space below (4%)
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily

Table C-12 Default Configuration for the LowInactivePartitionAvailableDiskSpace RTMT Alert

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

LowSwapPartitionAvailableDiskSpace

This alert indicates that the available disk space on the swap partition is low.

Note The swap partition is part of virtual memory, so low available swap partition disk space means low virtual memory as well.

Default Configuration

Table C-13 Default Configuration for the LowSwapPartitionAvailableDiskSpace RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Swap Partition available disk space below (105)
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ServerDown

This alert occurs when a remote node cannot be reached.

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

Default Configuration

Table C-14 Default Configuration for the ServerDown RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: ServerDown occurred
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SparePartitionHighWaterMarkExceeded

This alert occurs when the SparePartitionHighWaterMarkExceeded event gets generated. This indicates that the percentage of used disk space in the spare partition exceeds the configured high water mark.

Default Configuration

Table C-15 Default Configuration for the SparePartitionHighWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Spare Partition Used Disk Space Exceeds High Water Mark (95%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SparePartitionLowWaterMarkExceeded

This alert occurs when the SparePartitionLowWaterMarkExceeded event gets generated. This indicates that the percentage of used disk space in the spare partition has exceeded the low water mark threshold.

Default Configuration

Table C-16 Default Configuration for the SparePartitionLowWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Spare Partition Used Disk Space Exceeds Low Water Mark (90%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SyslogSeverityMatchFound

This alert occurs when the SyslogSeverityMatchFound event gets generated. This indicates that a syslog message with the matching severity level exists.

Default Configuration

Table C-17 Default Configuration for the SyslogSeverityMatchFound RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SyslogSeverityMatchFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Table C-17 Default Configuration for the SyslogSeverityMatchFound RTMT Alert (continued)

Value	Default Configuration
Syslog Severity Parameters	Critical
Enable Email	Selected
Trigger Alert Action	Default

SyslogStringMatchFound

This alert occurs when the SyslogStringMatchFound event gets generated. The alert indicates that a syslog message with the matching search string exists.

Default Configuration

Table C-18 Default Configuration for the SyslogStringMatchFound RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SyslogStringMatchFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Syslog Alert Parameters	(Text box for search string)
Enable Email	Selected
Trigger Alert Action	Default

SystemVersionMismatched

This alert occurs when a mismatch in system version exists.

Default Configuration

Table C-19 Default Configuration for the SystemVersionMismatched RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SystemVersionMismatched occurred
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

TotalProcessesAndThreadsExceededThreshold

This alert occurs when the TotalProcessesAndThreadsExceededThreshold event gets generated. The alert indicates that the current total number of processes and threads exceeds the maximum number of tasks that are configured for the Cisco RIS Data Collector Service Parameter. This situation could indicate that a process is leaking or that a process has thread leaking.

Default Configuration

Table C-20 Default Configuration for the TotalProcessesAndThreadsExceededThreshold RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: TotalProcessesAndThreadsExceededThreshold event generated
Duration	Trigger alert immediately

Table C-20 Default Configuration for the TotalProcessesAndThreadsExceededThreshold RTMT Alert (continued)

Value	Default Configuration
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

APPENDIX D

Cisco Unified Contact Center Express Alert Descriptions and Default Configurations

The following list comprises the Cisco Unified Contact Center Express alerts, their definitions, and default settings.

DB CRA % Space Used

This alert occurs when the DB CRA % Space Used event gets generated. This indicates the percentage of used space in the Cisco Unified Contact Center Express database, db_cra. The database, db_cra, contains the Cisco Unified Contact Center Express historical and configuration data.

Default Configuration

Table D-1 Default Configuration for the DB CRA % Space Used RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition meet: Percentage of the used DB space is above the configured threshold (80%).
Frequency	Trigger up to 3 alerts within 30 minutes.
Schedule	Trigger alert when it occurs. (Non-Stop Monitoring)
Enable Email	Selected
Trigger Alert Action	Default
Recommended Action	Purge data using the manual purge process to reclaim space.

DBReplicationStopped

This alert occurs when the Cisco Unified Contact Center Express Database Replication is removed, which typically happens when the replication queues become full due to the inability to contact the other node.

Default Configuration

Table D-2 Default Configuration for the DBReplicationStopped RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Not Applicable
Frequency	Trigger alert on every poll
Schedule	Trigger alert when it occurs. (Non-Stop Monitoring)

Table D-2 Default Configuration for the DBReplicationStopped RTMT Alert (continued)

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default
Recommended Action	The User should go to the Data Control Center page and re-esablish the replication setup using 'reset replication.'

HistoricalDataWrittenToFiles

This alert gets raised when the historical data has not been written to the Cisco Unified Contact Center Express database but has been written to the file system. You should verify the state of the Cisco Unified Contact Center Express database.

Default Configuration

Table D-3 Default Configuration for the HistoricalDataWrittenToFiles RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Not Applicable
Frequency	Trigger alert on every poll
Schedule	Trigger alert when it occurs. (Non-Stop Monitoring)
Enable Email	Selected
Trigger Alert Action	Default
Recommended Action	Go to Cisco Unified Contact Center Express Administration, and initiate the loading of data from the File System.

PurgeInvoked

This alert gets raised when the Cisco Unified Contact Center Express Auto Purging has completed.

Default Configuration

Table D-4 Default Configuration for the PurgeInvoked RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Informational
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Not Applicable
Frequency	Trigger alert on every poll
Schedule	Trigger alert when it occurs. (Non-Stop Monitoring)
Enable Email	Selected
Trigger Alert Action	Default
Recommended Action	No actions needed.

UnifiedCCXEngineMemoryUsageHigh

This alert occurs when the percentage of JVM heap memory used by Cisco Unified Contact Center Express Engine process is greater than the configured threshold value.

Default Configuration

Table D-5 Default Configuration for the UnifiedCCXEngineMemoryUsageHigh RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Cisco Unified Contact Center Express Engine heap memory usage crossed the configured threshold (70%).
Frequency	Trigger up to one alert within 30 minutes.
Schedule	Trigger alert when it occurs. (Non-Stop Monitoring)
Enable Email	Selected

Table D-5 Default Configuration for the UnifiedCCXEngineMemoryUsageHigh RTMT Alert

Value	Default Configuration
Trigger Alert Action	Default
Recommended Action	Monitor system call load.

Additional Information

See the Related Topics, page 7-8.

INDEX

A

B

C

D

E

I

L

M

N

O

P

R

S

T

U

Z