Trace and Log Central

This chapter provides information about Trace and Log Central.

Trace and Log Central

The Trace and Log Central feature in 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.

Note

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

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 node 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 Unified RTMT or choosing an appropriate program as an external viewer.

Note

- To use the Trace and Log Central feature, make sure that RTMT can directly access the node or all of the nodes in a cluster without Network Access Translation (NAT). If you have set up a NAT to access devices, configure the nodes with a hostname instead of an IP address and make sure that the hostnames (Fully Qualified Domain Name of the host) and their routable IP address are in the DNS node or host file.
- For devices that support encryption, the SRTP keying material does not display in the trace file.

Related Topics

Collect and Download Trace Files Using Query Wizard, on page 8

Collect Audit Logs, on page 19

Collect Crash Dump, on page 16

Collect Installation Logs, on page 8

Collect Trace Files, on page 5

Display and Download Trace Files Using Remote Browse, on page 23

Display Downloaded Trace Files Using Local Browse, on page 22

Display Report Information, on page 26

View Trace and Log Central Options, on page 3

Edit Trace Settings, on page 30

Import Certificates, on page 2

Log Compression, on page 31

Real-Time Trace, on page 27

Schedule Trace Collection, on page 13

View Trace Collection Status, on page 15

Import Certificates

Follow this procedure to import the node certificates.

You can import the server authentication certificate that the certificate authority provides for the node or for each node in the cluster.

We recommend 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 nodes each time that you sign in to Unified RTMT and access the Trace and Log Central option. You cannot change any data that displays for the certificate.

Procedure

Step 1 To import the certificate, choose **Tools** > **Trace** > **Import Certificate**.
A messages appears that states that the system imported the node certificates.

Step 2 Click **OK**.

Related Topics

Trace and Log Central, on page 1

View Trace and Log Central Options

Follow this procedure to view Trace and Log Central options in Unified RTMT.

Note From any option that displays in the tree hierarchy, you can specify the services and 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.

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

Before You Begin

Before you begin, import the security certificates.

Procedure

Step 1 Perform one of the following actions to access Trace and Log Central:

a) Select **System** in the Quick Launch Channel**.**
b) Select **System** > **Tools** > **Trace** > **Trace & Log Central**.
c) Select the **Trace & Log Central** icon in the tree hierarchy.

Step 2 Perform one of the following tasks after you display the Trace and Log Central options in the Real-Time Monitoring Tool:

- Collect traces for services, applications, and system logs on one or more servers in the cluster.
- Collect and download trace files that contain search criteria that you specify as well as save trace collection criteria for later use.
- Collect a crash dump file for one or more servers on your network.
- View the trace files that you have collected.

- View all of the trace files on the server.
- View the current trace file being written on the server for each application. You can perform a specified action when a search string appears in the trace file.

Related Topics

Trace and Log Central, on page 1
Collect and Download Trace Files Using Query Wizard, on page 8
Collect Audit Logs, on page 19
Collect Crash Dump, on page 16
Collect Trace Files, on page 5
Display and Download Trace Files Using Remote Browse, on page 23
Display Downloaded Trace Files Using Local Browse, on page 22
Import Certificates, on page 2
Schedule Trace Collection, on page 13
Real-Time Trace, on page 27

Trace Files Collection, Throttling, and Compression

The Collect Files option in Trace and Log Central collects traces for services, applications, and system logs on the server or on one or more servers in the cluster.

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

RTMT Trace and Log Central Disk I/O 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 I/O 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 I/O conditions, the system displays a warning that gives you the opportunity to abort the operation. You can configure the I/O 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 the following:

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

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

Caution Compressing files adds additional CPU cycles. Enabling the Trace Compression enterprise parameter can negatively affect 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 filename, and the file opens in the log viewer.

Related Topics

Collect Trace Files, on page 5

Collect Trace Files

Use the Collect Files option in Trace and Log Central to collect traces for services, applications, and system logs on one or more nodes in the cluster. You specify date and time range for which you want to collect traces, the directory in which to download the trace files and whether to delete the collected files from the node.

Follow this procedure to collect traces using the trace and log central feature.

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

Use the Query Wizard 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.

Before You Begin

Perform one or more of the following actions:

- 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, see 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 in Cisco Unified Serviceability. For more information, see the *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, see the *System Configuration Guide for Cisco Unified Communications Manager* .

Procedure

Step 1 Open the Trace and Log Central options.

Step 2 In the Trace & Log Central tree hierarchy, double-click **Collect Files**.
The Trace Collection wizard appears. The services that you have not activated also appear, so you can collect traces for those services.

Note Unified Communications Manager and Cisco Unity Connection clusters: If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node will not appear in the Trace and Log Central windows.

Note Unified Communications Manager and Cisco Unity Connection clusters: You can install some of the listed services/applications only on a particular node in the cluster. To collect traces for those services/applications, make sure that you collect traces from the node on which you have activated the service/application.

Step 3 *Cisco Unity Connection* users go to Step 4. For Unified Communations Manager or Cisco Business Edition, perform one of the following actions in the **Select CCM Services/Application** tab:

a) To collect traces for all services and applications for all nodes in a cluster, check the **Select All Services on All Servers** check box and click **Next**.

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

b) To collect traces for all services and applications on a particular node (or for particular system logs on the node for *Cisco Unity Connection*), check the check box next to the node and click **Next**.

c) To collect traces for particular services or applications on particular nodes, check the check boxes that apply and click **Next**.

d) To go to the next tab without collecting traces for services or applications, click **Next**.
Go to Step 4 for Cisco Business Edition or go to Step 5 for Unified Communications Manager.

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

a) To collect all system logs for the node, check the **Select All Services on all Servers** check box or check the check box next to the node and click **Next**.

b) To collect traces for particular system logs on the node, check the check boxes that apply and click **Next**.

c) To go to the next tab without collecting traces for system logs, click **Next**.

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

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

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

b) To collect traces for all system logs on a particular node, check the check box next to the node and click **Next**.

c) To collect traces for particular system logs on particular nodes, check the check boxes that apply and click **Next**.

d) 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:

a) **Absolute Range**: Specify the node 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, appear 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 nodes 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 a.m. to 10:00 a.m. and you have a second node (node x) that is in a time zone that is one hour ahead, TLC will download files from 10:00 a.m. to 11:00 a.m. from node 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.

b) **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 Unified RTMT returns logs of a different time stamp, than that configured through the wizard. This occurs specifically, when the specified time stamp is lesser than that of the existing log files.

Log files exist on the node 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; Unified 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 Unified Communications Manager, Cisco Business Edition 5000, or Cisco Unity Connection that is running on an appliance node to another version, and you restart the node 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 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_users_directory>\<server name or server IP address>\<download time>`.

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 node, 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>" appears 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.

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

Related Topics

- Collect and Download Trace Files Using Query Wizard, on page 8
- Display Downloaded Trace Files Using Local Browse, on page 22
- View Trace and Log Central Options, on page 3

Collect Installation Logs

Follow this procedure to collect installation and upgrade logs.

Procedure

Step 1 Choose **Tools** > **Trace** > **Trace & Log Central**.
The **Trace & Log Central** window appears.

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

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 **Browse** next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies `<rtmt_users_directory>`.

Step 5 Click **Finish**.

Collect and Download Trace Files Using 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.

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

Step 3 In the **Query Wizard Options** window, click one of the following radio buttons, and then click **Next** to modify the query.

- Saved Query

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

  If you choose a single-node, generic query, the server to which RTMT is connected appears 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 choose an all-node, generic query, all servers in the cluster appears 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 17, on page 12.

- Create Query

Step 4 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 appear, 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 5 *Cisco Unity Connection* users go to Step 7, on page 10. For *Unified Communications Manager* or *Cisco Business Edition*, 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 6 Click **Next**. *Unified Communications Manager* users go to Step 8, on page 10.

Step 7 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, then 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, then click **Next**.

Step 9 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, appear 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 10 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 11 In the Call Processing Impact Options box, specify the level of impact you want the string search activity to have on call processing, then click **Next**.
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 12 In the **Action Options** window, choose one of the following actions:

a) Trace Browse

b) 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.

c) 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 appears. 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.

Note 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 13 Choose one of the following options:

a) 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 appears. When the query completes, a dialog box that indicates that the query execution completed appears. Click **Close** and continue with Step 17, on page 12.

b) To save the query, click the **Save Query** button and continue with Step 14, on page 11.

c) 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.

Step 14 Check the check box next to the type of query that you want to create from the following options, and then click **Finish**.

a) **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 appears.
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 Business Edition 5000, 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.

b) **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 15 Browse to the location to store the query, enter a name for the query in the File Name field, and click **Save**.

Step 16 Perform one of the following actions:

a) To run the query that you have just saved, click **Run Query** and continue with Step 17, on page 12.

b) To exit the query wizard without running the query that you created, click **Cancel**.

Step 17 After the query execution completes, perform one or more of the following tasks:

a) 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 Communications Manager and Cisco Business Edition only*: To view reports that the QRT Quality Report Tool (QRT) generates, see the Display Report Information, on page 26.

b) 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.

c) To save the query, click **Save Query** button and complete Step 14, on page 11 through Step 15, on page 12.

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

Related Topics

Display Downloaded Trace Files Using Local Browse, on page 22

View Trace and Log Central Options, on page 3

Display Report Information, on page 26

Schedule 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 ten 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 actions:

- 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, see 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, see the *Cisco Unified Serviceability Administration Guide*.

Procedure

Step 1 Open the Trace and Log Central options.

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

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

Note Unified Communications Manager Cisco Unity Connection: If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node will not appear in the Trace and Log Central windows.

Note Unified Communications Manager and Cisco Unity Connection: You can install some listed services and applications on a particular node in the cluster. To collect traces for those services and applications, make sure that you collect traces from the node on which you have activated the service or application.

Step 3 Cisco Unity Connection users go to Step 4. For Unified Communications Manager or Cisco Business Edition, perform one of the following actions in the **Select CCM Services/Application** tab:

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

- To collect traces for all services and applications for all nodes, check the **Select All Services on All Servers** check box and click **Next**.
- To collect traces for all services and applications on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular services or applications on particular nodes, check the check boxes that apply and click **Next**.

- To continue the schedule collection wizard without collecting traces for services or applications, click **Next**.

For Cisco Business Edition, go to Step 4. For Unified Communications Manager, go to Step 5.

Step 4 In the **Select CUC Services/Application** tab, perform one of the following actions:

- To collect all system logs for the node, check the **Select All Services on all Servers** check box or check the check box next to the node and click **Next**.
- To collect traces for particular system logs on the node, 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 actions:

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

- To collect all system logs for all nodes, check the **Select All Services on all Servers** check box and click **Next**.
- To collect traces for all system logs on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular system logs on particular nodes, 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 node 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, appear 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. In the **Date** tab, choose the appropriate date. In 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. In the **Date** tab, choose the appropriate date. In 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 node, 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 node credentials for the node 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**.
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`.

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 appears. Verify that you entered the correct IP address, username, 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 appears. Click **OK**.

Related Topics

View Trace and Log Central Options, on page 3

View Trace Collection Status

Follow this procedure to view the trace collection event status and to delete scheduled trace collections.

Procedure

Step 1 Open the Trace & Log Central tree hierarchy.

Step 2 Double-click **Job Status**.
The **Job Status** window appears.

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 appears.

Possible job types include the following:

- Scheduled Job
- OnDemand
- RealTimeFileMon
- RealTimeFileSearch

Possible statuses include the following:

- Pending
- Running
- Cancel
- 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."

Related Topics

View Trace and Log Central Options, on page 3

Collect Crash Dump

Follow this procedure to collect a core dump of trace files:

Procedure

Step 1 Open the Trace & Log Central tree hierarchy.

Step 2 Double-click **Collect Crash Dump**.
The Collect Crash Dump wizard appears.

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

Note Unified Communications Manager and Cisco Unity Connection: If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node will not appear in the Trace and Log Central windows.

Note Unified Communications Manager clusters and Cisco Unity Connection clusters only: You can install some of the listed services/applications only on a particular node in the cluster. To collect traces for those services/applications, make sure that you collect traces from the node on which you have activated the service/application.

Step 3 Cisco Unity Connection users go to Step 4. For Unified Communications Manager or Cisco Business Edition, perform one of the following actions in the **Select CCM Services/Application** tab:

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

- To collect traces for all services and applications for all nodes, check the **Select All Services on All Servers** check box and click **Next**.
- To collect traces for all services and applications on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular services or applications on particular nodes, 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 Cisco Business Edition or go to Step 5 for Unified Communications Manager.

Step 4 In the **Select CUC Services/Application** tab, perform one of the following actions:

- To collect all system logs for the node, check the **Select All Services on all Servers** check box or check the check box next to the node and click **Next**.
- To collect traces for particular system logs on the nodes, 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 actions:

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

- To collect all system logs for all nodes, check the **Select All Services on all Servers** check box and click **Next**.
- To collect traces for all system logs on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular system logs on particular nodes, 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 node 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, appear 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 nodes in a cluster in a different time zone, TLC adjusts for the time change and gets files for the same period of time. For example, if you specify files from 9:00 a.m. to 10:00 a.m and you have a second node (node x) that is in a time zone that is one hour ahead, TLC downloads files from 10:00 a.m. to 11:00 a.m. from node 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.

When you upgrade from one version of your product that is running on the Linux platform to another version, and you restart the node 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, IM and Presence Service, 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 node, check the **Delete Collected Log Files from Server** check box.

Step 11 Click **Finish**.
A message appears 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.

Related Topics

View Trace and Log Central Options, on page 3

Collect 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 Open the Trace & Log Central tree hierarchy.

Step 2 Double-click **Collect Audit Logs**.
The Collect Audit Logs Action Options wizard appears.

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

a) To browse audit logs, check the **Browse Audit Logs** check box.
b) To download audit logs, check the **Download Audit Logs** check box.
c) 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 appears.

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.

a) To browse, download, or schedule a download of audit logs for all servers, check the **Select All Servers** check box.
b) 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:

a) Browse Audit Logs, go to Step 7, on page 19.
b) Download Audit Logs, go to Step 11, on page 20.
c) Schedule Download of Audit Logs, go to Step 16, on page 21.

Step 7 The Remote Browse is Ready window appears. Click the **Close** button.
The Nodes pane appears.

Step 8 On the left side of the Nodes pane, double-click the **Nodes** folder. Navigate through the tree hierarchy until the Audit App folder appears.

Step 9 After the audit log file names appear 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 10 Select an audit log file and perform one of the following actions:

a) To download the selected audit log file, click the **Download** button.
The Select Download Options wizard appears.

b) 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>`.

c) 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.

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

e) Click **Finish**.

f) To delete the selected audit log file, click the **Delete** button.

g) To refresh the selected audit log file, click the **Refresh** button.

h) 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 11 To download audit logs, click **Next**.

The **Download Audit Logs** window appears.

Step 12 In the Nodes Selection Options pane, select one of the following:

a) Check the **Select All Servers** check box.

b) Check a specific node check box.

Step 13 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, appear 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 14 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 15 Click **Finish**. You have completed the steps for the download of audit logs.

Step 16 The **Schedule Download of Audit Logs** window appears.

a) In the Nodes Selection Options pane, select one of the following options:

- Check the **Select All Servers** check box.
- Check a specific node check box.

b) In the Schedule Time pane, perform the following actions:

1. Highlight the **Select Reference Server Time Zone**.
2. Use the calendar and highlight a **Start Date/Time**.
3. Use the calendar and highlight an **End Date/Time**.
4. Select the Scheduler Frequency. You may choose Hourly, Daily, Weekly, or Monthly.
5. Check the **Zip All Files** check box if you want to zip the audit log files.
6. Check the **Delete Collected Log Files From Server** check box if you want to delete the collected audit log files from the server.

c) In the Action Options pane, check the **Download Files** check box.
The **Trace Download Configuration Dialog** window appears. 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 username.
- 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 **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.

Related Topics

View Trace and Log Central Options, on page 3

Display Downloaded Trace Files Using Local Browse

After you collect trace files and download 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 Unified RTMT.

Tip Do not use NotePad to view collected trace files.

Follow this procedure to display the log files that you collected with the Trace and Log Central feature. If you zipped the trace files when you downloaded them to your PC, you need to unzip the files to view them by using the viewers within Unified RTMT.

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

Before You Begin

Collect the required traces files. See topics related to collecting trace files, downloading trace files using Query Wizard, and scheduling trace collection for instructions.

Procedure

Step 1 Open Trace and Log Central.

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.
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 appears.

Step 5 Click the program that want to use to view the file. If your preferred program is not on the list, choose another program by clicking **Other**.
If you want to use this program as your default viewer, check the **Always use this program to open these files** check box.

Unified RTMT displays the file in the appropriate viewer for the file type. If no other appropriate viewer applies, Unified RTMT opens files in the Generic Log Viewer.

Related Topics

Collect and Download Trace Files Using Query Wizard, on page 8

Collect Trace Files, on page 5
Display Report Information, on page 26
View Trace and Log Central Options, on page 3
Schedule Trace Collection, on page 13

Display and Download Trace Files Using Remote Browse

After the system generates trace files, you can view them on the node by using the viewers within Unified RTMT. You can also use the remote browse feature to download the traces to your PC.

Follow this procedure to display and download the log files on the node 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 the required traces files. See topics related to collecting trace files, downloading trace files using Query Wizard, and scheduling trace collection.

Procedure

Step 1 Open the Trace and Log Central options.

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 appear, 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 Communications Manager clusters and Cisco Unity Connection clusters: You can install some of the listed services/applications only on a particular node in the cluster. To choose traces for those services/applications, make sure that you choose traces from the node on which you have activated the service/application.

Step 4 Cisco Unity Connection users go to Step 5. For Unified Communications Manager or Cisco Business Edition, perform one of the following actions in the Select CCM Services/Application tab:

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

- To collect traces for all services and applications for all nodes, check the **Select All Services on All Servers** check box and click **Next**.
- To collect traces for all services and applications on a particular node, check the check box next to the node and click **Next**.

- To collect traces for particular services or applications on particular nodes, 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 Cisco Business Edition or go to Step 6 for Unified Communications Manager.

Step 5 In the **Select CUC Services/Application** tab, perform one of the following actions:

- To collect all system logs for the node, check the **Select All Services on all Servers** check box or check the check box next to the node and click **Next**.
- To collect traces for particular system logs on the node, 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 actions:

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

a) To collect all system logs for all nodes, check the **Select All Services on all Servers** check box and click **Next**.
b) To collect traces for all system logs on a particular node, check the check box next to the node and click **Next**.
c) To collect traces for particular system logs on particular nodes, check the check boxes that apply and click **Next**.
d) To continue the Remote Browse wizard without collecting traces for system logs, click **Next**.
e) Go to Step 10.

Step 7 Cisco Unity Connection users go to Step 8. For Unified Communications Manager or Cisco Business Edition, perform one of the following actions in the **Select CCM Services/Application** tab:

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

a) To choose crash dump files for all services and applications for all nodes, check the **Select All Services on All Servers** check box and click **Next**.
b) To choose crash dump files for all services and applications on a particular node, check the check box next to the node and click **Next**.
c) To choose crash dump files for particular services or applications on particular nodes, check the check boxes that apply and click **Next**.
d) To continue the Remote Browse wizard without collecting crash dump files, click **Next**.
Go to Step 8 for Cisco Business Edition or go to Step 9 for Unified Communications Manager.

Step 8 In the **Select CUC Services/Application tab**, perform one of the following tasks:

a) To choose crash dump files for the node, check the **Select All Services on all Servers** check box or check the check box next to the node and click **Next**.
b) To choose crash dump files for particular system logs on the node, check the check boxes that apply and click **Next**.
c) 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 node and check the **Select All Services on All Servers** check box, the system collects crash dump files for your standalone node.

a) To choose crash dump files for all nodes, check the **Select All Services on all Servers** check box.

b) To choose crash dump files for all system logs on a particular node, check the check box next to the node.

c) To choose crash dump files for particular system logs on particular nodes, check the check boxes that apply.

d) To continue the Remote Browse wizard without collecting crash dump files, go to the next step.

Step 10 Click **Finish**.

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

Step 12 Perform one of the following actions:

a) To display the results, navigate to the file through the tree hierarchy. After the log filename appears 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 appear 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 Communications Manager and Cisco Business Edition: For more information, see topics related to using the QRT Viewer to display QRT reports.

b) 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 **Browse** 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 Unified 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 node, check the **Delete Files on server** check box.

c) To delete trace files from the node, click the file that appears in the pane on the right side of the window; then, click **Delete**.

d) To refresh a specific service or a specific node in a cluster, click the service or node name; then, click **Refresh**. After a message states that the remote browse is ready, click **Close**.

e) To refresh all services or all nodes in a cluster that appear in the tree hierarchy, click **Refresh All**. After a message states that the remote browse is ready, click **Close**.

Tip After you download the trace files, you can view them in Local Browse.

Related Topics

Collect and Download Trace Files Using Query Wizard, on page 8

Collect Trace Files, on page 5

Display Downloaded Trace Files Using Local Browse, on page 22

Display Report Information, on page 26

View Trace and Log Central Options, on page 3

Schedule Trace Collection, on page 13

Display Report Information

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

Note This section applies only to Cisco Unified Communications Manager.

You can view the IP phone problem reports that the Quality Report Tool 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 more information about how to configure and use QRT, see the *System Configuration Guide for Cisco Unified Communications Manager* .

Before You Begin

Collect or view the Quality Report Tool (QRT) log files. See topics related to collecting trace files, scheduling trace collection, and downloading trace files using either Query Wizard or the Remote Browser.

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 appears.

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

Note The QRT viewer allows only the .xml files with a specific structure (having phone details), not the default one. If you open generic log files, you may see the following error message:

```
Fail to Open Cisco QRT Viewer, No Records Available!
```

Step 2 From the **Extension** drop-down list box, choose the extension or extensions that you want the report to include.

Step 3 From the **Device** drop-down list box, choose the device or devices 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**.

Related Topics

Collect and Download Trace Files Using Query Wizard, on page 8
Collect Trace Files, on page 5
Display Downloaded Trace Files Using Local Browse, on page 22
Display and Download Trace Files Using Remote Browse, on page 23
Schedule Trace Collection, on page 13

Real-Time Trace

The real-time trace option of the Trace and Log Central feature 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 option to view real-time data and monitor user events.

Related Topics

Monitor User Event, on page 28
View Real-Time Data, on page 27

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 ten services, with a limit of three concurrent sessions on a single node. The log viewer refreshes every 5 seconds. As the traces are 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 Open the Trace & Log Central tree hierarchy.

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

Note Unified Communications Manager clusters and Cisco Unity Connection clusters only: If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node will not display in the Trace and Log Central windows.

Step 3 Double-click **View Real Time Data**.
The View Real Time Data wizard appears.

Step 4 From the **Nodes** drop-down list box, choose the node 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 appears 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 Perform one of the following actions:

- 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.
A message appears if you attempt to view data for too many services or too many services on a single node.

Step 9 After you finish with 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.

Related Topics

View Trace and Log Central Options, on page 3

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.

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.

Procedure

Step 1 Open the Trace & Log Central tree hierarchy.

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

Note Unified Communications Manager clusters and Cisco Unity Connection clusters only: If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node does not display in the Trace and Log Central windows.

Step 3 Double-click **Monitor User Event**.
The Monitor User Event wizard appears.

Step 4 Perform one of the following actions:

If you want to:	Action
View the monitoring events that you have already set up	• Click **View Configured Events** • Select a node from the drop-down list box. • Click **Finish**. **Note** To delete an event, choose the event and click **Delete**.

If you want to:	Action
Configure new monitoring events	• Select **Create Events.** • Select **Next**. • Continue with Step 5.

Step 5 Choose the node 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 appear, 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 node 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 nodes in a cluster in a different time zone, TLC adjusts for the time change and get files for the same period of time. For example, if you specify files from 9:00 a.m. to 10:00 a.m. and you have a second node (node x) that is in a time zone that is one hour ahead, TLC downloads files from 10:00 a.m. to 11:00 a.m. from node 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:

If you want the system to:	Action
Generate an alarm when the system encounters the specified search string	Check **Alert**. **Note** For the system to generate the alarm, you must enable the enable the TraceCollectionToolEvent alert.
Log the errors in the application logs area in the SysLog Viewer	Check **Local Syslog**. **Note** The system provides a description of the alarm and a recommended action. You can access the SysLog Viewer from Unified RTMT.
Store the syslog messages on a syslog node	Check **Remote Syslog**. Enter the syslog node name in the **Server Name** field. **Note** By default, audit events are not sent to the remote syslog node, unless the severity is lowered to Warning, Notice, or Informational.

If you want the system to:	Action
Download the trace files that contain the specified search string	Check **Download File**. Enter the node credentials for the node where you want to download the trace files in the SFTP Server Parameters group box. Select **Test Connection**. Select **OK** after the Trace and Log Central feature verifies the connection to the SFTP server. 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. 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.

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.

The following message appears: `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**.

Related Topics

View Trace and Log Central Options, on page 3

Set Up Alert Properties

Edit Trace Settings

Follow this procedure to edit trace settings for Unified RTMT.

Note The Error radio button is the default setting.

Procedure

Step 1 Choose **Edit** > **Trace Setting**

Step 2 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 is stored in `C:\Documents and Settings\<userid>\.jrtmt\log`.

Log Compression

In Unified Communications Manager 8.0 onward, the 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.

The following option is available with the file tail command:

file tail activelog cm/trace/cti/sdl recent

The recent option, when used with a compressed directory, continually tails the most recent log file. You do not need 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 do not need to register or pay for 7-Zip. On a Linux platform, you can use the gzip or gunzip commands.