Configuring Trace and Log Central in RTMT

April 5, 2013

About Trace Collection

You can use Trace and Log Central, an option in the Cisco Unified Presence Real-Time Monitoring Tool (RTMT), to collect, view, and zip various service traces and/or other log files. With the Trace and Log Central option, you can collect SDI traces, Application Logs, System Logs (such as Event View Application, Security, and System logs), and crash dump files.

The Trace and Log Central feature 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 RTMT. 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 application as an external viewer.

Consider the following recommendations:

- To collect CSA logs, check **Cisco Security Agent** in the Select System Services/Applications tab in RTMT. To access user logs that provide information about users that are signing in and out, check **Security Logs** in the Select System Services/Applications tab.
- For devices that support encryption, the SRTP keying material does not display in the trace file.
- 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.

- Do not use NotePad to view collected trace files.

- Time Zone and Date Range for Trace Collection, page 6-2
- Logs for Trace Collection, page 6-2

Time Zone and Date Range for Trace Collection

The time zone of the client computer 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 list box.

The trace or crash dump files that are modified in the date range (between the From date and the To date), are collected if the chosen time zone matches the time zone settings of the server (for example Server 1). If another server exists in the same Cisco Unified Presence cluster (Server 2), but that server resides in a different time zone, then the files that are modified in the corresponding date range in Server 2 are collected from Server 2.

- **Absolute Range**—Specify the server time zone and the time range (start and end date and time) for which you want to collect traces.
- **Relative Range**—Specify the time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect traces.

Logs for Trace Collection

Cisco Unified Serviceability stores logs for up to two Linux-based versions of Cisco Unified Presence. Cisco Unified Serviceability stores the logs for the version of Cisco Unified Presence that you are signed in to in the active partition and stores the logs for the other version of Cisco Unified Presence (if installed) in the inactive directory.

When you upgrade from one version of Cisco Unified Presence that is running on the Linux platform to another and sign in to the new version of Cisco Unified Presence that is running on the Linux platform, Cisco Unified Serviceability moves the logs from the previous version to the inactive partition and stores logs for the newer version in the active partition. If you sign in to an earlier version of Cisco Unified Presence, Cisco Unified Serviceability moves the logs for the newer version of Cisco Unified Presence to the inactive partition and stores the logs for the earlier version in the active directory.

Note Cisco Unified Serviceability does not retain logs from Cisco Unified Presence versions that run on Windows platforms.

How to Prepare for Trace Collection

To use the Trace and Log Central feature in the RTMT, make sure that RTMT can access all of the nodes in the cluster directly without Network Access Translation (NAT). If you have set up a NAT to access devices, configure the Cisco Unified Presence 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.

- Importing Certificates, page 6-3
- Viewing Trace & Log Central Options in RTMT, page 6-3

Importing Certificates

You can import the server authentication certificate that the certificate authority provides 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 each node in the cluster each time that you sign into RTMT and access the trace and log central option. You cannot change any data that displays for the certificate.

Procedure

Step 1 Select **System > Tools > Trace > Import Certificate**.

Step 2 Select **OK** when the message dialog confirms that the import is complete.

Viewing Trace & Log Central Options in RTMT

Before You Begin

Import the certificate.

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.
- Schedule a recurring trace collection and download the trace files to a SFTP or FTP server on your network.
- 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.

Troubleshooting Tips

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

Related Topics

- How to Configure Trace Collection, page 6-5
- Importing Certificates, page 6-3

About Types of Trace Support

- RTMT Trace and Log Central Disk IO and CPU Throttling, page 6-4
- Trace Compression Support, page 6-4

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.

When you make a request for an on-demand operation when the node is running under high IO conditions, the system displays a warning which gives you the opportunity to cancel the operation. Be aware that the IO rate threshold values that control when the warning displays are configurable with the following service parameters (Cisco RIS Data Collector service):

- TLC Throttling CPU Goal
- TLC Throttling IOWait Goal

The values of these parameters are compared to 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 trace files. The system compresses the files as they are being generated. The following benefits of tracefile compression apply:

- Reduces the capacity required to store tracefiles.
- Reduces the disk head movement which results in significantly improved call load. This prevents CPU blockage due to tracefile demands.

Use the enterprise parameter, Trace Compression, to enable or disable trace compression. The default value for this parameter specifies Disabled.

Compressed files have a .gz extension (.gzo if the file is still being written to). To open a compressed file, double-select the file name. If there is a viewer associated with the extension, the file opens in that viewer. If a viewer is not associated with the extension, the Open With dialog box displays. Select the viewer that you want to use and check Always use this program to skip this viewer selection process in the future.

How to Configure Trace Collection

Collecting Trace Files

Use the Collect Traces option of the trace and log central feature to collect traces for services, applications, and system logs 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.

Before You Begin

- Configure the information that you want to include in the trace files for the various services from the Trace Configuration window.
- If you want alarms to be sent to a trace file, select an SDI trace file as the alarm destination in the Alarm Configuration window.
- 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, use the Query Wizard.
- 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).
- Optionally, enable trace compression by setting the value of the Trace Compression enterprise parameter to Enabled.

Procedure

Step 1 Open Trace & Log Central.

Step 2 Double-select **Collect Files** in the tree hierarchy.

Step 3 Perform one of the following actions to collect trace for Cisco Unified Presence services and applications:

If you want to:	Action
Collect traces for all services and applications from all servers in the cluster	Check **Select All Services on All Servers**.
Collect traces for all services and applications on a particular server	Check the name of the server.

If you want to:	Action
Collect traces for particular services or applications on particular servers	Check the traces that apply.
Continue the Trace Collection wizard without collecting traces for services or applications	Go to Step 4.

Step 4 Select **Next**.

Step 5 Perform one of the following actions to collect trace for system services and applications:

If you want to:	Action
Collect all system logs for all servers in the cluster	Check **Select All Services on All Servers**.
Collect traces for all services and applications on a particular server	Check the name of the server.
Collect traces for particular system logs on particular servers	Check the traces that apply. For example, to collect CSA logs, check **Cisco Security Agent**. To access user logs that provide information about users that are signing in and out, check **Security Logs**.
Continue the trace collection wizard without collecting traces for system logs	Go to Step 6.

Step 6 Select **Next**.

Step 7 Specify the time zone and time range for which you want to collect traces in the Collection Time group box.

Step 8 Select the partition that contains the logs for which you want to collect traces from the Select Partition list box.

Step 9 Perform one of the following actions to download trace files:

If you want to:	Action
Specify the directory in which you want to download the trace files	**a.** Select **Browse** next to the Download File Directory field. **b.** Navigate to the directory. **c.** Select **Open**. **Note** The default specifies C:\Program Files\Cisco\Presence Serviceability\jrtmt\<server IP address>\<download time>.
Create a zip file of the trace files that you collect	**a.** Select **Zip File.**
Download the trace files without zipping the files	**a.** Select **Do Not Zip Files**.
Delete collected log files from the server	**a.** Check **Delete Collected Log Files from Server**.

Step 10 Select **Finish**.

Troubleshooting Tips

- The window shows the progress of the trace collection. Select **Cancel** if you want to stop the trace collection.
- When the trace collection process is complete, the message "Completed downloading for node <IP address>" displays at the bottom of the window. To view the trace files that you collected, you can use the Local Browse option of the trace collection feature.
- 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 does not display in the Trace & Log Central windows.
- 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 server on which you have activated the service/application.
- The services that you have not activated also display, so you can collect traces for those services.

Related Topics

- *Serviceability Configuration and Maintenance Guide for Cisco Unified Presence*
- Time Zone and Date Range for Trace Collection, page 6-2
- About Types of Trace Support, page 6-4
- How To Use the Query Wizard, page 6-8
- Viewing Collected Trace Files Using Local Browse, page 6-19

Collecting Installation Logs

You can collect installation and upgrade logs in Trace and Log Central.

Procedure

Step 1 Perform one of the following tasks:

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

Step 2 Double-select **Collect Install Logs** in the Trace & Log Central tree hierarchy.

The Collect Install Logs wizard displays

Step 3 Specify from which server you would like to collect the install logs in the Select Servers Options box:

a. Check the server to collect the install logs for a particular server.

b. Check **Select All Servers** to collect the install logs for all servers.

Step 4 Specify the directory where you want to download the log file in the Download File Options:

- To specify the directory in which you want to download the log files, select **Browse** next to the Download File Directory field, navigate to the directory, and select **Open**. The default specifies <rtmt_install_directory> where <rtmt_install_directory> specifies the directory where RTMT is installed.

Step 5 Select **Finish**.

How To Use the Query Wizard

- Starting a Query, page 6-8
- Executing the Query, page 6-10

Before You Begin

- Configure the information that you want to include in the trace files for the various services from the Trace Configuration window.
- If you want alarms to be sent to a trace file, select an SDI trace file as the alarm destination in the Alarm Configuration window.

Starting a Query

Procedure

Step 1 Open Trace & Log Central.

Step 2 Double-select **Query Wizard** in the tree hierarchy.

Step 3 Perform one of the following actions:

If you want to:	Action	Result
Run a saved Query	**a.** Select **Saved Query.** **b.** Select **Browse** to navigate to the query that you want to use. **c.** Select the query and select **Open**.	• If you chose a single node generic query, the node to which RTMT is connected displays with a checkmark next to **Browse**. You can run the query on additional nodes by placing a checkmark next to those servers. • If you chose an all node generic query, all nodes display with a checkmark next to **Browse**. You can uncheck any server for which you do not want to run the query. • If you chose a regular query, all of the nodes that you selected when you saved the query display with a checkmark. You can check or uncheck any of the servers in the list. If you select new servers, you must use the wizard to select the services for that node
Create a query	Select **Create Query.**	

If you want to:	Action	Result
Run the query without any modification	a. Select **Run Query**. b. Complete the steps in Executing the Schedule.	
Modify the query	Go to Step 4	

Step 4 Select **Next**.

Step 5 Perform one of the following actions:

a. If you selected **Saved Query** and chose a query, the criteria that you specified for query display. If necessary, modify the list of services and applications for which you want to collect traces.

b. If you selected **Create Query**, you must select all services and applications for which you want to collect traces.

Step 6 Select **Next**.

Step 7 Perform one of the following actions:.

If you want to:	Action
Collect traces for system logs or all system logs for all servers in the cluster	a. Perform one of the following actions: – Check the traces that apply. – Check **Select All Services on All Servers**. b. Select **Next**.
Collect traces for all services and applications for all servers in the cluster,	a. Check **Select All Services on All Servers**. b. Select **Next**.
Collect traces for all services and applications on a particular server,	a. Check the name of the server. b. Select **Next**.

Step 8 Perform one of the following actions to specify the time range for which you want to collect traces:.

If you want to:	Action
Collect all the traces on the server for the service(s) that you chose	Select **All Available Traces.**
Collect all the traces within an absolute date and time range	a. Select **Absolute Range.** b. Specify the server time zone and the time range (start and end date and time) for which you want to collect traces.
Collect all the traces within a relative date and time range	a. Select **Relative Range.** b. Specify the time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect traces.

Step 9 Enter the word or phrase in the Search String field to search by phrases or words that exist in the trace file. The tool searches for an exact match to the word or phrase that you enter.

What To Do Next

Executing the Query, page 6-10

Related Topics

- *Serviceability Configuration and Maintenance Guide for Cisco Unified Presence*

Executing the Query

Procedure

Step 1 Perform one of the following actions:

a. Select **Run Query** to execute the query.

– Select **OK** when the dialog box displays that indicates that the query execution completed.

– Continue with Step 2.

b. Select **Save Query** to save the query and continue with Step 6.

Step 2 Perform the following actions:

If you want to:	Action	Result
Create a query that you can run on nodes other than the one on which it was created	a. Select **Generic Query.** b. Select either the **Single Node Query** or **All Node Query**. c. Select **Finish**.	• You can only create a generic query if the services that you chose exist on a single node. If you chose services on more than one node, a message displays. You can either save the query as a regular query or select services on a single node. • If you select the Single Node Query, the trace collection tool by default selects the server on which you created the query when you execute the query. • If you select the All Node Query option, the trace collection tool by default selects all of the servers in the cluster when you execute the query.
Run the query on that node or cluster on which you created the query	a. Select **Regular Query.** b. Select **Finish**.	

Step 3 Browse to the location to store the query, enter a name for the query in the File Name field.

Step 4 Select **Save**.

Step 5 Perform one of the following actions:

If you want to:	Action
Run the query that you have just saved	**a.** Select **Run Query.** **b.** Continue with Step 6.
Exit the query wizard without running the query that you created	Select **Cancel**.

Step 6 Perform one of the following actions after the query execution completes:

If you want to:	Action
View a file that you collected	Navigate to the file as follows; • Double-select **Query Results**. • Double-select the <node> folder, where <node> equals the IP address or host name for the server that you specified in the wizard. • Double-select the folder that contains the file that you want to view. • After you have located the file, double-select that file.
Download the trace files and the result file that contains a list of the trace files that your query collected	**a.** Select the files that you want to download **b.** Select **Download.** **c.** Specify the criteria for the download. **d.** Select **Finish**.
Specify the directory in which you want to download the trace files and the results file	**a.** Select **Browse** next to the Download all files field. **b.** Navigate to the directory. **c.** Select **Open**. **Note** The default specifies C:\Program Files\Cisco\Presence Serviceability\jrtmt\<server IP address>\<download time>
Create a zip file of the trace files that you collected	Select **Zip File.**
Delete collected log files from the server	Check **Delete Collected Log Files from Server.**
Save the query	**a.** Select **Save Query.** **b.** Complete Step 2 through Step 4.

Troubleshooting Tips

- 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 does not display in the Trace & Log Central windows.

- You can install some listed services or applications only on a particular node in the cluster. To collect traces for those services or applications, make sure that you collect traces from the server on which you have activated the service or application.
- The services that you have not activated also display, so you can collect traces for those services.
- After you have downloaded the trace files, you can view them by using the Local Browse option of the trace and log central feature.
- An error message displays if the service parameter values are exceeded or if the system is in code yellow.

Related Topics

Viewing Collected Trace Files Using Local Browse, page 6-19

How to Schedule Trace Collection

You can use the Schedule Collection option of the trace and log central feature to schedule recurring up to six concurrent trace collections and to download the trace files to an SFTP 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.

- Starting a Schedule, page 6-12
- Executing the Schedule, page 6-14

Starting a Schedule

Before You Begin

- Configure the information that you want to include in the trace files for the various services from the Trace Configuration window.
- If you want alarms to be sent to a trace file, select an SDI trace file as the alarm destination in the Alarm Configuration window.

Procedure

Step 1 Open Trace & Log Central.

Step 2 Double-select **Schedule Collection** in the tree hierarchy.

Step 3 Perform one of the following actions to collect trace on Cisco Unified Presence logs:.

If you want to:	Action
Collect traces for all services and applications for all servers in the cluster	**a.** Check **Select All Services on All Servers**. **b.** Select **Next**.
Collect traces for all services and applications on a particular server	**a.** Check the name of the server. **b.** Select **Next**.
Collect traces for particular services or applications on particular servers	**a.** Check the traces that apply. **b.** Select **Next.**
Continue the trace collection wizard without collecting traces for services or applications	Select **Next.**

Step 4 Perform one of the following actions to collect traces on system logs

If you want to:	Action
Collect all system logs for all servers in the cluster	**a.** Check **Select All Services on all Servers**. **b.** Select **Next**.
Collect traces for all system logs on a particular server	**a.** Check the name of the server. **b.** Select **Next**.
Collect traces for particular system logs on particular servers	Check the traces that apply. For example, to collect CSA logs, check **Cisco Security Agent**. To access user logs that provide information about users that are signing in and out, check **Security Logs**.
Continue the trace collection wizard without collecting traces for system logs	Select **Next.**

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

Step 6 Perform the following actions to specify the date and time that you want to start the trace collection:

a. Select the down arrow button next to the Schedule Start Date/Time field.

b. From the Date tab, select the appropriate date.

c. From the Time tab, select the appropriate time.

Step 7 To specify the date and time that you want to end the trace collection, perform the following actions:

a. Select the down arrow button next to the Schedule End Date/Time field.

b. From the Date tab, select the appropriate date.

c. From the Time tab, select the appropriate time.

Troubleshooting Tips

- The time zone of the client computer 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 list box.

- 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.

Related Topics

- *Serviceability Configuration and Maintenance Guide for Cisco Unified Presence*

What To Do Next

Executing the Schedule, page 6-14

Executing the Schedule

Procedure

Step 1 Select how often you want to run the configured trace collection from the Scheduler Frequency list box.

Step 2 Specify the time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect traces.

Step 3 Enter the word or phrase in the Search String field to search by phrases or words that exist in the trace file. The tool searches for an exact match to the word or phrase that you enter and only collects those files that match the search criteria.

Step 4 Check **Zip All Files** to create a zip file of the trace files that you collect.

Step 5 Check **Delete Collected Log Files from the Server** to delete collected log files from the server.

Step 6 Perform one or more of the following actions:

If you want to:	Action
Download Files	**a.** Select **Download Files.** **b.** In the SFTP Server Parameters group box, enter the server credentials for the server where the trace and log central feature downloads the results. **c.** Select **Test Connection**. **d.** After the trace and log central feature verifies the connection to the SFTP server, select **OK**.
Run Another Query	**a.** Select **Run Another Query.** **b.** Select **Browse** to locate the query that you want to run. **c.** Select **OK**.
Generate Syslog	Select **Generate Syslog.**

Step 7 Select **Finish**.

Troubleshooting Tips

- 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 does not display in the Trace & Log Central windows.

- If the Real-Time Monitoring Tool cannot access the SFTP server, a message displays. Verify that you entered the correct IP address, user name, and password.
- 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 server on which you have activated the service/application.
- The services that you have not activated also display, so you can collect traces for those services.
- 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.
- 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 parameters fields: /home/<user>/Trace.
- The trace and log central feature only executes the specified query if the first query generates results.

Viewing Trace Collection Status and Deleting Scheduled Collections

You can view trace collection event status and delete scheduled trace collections. Available job types include Scheduled Job, OnDemand, RealTimeFileMon, and RealTimeFileSearch. Available statuses include Pending, Terminated, Running, Cancel, and Terminated.

Procedure

Step 1 Open Trace & Log Central.

Step 2 Perform one of the following actions:

a. Double-select **Job Status** in the Quick Launch Channel.

b. Select **System > Tools > Trace > Job Status**.

Step 3 Select the server for which you want to view or delete trace collection events from the Select a Node list box.

Step 4 Select the event that you want to delete and select **Delete**.

Step 5 Select **OK** when the confirmation message displays.

Troubleshooting Tips

- You can only delete jobs with a status of “Pending” or “Running” and a job type of “ScheduleTask.”
- Cisco Unified Presence does not support the Q931 Translator. Cisco Unified Presence does not support QRT report information.

Collecting a Crash Dump

You can collect a crash dump file for one or more servers on your network.

Procedure

Step 1 Open the Trace & Log Central.

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

Step 3 Perform one of the following actions:

If you want to:	Action
Collect crash dump files for all services and applications for all servers in the cluster	**a.** Check **Select All Services on All Servers**. **b.** Select **Next**.
Collect crash dump files for all services and applications on a particular server	**a.** Check the name of the server. **b.** Select **Next**.
Collect crash dump files for particular services or applications on particular servers	**a.** Check the traces that apply. **b.** Select **Next.**
Continue the collect crash dump wizard without collecting traces for services or application	Select **Next.**

Step 4 Perform one of the following actions to collect crash dump files on system logs

If you want to:	Action
Collect all system logs for all servers in the cluster	**a.** Check **Select All Services on all Servers**. **b.** Select **Next.**
Collect crash dump files for all system logs on a particular server	**a.** Check the name of the server. **b.** Select **Next.**
Collect crash dump files for particular system logs on particular servers	Check the traces that apply. For example, to collect CSA logs, check **Cisco Security Agent**. To access user logs that provide information about users that are signing in and out, check **Security Logs**.
Continue the collect crash dump wizard without collecting traces for system log	Select **Next**.

Step 5 Specify the time zone and time range for which you want to collect traces in the Collection Time group box. Select one of options specified in Time Zone and Date Range for Trace Collection, page 6-2.

Step 6 Select the partition that contains the logs for which you want to collect traces from the Select Partition list box.

Step 7 Perform one of the following actions:

If you want to:	Action
Specify the directory in which you want to download the crash dump files	**a.** Select **Browse** next to the Download File Directory field. **b.** Navigate to the directory. **c.** Select **Open**. **Note** The default specifies C:\Program Files\Cisco\Presence Serviceability\jrtmt\<server IP address>\<download time>.
Create a zip file of the crash dump file that you collect	Select **Zip File.**
Download the crash dump files without zipping the files	Select **Do Not Zip Files**.
Delete collected crash dump files from the server	Check **Delete Collected Log Files from the server**.

Step 8 Select **Finish**.

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

Troubleshooting Tips

- 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 does not display in the Trace & Log Central windows.
- 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 server on which you have activated the service/application.
- The services that you have not activated also display, so you can collect traces for those services.
- You cannot download a zipped crash dump file that exceeds two gigabytes. If you chose the **Zip File** radio button and the crash dump files exceed two 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 selected. Select the **Do Not Zip Files** radio button, and try the collection again.

Related Topics

- Viewing Collected Trace Files Using Local Browse, page 6-19
- How to Use Remote Browse to View Collected Trace Files, page 6-20
- How to Use Real-Time Trace to View Trace Files, page 6-24
- Updating the Trace Configuration Setting for RTMT, page 6-27

Collecting Audit Logs

In Cisco Unified Presence Release 8.6(4), you can collect information about various changes to the Cisco Unified Presence system. For more information about the different types of audit logs, see the *Serviceability Guide for Cisco Unified Presence*.

Note The audit user can collect, view, and delete the audit logs while an end user can only view the audit logs.

Procedure

Step 1 Display the Trace & Log Central tree hierarchy, as described in Viewing Trace & Log Central Options in RTMT, page 6-3.

Step 2 Select **Audit Logs**.

Step 3 In the **Action Options** dialog box, select one of the following:

- Browse Audit Logs
- Download Audit Logs
- Schedule Download of Audit Logs

Note These options are only available in RTMT version 8.9.

Step 4 Click **Next**.

Step 5 In the **Nodes Selection Options** dialog box, choose either **Select All Servers** or **<cup-server>**, where <cup-server> indicates the hostname of your server.

Step 6 Click **Finish**

Step 7 The Nodes pane displays.

Step 8 On the left side of the Nodes pane, double-click on the **Nodes** folder.

Step 9 Select **<servername> > System > Cisco Audit Logs** and choose one of the following options:

- **vos**—this option is applicable to System Audit Logs.
- **AuditApp**—this option is applicable to Application Audit Logs.
- **informixauditlogs**—this option is applicable to Database Audit Logs.

Step 10 Select an audit log file and perform one of the following actions:

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

  The Select Download Options wizard displays.

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

  – To create a zip file of the audit log files that you collect, select **Zip all Files** .

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

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

  - Click **Finish**.
- To delete the selected audit log file, click **Delete**.
- To refresh the selected audit log file, select either the relevant Cisco Audit Logs, System or [CUP-Hostname] nodes and click **Refresh**.

Step 11 You have completed the steps for Browse Audit Logs.

Viewing Collected Trace Files 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.

If you zipped the trace files when you downloaded them to your PC, you must unzip them to view them by using the viewers within the Real-Time Monitoring Tool.

Before You Begin

Collect traces files as described in Collecting Trace Files, page 6-5.

Procedure

Step 1 Open Trace & Log Central.

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

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

Step 4 Double-select the file to display the results.

Step 5 Perform the following actions:

a. Select on the program (viewer) that you would like to use to view the file.

b. If the program is not on the list, select another program by selecting **Other**.

c. If you wish to use this program as your default viewer, check **Always use this program to open these files**.

Troubleshooting Tips

- The Real Time Monitoring Tool (RTMT) 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.
- Cisco Unified Presence does not support the Q931 Translator. Cisco Unified Presence does not support QRT report information.

Related Topics

- Collecting Trace Files, page 6-5

- How To Use the Query Wizard, page 6-8
- How to Schedule Trace Collection, page 6-12

How to Use Remote Browse to View Collected Trace Files

- Setting Trace Collection Attributes, page 6-20
- Viewing the Trace Results, page 6-22

Setting Trace Collection Attributes

Before You Begin

Collect traces files as described in Collecting Trace Files, page 6-5.

Procedure

Step 1 Open Trace & Log Central.

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

Step 3 Select the appropriate radio button, Trace Files or Crash Dump.

Step 4 Select **Next**.

Step 5 Perform one of the following actions:

a. If you select Trace Files, go to Step 6.

b. If you select Crash Dump, go to Step 8.

Step 6 Perform one of the following actions in the CUP Applications/Services tab:

If you want to:	Action
Collect traces for all services and applications for all servers in the cluster	a. Check **Select All Services on All Servers**. b. Select **Next.**
Collect traces for all services and applications on a particular server	a. Check the name of the server. b. Select **Next**.
Collect traces for particular services or applications on particular servers	a. Check the traces that apply. b. Select **Next**.
Continue the trace collection wizard without collecting traces for services or applications	Select **Next**.

Step 7 Perform one of the following actions in the Select System Services/Application tab:

If you want to:	Action
Collect all system logs for all servers in the cluster	a. Check **Select All Services on all Servers**. b. Select **Next**.
Collect traces for all system logs on a particular server	a. Check the name of the server. b. Select **Next**.

If you want to:	Action
Collect traces for particular system logs on particular servers	**a.** Check the traces that apply. **Note** For example, to collect CSA logs, check **Cisco Security Agent**. To access user logs that provide information about users that are signing in and out, check **Security Logs**. **b.** Select **Next**.
Continue the remote browse wizard without collecting traces for system logs	Go to Step 10.

Step 8 Perform one of the following actions in the CUP Applications/Services tab:.

If you want to:	Action
Collect crash dump files for all services and applications for all servers in the cluster	**a.** Check **Select All Services on All Servers**. **b.** Select **Next**.
Collect crash dump files for all services and applications on a particular server	**a.** Check the name of the server. **b.** Select **Next**.
Collect crash dump files for particular services or applications on particular servers	**a.** Check the traces that apply. **b.** Select **Next.**

Step 9 Perform one of the following actions in the Select System Services/Application tab:.

If you want to:	Action
Collect crash dump files for all services and applications for all servers in the cluster	**a.** Check **Select All Services on All Servers**. **b.** Select **Next**.
Collect crash dump files for all services and applications on a particular server	**a.** Check the name of the server. **b.** Select **Next**.
Collect crash dump files for particular services or applications on particular servers.	**a.** Check the traces that apply. **b.** Select **Next.**
Continue the collect crash dump wizard without collecting crash dump files	Go to Step 10.

Step 10 Select **Finish**.

Related Topics

- Collecting Trace Files, page 6-5
- How To Use the Query Wizard, page 6-8
- How to Schedule Trace Collection, page 6-12

What To Do Next

Viewing the Trace Results, page 6-22

Viewing the Trace Results

Before You Begin

Set your trace collection attributes.

Procedure

Step 1 Select **Close** when a message states that the trace results are available.

Step 2 Perform one of the following actions::

If you want to:	Action
To display the results	**a.** Perform one of the following actions to navigate to the file: – Right-select the mouse to select the type of program that you would like to use to view the file. – Double-select the file to display the file in the default viewer.
Download the trace files and the result file that contains a list of the trace files that your query collected	**a.** Select the files that you want to download. **b.** Select **Download.** **c.** Specify the criteria for the download. **d.** Select **Finish**.
Specify the directory in which you want to download the trace files and the results file	**a.** Select **Browse** next to the Download all files field. **b.** Navigate to the directory. **c.** Select **Open**. The default specifies C:\Program Files\Cisco\Presence Serviceability\jrtmt\<server IP address>\<download time>
Create a zip file of the trace files that you collected	Check **Zip File.**
Delete collected log files from the server	Check **Delete Collected Log Files from Server.**
Delete trace files from the node	**a.** Select the file that displays in the pane on the right side of the window**.** **b.** Select **Delete**.
Refresh a specific service or node	**a.** Select the server name or service. **b.** Select **Refresh.** **c.** Select **Close** when a message states that the remote browse is ready.
Refresh all services and nodes that display in the tree hierarchy	**a.** Select **Refresh All.** **b.** Select **Close** when a message states that the remote browse is ready.

Troubleshooting Tips

- You can install some listed services/applications only on a particular node in the cluster. To select traces for those services/applications, make sure that you select traces from the server on which you have activated the service/application.
- The services that you have not activated also display, so you can select traces for those services.
- After you have downloaded the trace files, you can view them by using the Local Browse option of the trace and log central feature.

- To sort the files that displays in the pane, select a column header; for example, to sort the files by name, select 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.
- Cisco Unified Presence does not support the Q931 Translator. Cisco Unified Presence does not support QRT report information.

Related Topics

- Setting Trace Collection Attributes, page 6-20
- Viewing Collected Trace Files Using Local Browse, page 6-19

How to Use Real-Time Trace to View Trace Files

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.

- Viewing Real-Time Data, page 6-24
- Monitoring User Event, page 6-25

Viewing 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, five of which can exist on a single node. The log viewer refreshes every five 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 Trace & Log Central.

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

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

Step 4 Select the node for which you want to view real-time data and select **Next**.

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

Step 6 Perform one of the following actions:

a. Check **Enable Auto-Scrolling** to keep the cursor at the end of the window to display new traces as they appear.

b. Uncheck **Enable Auto-Scrolling** if you do not want the cursor to move to the bottom of the window as new traces display.

Step 7 Repeat this procedure to view data for additional services.

Step 8 Select **Close** on the Generic Log Viewer when you have finished viewing the real-time data.

Troubleshooting Tips

- You can view data for up to 10 services, five of which can exist on a single node. A message displays if you attempt to view data for too many services or too many services on a single node.
- 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 does not display in the Trace & Log Central windows.
- The services that you have not activated also display, so you can collect traces for those services.
- Cisco Unified Presence does not support the Q931 Translator. Cisco Unified Presence does not support QRT report information.

Monitoring 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 five seconds. If the search string occurs more than once in one polling interval, the system only performs the action once. For each event, you can monitor one service on one node.

Before you Begin

If you want to generate an alarm when the specified search string exists in a monitored trace file, enable the TraceCollectionToolEvent alert.

Procedure

Step 1 Open Trace & Log Central.

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

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

Step 4 Perform one of the following actions:

If you want to:	Action
View the monitoring events that you have already set up	a. Select **View Configured Events**. b. Select a server from the list box. c. Select **Finish**.
Configure new monitoring events	a. Select **Create Events.** b. Select **Next**. c. Continue with Step 5.

Step 5 Select the node that you want the system to monitor from the **Nodes** list box and select **Next**.

Step 6 Select the service and the trace file type that you want the system to monitor and select **Next**.

Step 7 Specify the phrases or words that you want the system to locate in the trace files in the **Search String** field. 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.

Step 9 Perform one of the following actions to indicate what you want the system to do when it encounters the search string that you specified in the Search String fields:

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 RTMT
Store the syslog messages on a syslog server	**a.** Check **Remote Syslog.** **b.** Enter the syslog server name in the **Server Name** field.
Download the trace files that contain the specified search string	**a.** Check **Download File.** **b.** Enter the server credentials for the server where you want to download the trace files in the SFTP Server Parameters group box. **c.** Select **Test Connection**. **d.** Select **OK** after the Trace and Log Central feature verifies the connection to the SFTP server.

Step 10 Select **Finish**.

Troubleshooting Tips

- 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 does not display in the Trace & Log Central windows.
- The services that you have not activated also display, so you can collect traces for those services
- To delete an event, select the event and select **Delete**.
- 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 parameters fields: /home/<user>/Trace.
- 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.
- Cisco Unified Presence does not support the Q931 Translator. Cisco Unified Presence does not support QRT report information.

Related Topics

- How To Configure Alert Actions, page 5-9
- Time Zone and Date Range for Trace Collection, page 6-2

Updating the Trace Configuration Setting for RTMT

From RTMT, 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.

Procedure

Step 1 Select **Edit > Trace Settings.**

Step 2 Select the radio button that applies.

Troubleshooting Tips

- The Error radio button represents the default setting.
- The system stores the rtmt.log file in the logs directory where you installed the RTMT plug-in; for example, C:\Program Files\Cisco\Presence Serviceability\jrtmt\log.