CHAPTER 11

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 11-33.

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 11-2.

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:

Note Cisco Unified Serviceability supports only these options on Windows servers: Collect Files and Schedule Collection.

- 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 11-3
- 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 11-8

- 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 11-12
- Collect a crash dump file for one or more servers on your network. See "Collecting a Crash Dump" section on page 11-16.
- 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 11-19.
- View the trace files that you have collected. See the "Using Local Browse" section on page 11-22.
- View all of the trace files on the server. See the "Using Remote Browse" section on page 11-23.
- 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 11-28.

Additional Information

- See Related Topics, page 11-33.

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 11-8.

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.

Trace Compression Support

This feature enables the ROS (Recoverable Outstream) library to support the compressed output of tracefiles. The files get compressed as they are being generated. The benefits of tracefile compression include

- Reduces the capacity that is required to store tracefiles.
- Reduces the disk head movement, which results in significantly improved disk I/O wait. This may prove of value when tracefile demand is high.

Use the enterprise parameter, Trace Compression, to enable or disable trace compression. The default value for this parameter specifies Disabled. For information on setting the values of enterprise parameters, see the "Enterprise Parameters Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Caution Compressing files adds additional CPU cycles. Enabling the Trace Compression enterprise parameter can negatively impact overall call throughput by as much as 10 percent.

You can recognize compressed files by their .gz extension (.gzo if the file is still being written to). To open a compressed file, double click the file name, and the file opens in the log viewer.

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, refer to *Cisco Unified Serviceability Administration Guide*.
- 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. For more information, refer to *Cisco Unified Serviceability Administration Guide*.
- 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). For more information on configuring service parameters, refer to the *Cisco Unified Communications Manager Administration Guide.*
- Optionally, enable trace compression by setting the value of the Trace Compression enterprise parameter to Enabled. For more information on configuring enterprise parameters, refer to the *Cisco Unified Communications Manager Administration Guide.*

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 11-2.

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 *Unified CM clusters and Connection clusters only:* 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 Unified *CM clusters and Connection clusters only:* 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 3 *Connection* users go to Step 4. For *Unified CM* or *Unified CM BE*, perform one of the following actions in the Select CCM Services/Application tab:

- To collect traces for all services and applications 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 all service and applications for your standalone server.

- To collect traces for all services and applications on a particular server (or for particular system logs on the server for Connection), 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 go to the next tab without collecting traces for services or applications, click **Next**.

Go to Step 4 for *Unified CM BE* or go to Step 5 for *Unified CM*.

Step 4 In the Select CUC 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.** *Connection* users go to Step 6.

Step 5 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 6 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.

Note RTMT returns logs of a different timestamp, than that configured through the wizard. This occurs specifically, when the specified timestamp is lesser than that of the existing log files. For example:
Log files exist on the server for a specific service from 11/24/09, and you have given the time range from 11/23/09 5:50 to 11/23/09 7:50; RTMT still returns the existing log files.

Step 7 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 Cisco Unified Communications Manager, Cisco Unified Communications Manager Business Edition, or Cisco Unity Connection 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 Cisco Unified Communications Manager or Cisco Unity Connection versions that ran on the Windows platform.

Step 8 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 9 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 10 To delete collected log files from the server, check the **Delete Collected Log Files from the server** check box.

Step 11 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 12 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 11-22.

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

Additional Information

- For more information about setting the values of enterprise parameters, see the "Enterprise Parameters Configuration" chapter, *Cisco Unified Communications Manager Administration Guide*
- For information about setting the values of service parameters, see the "Service Parameters Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide.*
- Also see Related Topics, page 11-33.

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*.
- 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*.

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 11-2.

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 22. 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 Cisco Unified Communications Manager 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 *Connection* users go to Step 8. For *Unified CM* or *Unified CM BE*, choose the services and application logs in which you are interested by checking all check boxes that apply in the Select CallManager Services/Applications tab.

Step 7 Click **Next**. *Unified CM* users go to Step 10.

Step 8 In the Select CUC Services/Application tab, choose the services and application logs in which you are interested by checking all check boxes that apply.

Step 9 Click **Next**.

Step 10 In the Select System Logs tab, choose the logs in which you are interested by checking all check boxes that apply.

Step 11 Click **Next**.

Step 12 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 13 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 14 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 15 Click **Next**.

Step 16 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 Trace Download Configuration dialog box displays. In the dialog box, you can configure the following parameters:
  - Host IP Address
  - User Name
  - Password
  - Port
  - Download Directory Path

Note You can choose **Localhost** download option when downloading traces. This option is available only for Cisco Intercompany Media Engine servers.
If you download trace files to the local host directories on the Cisco Intercompany Media Engine server, you can offload the files to a remote SFTP server by using the **file get** CLI command.

Note FTP is not supported for Cisco Intercompany Media Engine.

Step 17 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 22.
- To save the query, click the **Save Query** button and continue with Step 18.
- 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 11-22.

Step 18 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 servers by default:

  - For Cisco Unified Communications Manager clusters, the trace collection tool chooses all the servers in the cluster by default when you execute the query.
  - For Cisco Unified Communications Manager Business Edition, the trace collection tool chooses the server on which you created the query when you executed the query.
  - For Cisco Unity Connection, 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 19 Click **Finish**.

Step 20 Browse to the location to store the query, enter a name for the query in the File Name field, and click **Save**.

Step 21 Do one of the following tasks:

- To run the query that you have just saved, click **Run Query** and continue with Step 22.
- To exit the query wizard without running the query that you created, click **Cancel**.

Step 22 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.

Note *Unified CM and Unified CM BE only:* To view reports that the QRT Quality Report Tool (QRT) generates, see the "Displaying QRT Report Information" section on page 11-27.

- 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 11-22.

- To save the query, click **Save Query** button and complete Step 18 through Step 20.

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 11-33.

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*.
- 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*.

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 11-2.

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 *Unified CM clusters and Connection clusters only:* 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 *Unified CM clusters and Connection clusters only:* You can install some 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 3 *Connection* users go to Step 4. For *Unified CM* or *Unified CM BE*, perform one of the following actions in the Select CCM Services/Application tab:

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.**

Go to Step 4 for *Unified CM BE* or go to Step 5 for *Unified CM*.

Step 4 In the Select CUC 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 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 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 6 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 7 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 8 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 9 From the Scheduler Frequency drop-down list box, choose how often you want to run the configured trace collection.

Step 10 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 11 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 12 To create a zip file of the trace files that you collect, check the **Zip File** check box.

Step 13 To delete collected log files from the server, check the **Delete Collected Log Files from the Server** check box.

Step 14 Choose one or more of the following actions:

- Download Files. If you chose Download Files or Run Another Query, continue with Step 15.
- Run Another Query
- Generate Syslog. If you chose Generate Syslog, go to Step 17.

Step 15 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.

Note You can choose **Localhost** download option when downloading traces. This option is available only for Cisco Intercompany Media Engine servers.
If you download trace files to the local host directories on the Cisco Intercompany Media Engine server, you can offload the files to a remote SFTP server by using the **file get** CLI command.

Note FTP is not supported for Cisco Intercompany Media Engine.

Step 16 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 17 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 18 Click **OK**.

Step 19 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 11-33.

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 11-2.

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 11-33.

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 11-2.

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 *Unified CM clusters and Connection clusters only:* 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 *Unified CM clusters and Connection clusters only:* 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 3 *Connection* users go to Step 4. For *Unified CM* or *Unified CM BE*, perform one of the following actions in the Select CCM Services/Application tab:

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**.

Go to Step 4 for *Unified CM BE* or go to Step 5 for *Unified CM*.

Step 4 In the Select CUC 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 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 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 6 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 7 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 Cisco Unified Communications Manager, Cisco Unified Communications Manager Business Edition, or Cisco Unity Connection 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 Cisco Unified Communications Manager and Cisco Unity Connection versions that ran on the Windows platform.

Step 8 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 9 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 10 To delete collected crash dump files from the server, check the **Delete Collected Log Files from Server** check box.

Step 11 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 11-33.

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 11-2.

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.

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

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 Trace Download Configuration 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.

Note You can choose **Localhost** download option when downloading traces. This option is available only for Cisco Intercompany Media Engine servers.
If you download trace files to the local host directories on the Cisco Intercompany Media Engine server, you can offload the files to a remote SFTP server by using the **file get** CLI command.

Note FTP is not supported for Cisco Intercompany Media Engine.

Additional Information

See the Related Topics, page 11-33.

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 11-3
- “Using the Query Wizard” section on page 11-8
- “Scheduling Trace Collection” section on page 11-12

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 11-2.

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.

Unified CM and Unified CM BE only: For more information on using the QRT Viewer, see the "Displaying QRT Report Information" section on page 11-27.

Additional Information

See the Related Topics, page 11-33.

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 11-3
- "Using the Query Wizard" section on page 11-8
- "Scheduling Trace Collection" section on page 11-12

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 11-2.

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

Step 3 Choose the appropriate radio button, and click **Next**. If you choose Trace Files, go to Step 4. If you choose Crash Dump, go to Step 7.

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 *Unified CM clusters and Connection clusters only:* You can install some of the listed services/applications only on a particular server in the cluster. To choose traces for those services/applications, make sure that you choose traces from the server on which you have activated the service/application.

Step 4 *Connection* users go to Step 5. For *Unified CM* or *Unified CM BE*, perform one of the following actions in the Select CCM Services/Application tab:

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.**

Go to Step 5 for *Unified CM BE* or go to Step 6 for *Unified CM*.

Step 5 In the Select CUC 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 6 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 10.

Step 7 *Connection* users go to Step 8. For *Unified CM* or *Unified CM BE*, perform one of the following actions in the Select CCM Services/Application tab:

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**.

Go to Step 8 for *Unified CM BE* or go to Step 9 for *Unified CM*.

Step 8 In the Select CUC 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 9 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 10.

Step 10 Click **Finish**.

Step 11 After the traces become available, a message displays. Click **Close**.

Step 12 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.

Unified CM and Unified CM BE only: For more information on using the QRT Viewer, see the "Displaying QRT Report Information" section on page 11-27.

- 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 11-22.

Additional Information

See the Related Topics, page 11-33.

Displaying QRT Report Information

Note This section applies only to Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition.

You can view the IP phone problem reports that the Quality Report Tool (QRT) generates by using the QRT viewer. QRT serves as a voice-quality and general problem-reporting tool for Cisco Unified IP Phones. After you collect the QRT log files, you can use the following procedure to list and view Cisco Unified Communications Manager IP Phone problem reports by using the QRT viewer. The QRT viewer allows you to filter, format, and view phone problem reports that are generated. For detailed information about how to configure and use QRT, refer to the *Cisco Unified Communications Manager Features and Services Guide*.

Before You Begin

You can view the QRT log files by either viewing the files on the server or by downloading the files onto your computer.

Collect or View the QRT log files as described in one of the following sections:

- "Collecting Trace Files" section on page 11-3
- "Using the Query Wizard" section on page 11-8
- "Scheduling Trace Collection" section on page 11-12
- "Using Remote Browse" section on page 11-23

After you download the files onto your computer, you can use the Local Browse option in the trace and log central feature as described in the "Using Local Browse" section on page 11-22.

Procedure

Step 1 Display the log file entries by using the Query Wizard, the Remote Browse or the Local Browse option in trace and log central.

The QRT Viewer window displays.

Note Only log files from the Cisco Extended Functions service contain QRT information. The following format for the log file name that contains QRT data applies: qrtXXX.xml.

Step 2 From the Extension drop-down list box, choose the extension(s) that you want the report to include.

Step 3 From the Device drop-down list box, choose the device(s) that you want the report to include.

Step 4 From the Category drop-down list box, choose the problem category that you want the report to include.

Step 5 From the Select Fields drop-down list box, choose the fields that you want the report to include.

Note The order in which you choose the fields determines the order in which they appear in the QRT Report Result pane.

Step 6 To view the report in the QRT Report Result pane, click **Display Records**.

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 11-28
- Monitor User Event, page 11-29

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 11-2.

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

Note *Unified CM clusters and Connection clusters only:* 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.The following limitations apply for your configuration:

Cisco Unified Communications Manager	You can view data for up to 10 services, 5 of which can exist on a single server.
Cisco Unified Communications Manager Business Edition	You can view data for 5 services.
Connection	You can view data for 5 services.

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 11-33.

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. The following limitations apply for your configuration:

Cisco Unified Communications Manager	For each event, you can monitor one service on one server.
Cisco Unified Communications Manager Business Edition	You can monitor one service for each event.
Connection	You can monitor 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 10-3.

Procedure

Step 1 Display the Trace & Log Central tree hierarchy, as described in "Displaying Trace and Log Central Options in RTMT" section on page 11-2.

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

Note *Unified CM clusters and Connection clusters only:* 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 10-3.
- 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.

Note By default, audit events are not sent to the remote syslog server, unless the severity is lowered to Warning, Notice or Informational.

- 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 You can choose **Localhost** download option when downloading traces. This option is available only for Cisco Intercompany Media Engine servers.
If you download trace files to the local host directories on the Cisco Intercompany Media Engine server, you can offload the files to a remote SFTP server by using the **file get** CLI command.

Note FTP is not supported for Cisco Intercompany Media Engine.

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 11-33.

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 11-33.

Log Compression

In previous releases of Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition, there were trace service parameters that enabled and disabled log file compression to the hard disk. The service parameters have been deprecated along with that feature.

There is a new implementation of log compression in 8.0, and is not configurable.

The new log compression feature only compresses the following log files:

- cm/trace/cti/sdl
- cm/trace/cti/sdi
- cm/trace/ccm/sdl
- cm/trace/ccm/sdi

The other log files are not compressed and are written directly to the hard disk.

The compressed files have a .gz extension. The file that is being actively written to the disk will have a .gzo extension.

All the CLI commands used to view and tail the files will work on the compressed files and will automatically uncompress them for viewing or tailing. The only difference is in specifying file names with the .gz and .gzo extension.

There is a new option available with the file tail command as follows:

```
file tail activelog cm/trace/cti/sdl recent
```

The recent option, when used with a compressed directory, will continually tail the most recent log file. It is not necessary to switch to a newer log file when the currently written-to log file is closed, so it is an infinite and ongoing tail. This option is only available with the compressed log files.

The log files are compressed in the gzip format. For uncompressing the log files, the open source program 7-Zip is available at http://www.7-zip.org, and works on all Windows platforms. You can use 7-Zip on any computer, including a computer in a commercial organization. You don't need to register or pay for 7-Zip. On a linux platform, you can use the gzip or gunzip commands.

Where to Find More Information

Related Topics

- Using the Query Wizard, page 11-8
- Using Local Browse, page 11-22
- Collecting Trace Files, page 11-3
- Scheduling Trace Collection, page 11-12
- Displaying Trace and Log Central Options in RTMT, page 11-2
- Collecting a Crash Dump, page 11-16
- Using Local Browse, page 11-22

Additional Cisco Documentation

- *Cisco Unified Serviceability Administration Guide*