Getting Started

Install and Configure Unified RTMT

Install Unified RTMT

Note

- Only the administrators with Standard Audit Users and Standard CCM Super Users privileges have access to Unified RTMT features. If an application user without these privileges logs into Unified RTMT, some of the features such as Call Control Discovery (CCD) and Service Advertisement Framework (SAF) will not work as expected.
- The current Unified RTMT download supports earlier releases of Unified Communications Manager, IM and Presence Service, and Unity Connection. Verify that the Unified RTMT version that you install is compatible with the product that you are monitoring. If the Unified RTMT version that you are using is not compatible with the server that you want to monitor, the system prompts you to download the compatible version.
- Your computer stores the user preferences, such as the IP address and Unified RTMT frame size, based on the latest instance of Unified RTMT that you run.

Before you begin

- The current Unified RTMT requires JRE to run. Verify that the system has JRE installed (Java 1.8).
- Download the CiscoRTMTPlugin.zip file for installation.
- Unified RTMT requires at least 128 MB in memory to run on a Windows OS platform; the tool requires at least 300 MB of disk space to run on a Windows/Linux OS platform.

Note Red Hat Linux installation with KDE or GNOME client installed on Linux machines.

Procedure

Step 1 Go to the **Plug-ins** window of the administration interface for your configuration:

Interface	How to access
Cisco Unified Communications Manager	From Unified Communications Manager Administration, choose **Application** > **Plugins**.
Cisco Unified Communications Manager IM and Presence Service	From Unified Communications Manager IM and Presence Administration, choose **Application** > **Plugins**.
Cisco Unity Connection	From Cisco Unity Connection Administration, choose **System Settings** > **Plugins**.

Step 2 Click **Find**.

Step 3 To install Unified RTMT on a client that is running on Linux or Microsoft Windows operating system, download the CiscoRTMTPlugin.zip from the **Download** link for the Cisco Unified Real-Time Monitoring Tool - Windows and Linux Tool.

Tip When you install Unified RTMT on Windows 10 or later, only administrators with privileges can launch RTMT.

Step 4 Download the CiscoRTMTPlugin.zip to the preferred location on your client machine.

Step 5 To install the Windows version,

a) Unzip the CiscoRTMTPlugin.zip file.
b) Double-click the `run.bat` file.

Step 6 To install the Linux version,

a) Unzip the CiscoRTMTPlugin.zip file.
b) Once the files are extracted, you must set permissions to the `run.sh` file by executing the command **chmod 755 run.sh**.
c) Double-click the `run.sh` file.

Note You can add desktop shortcut icons to the home directory for the `run.bat` or the `run.sh` files. See Create shortcut to launch Unified RTMT (Optional), on page 3.

Create shortcut to launch Unified RTMT (Optional)

You can add desktop shortcut icons to the home directory for the `run.bat` (Windows) or the `run.sh` (Linux) version files.

Procedure

Step 1 To install the Windows version,

a) Right-click the desktop or preferred location and select **New and Shortcut**.
b) Browse to the location where the `run.bat` file is unzipped in the CiscoRTMTPlugin.zip folder and click **OK** after selecting the file.
c) Click the **Next** button to type in a name for the shortcut (for example, Unified RTMT 15), and then click **Finish**.
d) Double-click the shortcut to launch Unified RTMT.

Step 2 To install the Linux version,

a) Right-click the desktop or preferred location and select **Create New** and **Link to Location (URL)...** to the location.
b) Browse to the location where the `run.sh` file is unzipped in the CiscoRTMTPlugin.zip folder, provide a name for the shortcut, and click **OK**.
c) Double-click the shortcut to launch Unified RTMT.

Upgrade RTMT

Tip To ensure compatibility, we recommend that you upgrade RTMT after you complete the upgrade on all servers in the cluster.

RTMT saves user preferences and downloaded module jar files locally on the client machine. The system saves user-created profiles in the database, so you can access these items in Unified RTMT after you upgrade the tool.

Note Before you upgrade to a newer version of RTMT, we recommend that you delete the previous or older versions of the unzipped CiscoRTMTPlugin.zip folder.

To upgrade RTMT, see Install Unified RTMT, on page 1.

Launch Unified RTMT

Before you begin

For single sign-on in Windows 10 and above, run Unified RTMT as an administrator.

Note Ensure that the required hostnames for the Unified Communications Manager clusters are reachable from your local machine for the Unified RTMT functionalities to work properly.

This requires adding the hostnames to the host file on the local machine. For example:

- For Unified RTMT running on Windows OS platform, use the following format to update the host file located at `C:\Windows\System32\drivers\etc\hosts`: **<ServerIP> <Hostname> <FQDN>**
- For Unified RTMT running on Linux OS platform, use the following format to update the host file located at

  `->/etc/hosts`: **<ServerIP> <Hostname> <FQDN>**

If there is a latest version of the tzupdater.jar file available, download the tzupdater.jar files to the JRE_HOME/bin directory used by Unified RTMT before launching Unified RTMT. It's required to update the time zone of your system's JRE used by Unified RTMT to that of the server that Unified RTMT tries to connect.

Procedure

Step 1 After you extract the CiscoRTMTPlugin.zip folder, open the folder and double-click the `run.bat` file for Windows client or the `run.sh` file for Linux clients.

Before launching Unified RTMT on Windows 10 or above, ensure that the User Account Control (UAC) feature is disabled. For more information on UAC feature, go to this URL: https://docs.microsoft.com/en-us/windows/desktop/uxguide/winenv-uac.

Step 2 If you choose to synchronize the time zone, perform the following steps.

a) Open the command prompt and navigate to JRE_HOME/bin directory used by Unified RTMT.

b) Verify the existing time zone version using the TZUpdater tool with the following command, which is: **java -jar tzupdater.jar -V**

Important To update the time zone data successfully, you should ensure that you have sufficient privileges to modify the JDK_HOME/jre/lib or JRE_HOME/lib directory used by Unified RTMT. If you don't have sufficient privileges to modify these directories, contact your system administrator.

c) Download a copy of the desired tzdata.tar.gz bundle to a local directory from http://www.iana.org/time-zones/.

d) Enter the following command, which is: **Java -jar tzupdater.jar -l < location of tzdata.tar.gz bundle>**

Note -l supports URL protocols. For example, http://www.iana.org/time-zones/repository/tzdata-latest.tar.gz. The supported URL protocols are http://, https://, file://. If no URL link is provided, then the tool uses the latest IANA tzdata bundle at http://www.iana.org/time-zones/repository/tzdata-latest.tar.gz.

For more information on the time zone updates, see http://www.oracle.com/technetwork/java/javase/tzupdater-readme-136440.html.

e) Check the time zone version updated in your system by using the TZUpdater tool with the following command, which is: **java -jar tzupdater.jar -V**

f) Relaunch Unified RTMT.

Important Run the commands as an Administrator.

Step 3 In the **Host IP Address** field, enter either the IP address or hostname of the node or (if applicable) the node in a cluster.

Step 4 Click **OK**.

- If the single sign-on feature is enabled, Unified RTMT launches another browser to sign in with the IdP credentials. After successful authentication, the administrator is redirected to the Unified RTMT home screen.

  Note For IdPs enabled with certificate-based authentication, ensure that you use CA signed certificates for the following:

  - Launch Unified RTMT using certificate based authentication—Windows, on page 6
  - Launch Unified RTMT using certificate based authentication—Linux, on page 6

- If the single sign-on isn't enabled, Unified RTMT displays another window prompting for the username and password. Enter the details as given in the following steps.

Step 5 In the **User Name** field, enter the Administrator username for the application.

Step 6 In the **Password** field, enter the Administrator user password that you established for the username.

Note If the authentication fails or if the node is unreachable, the tool prompts you to reenter the node and authentication details, or you can click the **Cancel** button to exit the application. After the authentication succeeds, Unified RTMT launches the monitoring module from local cache or from a remote node, when the local cache doesn't contain a monitoring module that matches the back-end version.

Step 7 When prompted, add the certificate store by clicking **Yes**.
Unified RTMT starts.

Note If you sign in using the single sign-on feature, Unified RTMT prompts to enter the username and password after you click any one of the following menus:

- **System** > **Performance** > **Performance log viewer**
- **System** > **Tools** > **Trace and Log Central**
- **System** > **Tools** > **Job status**
- **System** > **Tools** > **Syslog Viewer**
- **Voice/Video** > **CallProcess** > **Session Trace**
- **Voice/Video** > **CallProcess** > **Called Party Tracing**
- **Voice/Video** > **Report** > **Learned Pattern**
- **Voice/Video** > **Report** > **SAF forwarders**
- **Analysis Manager**

What to do next

You can create a user with a profile that is limited only to Unified RTMT usage. The user will have full access to Unified RTMT but won't have permission to administer a node.

You can create a Unified RTMT user by adding a new application user in the administration interface and adding the user to the predefined Standard RealtimeAndTraceCollection group.

Launch Unified RTMT using certificate based authentication—Windows

Before you begin

- Oracle JDK (1.8)/OpenJDK (1.8) with JFX module should be installed
- Client certificates should be imported into the Windows systems keystore before launching the Unified RTMT application

Procedure

Step 1 Press **Windows+R** and type **mmc** to launch the Microsoft Management Console.

Step 2 Navigate to the File Menu and select **Add/Remove Snap-In** option.

Step 3 Add the Certificates option from the **Available Snap-in** drop-down list.

Step 4 Choose "**My user account**" and finish the task by clicking the **OK** button.

Step 5 Select **Certificates (Current user) > Personal** from the Certificates Tree.

Step 6 Right-click on the certificate screen to import the user certificate into the system keystore.

Step 7 Launch Unified RTMT using the `run.bat` file to start using the user certificate.

When Unified RTMT displays the User Identification Request pop-up window, you must select a valid user certificate from the drop-down list.

Launch Unified RTMT using certificate based authentication—Linux

Follow the given procedure to import user certificates into the keystore and generate a new passphrase for the Unified RTMT certificate-based authentication.

Before you begin

- OpenSSL 3.0 version should be installed
- Oracle JDK (1.8)/OpenJDK (1.8) with JFX module rpm installed
- User keystore and passphrase should be generated with the `genkeystore.sh` file before launching Unified RTMT.

Procedure

Step 1 Upload the user certificate to a directory on the Linux server.

Step 2 Navigate to the `genkeystore.sh` script present in the Unified RTMT home directory (for example, `/home/user/JRTMTPlugin/genkeystore.sh`) and set permission to the `genkeystore.sh` file using the following command `chmod 755 genkeystore.sh`. For example, `sh genkeystore.sh`.

Enter the client certificate's absolute path `<Certificate path>` and then the passphrase `<Certificate passphrase>`.

Step 3 After the user certificate is successfully exported into the new keystore, relaunch Unified RTMT to start using this keystore.

Step 4 Launch Unified RTMT using the `run.sh` file to start using the user certificate.

When Unified RTMT displays the User Identification Request pop-up window, you must select a valid user certificate from the drop-down list.

Note To import another certificate into the Unified RTMT User Keystore, ensure that you rerun the `genkeystore.sh` script and relaunch Unified RTMT for the changes to reflect.

Multiple installations of Unified RTMT

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

- A Unified Communications Manager product on one node.
- An IM and Presence Service on one node.
- A Unity Connection product on one node.
- A node on a cluster to monitor the health of the cluster.

To monitor a product on a different node, you must use a new instance of Unified RTMT that is installed.

Multiple copies of Unified RTMT that are installed on your computer let you simultaneously monitor multiple Unified CM, IM and Presence Service, and Unity Connection that are installed on different nodes.

You can install multiple versions of Unified Communications Manager Unified RTMT on a single computer. You can also launch multiple instances of the same Unified RTMT from the downloaded zip file.

Note Your computer stores the user preferences, such as the IP address and Unified RTMT frame size, from the Unified RTMT client that last exits.

Uninstall Unified RTMT

To uninstall Unified RTMT, perform one of the following actions:

1. Close any active sessions of Unified RTMT.

2. Delete all instances of the unzipped CiscoRTMTPlugin.zip folders.

Administration Tools

System Interface

The Unified RTMT interface consists of the following components:

- **Menu bar**: the menu bar includes some or all of the following options, depending on your configuration:

  File

  Allows you to save, restore, and delete existing RTMT profiles, monitor Java Heap Memory Usage, go to the Serviceability Report Archive window in Cisco Unified Serviceability, log off, or exit RTMT.

Note

1. The RTMT menu option **File** > **Cisco Unified Reporting** lets you access Cisco Unified Reporting from RTMT. You can use the Cisco Unified Reporting application to snapshot cluster data for inspection or troubleshooting. For more information, see the *Cisco Unified Reporting Administration Guide*.
2. As part of creating the heap dump faster, a core(core.jvm.core) file is generated to make the heap dump creation process (generation) fast.

  System

  Allows you to monitor system summary, monitor server resources, work with performance counters, work with alerts, collect traces, and view syslog messages.

  Voice/Video

  Allows you to view Unified Communications Manager summary information on the server; monitor call-processing information; and view and search for devices, monitor services, and CTI.

  IM and Presence

  Allows you to view IM and Presence Service and Cisco Jabber summary information on the server.

  Cisco Unity Connection

  Allows you to view the Port Monitor tool.

  IME Service

  Allows you monitor server and network activity of the Cisco Intercompany Media Engine server.

  Edit

  Allows you to configure categories (for table format view), set the polling rate for devices and performance monitoring counters, hide the quick launch channel, and edit the trace setting for RTMT.

  Window

  Allows you to close a single RTMT window or all RTMT windows.

Application

Depending on your configuration, allows you to browse the applicable web pages for administration interfaces, Cisco Unified Serviceability, and Cisco Unity Connection Serviceability.

Help

Allows you to access RTMT online help documentation and to view the RTMT version.

- **Quick Launch channel**: Pane that displays information about the server or information about the applications. The tab contains groups of icons that you can click to monitor various objects.
- **Monitor pane**: Pane where monitoring results are displayed.

Performance Monitoring

Unified Communications Manager, Unified Communications Manager IM and Presence Service, and Cisco Unity Connection directly update Performance counters (called perfmon counters). The counters contain simple, useful information about the system and devices on the system, such as number of registered phones, number of active calls, number of available conference bridge resources, and voice messaging port usage.

You can monitor the performance of the components of the system and the components for the application on the system by choosing the counters for any object by using the Cisco Unified Real-Time Monitoring Tool. The counters for each object display when the folder expands.

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

RTMT integrates with existing software for performance monitoring:

- RTMT integrates with your administration and serviceability software.
- RTMT displays performance information for all system components.

RTMT provides alert notifications for troubleshooting performance. It also periodically polls performance counter to display data for that counter. You can choose to display perfmon counters in a chart or table format.

Performance monitoring allows you to perform the following tasks:

- Monitor performance counters from all Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection servers.
- Continuously monitor a set of preconfigured objects and receive notification in the form of an email message.
- Associate counter threshold settings to alert notification. An email or popup message provides notification to the administrator.
- Save and restore settings, such as counters that are being monitored, threshold settings, and alert notifications, for customized troubleshooting tasks.
- Display up to six perfmon counters in one chart for performance comparisons.
- Use performance queries to add a counter to monitor.

System summary status

The Real-Time Monitoring Tool provides a set of default monitoring objects that help you to monitor the health of the system. Default objects include performance counters or critical event status for the system and other supported services. The system summary in Unified RTMT allows you to monitor important common information in a single monitoring pane. In system summary, you can view information about the following predefined objects:

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

Server Status Monitoring

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

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

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

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

Note If more than one logical disk drive is available in your system, the system stores CTI Manager traces in the spare partition on the first logical disk and Cisco CallManager traces on the second logical disk. Unified RTMT monitors the disk usage for the spare partition in the **Disk Usage** window.

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

For a specific description of each state, see the following table.

Table 1: Status of Critical Services

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

Performance Counter Interface

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

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

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

Category Tabs

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

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

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

Sample Rate

The application polls the counters, devices, and gateway ports to gather status information.

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

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

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

Zoom In on Perfmon Counter

To get a closer look at perfmon counters, you can zoom in on a perfmon monitor counter in the RTMT.

Procedure

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

- To zoom in predefined objects, such as System Summary, perform one of the following actions:
  - Drag the mouse over the plot area in the counter to frame the data and release the mouse button. The counter zooms in the chart.
  - Click the counter. The counter zooms in.
- To zoom counters in the Performance pane, perform one of the following actions (and resize the window, if necessary):

- Double-click the counter that you want to zoom. The box with the counter appears highlighted and the Zoom window launches. The minimum, maximum, average, and last fields show the values for the counter since the monitoring began for the counter.
- Click the counter to select the counter to zoom. The box with the counter appears highlighted.
- Right-click the counter and select **Zoom Chart** or choose **System** > **Performance** > **Zoom Chart**. The **Zoom** window launches. The minimum, maximum, average, and last fields show the values for the counter since the monitoring began for the counter.

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

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

Highlight Charts and Graphs

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

Procedure

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

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

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

Counter Properties

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

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

Related Topics

Performance Counters and Alerts

Alert Notification for Counters

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

1. From the RTMT Perfmon Monitoring pane, choose the system perfmon counter.
2. Set up an email or a message pop-up window for alert notification.
3. Determine the threshold for the alert (for example, an alert activates when calls in progress exceed the threshold of over 100 calls or under 50 calls).
4. Determine the frequency of the alert notification (for example, the alert occurs once or every hour).
5. Determine the schedule for when the alert activates (for example, on a daily basis or at certain times of the day).

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.

Important From Release 14SU3 onwards, FTP server is no longer supported. We recommend that you use SFTP server for scheduled trace collections.

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 doesn't display in the trace file.

Related Topics

Cisco Unified Analysis Manager Setup

Trace Files Collection, Throttling, and Compression

The Collect Files option in Trace and Log Central collects traces for services, applications, endpoints, 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.

Configuration Profiles

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

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

Unified Communications Manager clusters only: Default profile also dynamically monitors all registered phones for all Unified Communications Manager servers in a cluster. If your cluster contains five configured Unified Communications Manager servers, CM-Default displays the registered phones for each server in the cluster, as well as calls in progress and active gateway ports and channels.

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

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

Related Topics

Add Configuration Profile

Categories

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

If you perform various searches for devices, for example, for phones, gateways, and so on, you can create a category for each search and save the results in the category.

Note Changes to the profile settings for the default profile on IM and Presence Service are not transferred to Unified Communications Manager. IM and Presence Service profiles are renamed with the prefix “Presence_”.

Related Topics

Add Category

Alerts

The system generates alert messages to notify administrators when a predefined condition is met, such as when an activated service goes from up to down. Alerts can be sent out as email or epage.

Unified RTMT, which supports alert defining, setting, and viewing, contains preconfigured and user-defined alerts. Although you can perform configuration tasks for both types, you cannot delete preconfigured alerts (whereas you can add and delete user-defined alerts).

Alert options

The Alert menu (**System** > **Tools** > **Alert**) comprises the following menu options:

- Alert Central: This option comprises the history and current status of every alert in the system.

Note You can also access Alert Central by selecting the Alert Central icon in the hierarchy tree in the system drawer.

- Set Alert/Properties: This menu option allows you to set alerts and alert properties.
- Remove Alert: This menu category allows you to remove an alert.

- Enable Alert: With this menu category, you can enable alerts.
- Disable Alert: You can disable an alert with this category.
- Suspend cluster/Node Alerts: This menu category allows you to temporarily suspend alerts on a particular IM and Presence node or on the entire cluster.
- Clear Alerts: This menu category allows you to reset an alert (change the color of an alert item from red to black) to signal that an alert has been taken care of. After an alert has been raised, its color automatically changes to in Unified RTMT and stays that way until you manually clear the alert.
- Clear All Alerts: This menu category allows you to clear all alerts.
- Reset all Alerts to Default Config: This menu category allows you to reset all alerts to the default configuration.
- Alert Detail: This menu category provides detailed information on alert events.
- Config Email Server: In this category, you can configure your email server to enable alerts.
- Config Alert Action: This category allows you to set actions to take for specific alerts; you can configure the actions to send the alerts to desired email recipients.

In Unified RTMT, you configure alert notification for perfmon counter value thresholds and set alert properties for the alert, such as the threshold, duration, frequency, and so on.

You can locate Alert Central under the Tools hierarchy tree in the quick launch. Alert Central provides both the current status and the history of all the alerts in the system.

Alert Fields

You can configure both preconfigured and user-defined alerts in Unified RTMT. You can also disable both preconfigured and user-defined alerts in Unified RTMT. You can add and delete user-defined alerts in the performance-monitoring window; however, you cannot delete preconfigured alerts.

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

The following table provides a list of fields that you may use to configure each alert; users can configure preconfigured fields, unless otherwise noted.

Table 2: Alert Customization

Field	Description	Comment
Alert Name	High-level name of the monitoring item with which Unified RTMT associates an alert	Descriptive name. For precon you cannot change this field. related to Alert Central displ of preconfigured alerts.
Description	Description of the alert	You cannot edit this field for alerts. See topics related to A displays for a list of preconfi

Field	Description	Comment
Performance Counter(s)	Source of the performance counter	You cannot change this field. Yo associate only one instance of th performance counter with an ale
Threshold	Condition to raise alert (value is...)	Specify up < - > down, less than greater than #, %, rate. This field applicable only for alerts based o performance counters.
Value Calculated As	Method used to check the threshold condition	Specify value to be evaluated as delta (present - previous), or % c field is applicable only for alerts performance counters.
Duration	Condition to raise alert (how long value threshold has to persist before raising alert)	Options include the system sendir immediately or after a specified the alert has persisted. This field applicable only for alerts based o performance counters.
Number of Events Threshold	Raise alert only when a configurable number of events exceeds a configurable time interval (in minutes).	For ExcessiveVoiceQualityRepo default thresholds equal 10 to 60 For RouteListExhausted and MediaListExhausted, the default to 60 minutes. This field is appli for event based alerts.
Node IDs (Applies to Unified Communications Manager and the IM and Presence Service)	Cluster or list of servers to monitor	Unified Communications Manag CiscoTFTP server, or first server. is applicable only for non-cluste alerts. **Note** When you deactivat CiscoCallManager a CiscoTFTP services server, the system c that server as remov the currently monito list. When you reacti CiscoCallManager a CiscoTFTP services server is added back settings are restored values.
Alert Action ID	ID of alert action to take (System always logs alerts no matter what the alert action.)	Alert action is defined first (see Customization topic). A blank fi indicates that e-mail is disabled.
Enable Alerts	Enable or disable alerts.	Options include enabled or disab

Field	Description	Comment
Clear Alert	Resets alert (change the color of an alert item from red to black) to signal that the alert is resolved	After an alert is raised, its co automatically changes to blac until you manually clear the a All to clear all alerts.
Alert Details (Applies to Unified Communications Manager and the IM and Presence Service)	Displays the detail of an alert (not configurable)	For ExcessiveVoiceQualityR RouteListExhausted, and MediaListExhausted, up to 30 details display in the current interval if an alert is raised in interval. Otherwise, the prev details in the previous interva DChannel OOS alert, the list OOS devices at the time the a appears.
Alert Generation Rate	How often to generate alert when alert condition persists	Specify every X minutes. (Ra every X minutes if condition Specify every X minutes up (Raise alert Y times every X condition persists.)
User Provide Text	Administrator to append text on top of predefined alert text	—
Severity	For viewing purposes (for example, show only Sev. 1 alerts)	Specify defaults that are prov predefined (for example, Err Information) alerts.

Related Topics

Performance Counters and Alerts

Alert Logs

The alert log stores the alert, which is also stored in memory. The memory is cleared at a constant interval, leaving the last 30 minutes of data in the memory. When the service starts or restarts, the last 30 minutes of the alert data load into the memory by the system reading from the alert logs on the server or on all servers in the cluster (if applicable). The alert data in the memory is sent to the RTMT clients on request.

Upon RTMT startup, RTMT shows all logs that occurred in the last 30 minutes in the Alert Central log history. The alert log is periodically updated, and new logs are inserted into the log history window. After the number of logs reaches 100, RTMT removes the oldest 40 logs.

The following filename format for the alert log applies: `AlertLog_MM_DD_YYYY_hh_mm.csv`.

The alert log includes the following attributes:

- Time Stamp: Time when RTMT logs the data
- Alert Name: Descriptive name of the alert
- Node: Server name for where RTMT raised the alert

- Alert Message: Detailed description about the alert
- Type: Type of the alert
- Description: Description of the monitored object
- Severity: Severity of the alert
- PollValue: Value of the monitored object where the alert condition occurred
- Action: Alert action taken
- Group ID: Identifies the source of the alert

The first line of each log file comprises the header. Details of each alert are written in a single line, separated by a comma.

Log Partition Monitoring Tool

Log Partition Monitoring (LPM), which is installed automatically with the system, uses configurable thresholds to monitor the disk usage of the log partition on a server. The Cisco Log Partition Monitoring Tool service starts automatically after installation of the system.

Every 5 minutes, Log Partition Monitoring uses the following configured thresholds to monitor the disk usage of the log partition and the spare log partition on a server:

- LogPartitionLowWaterMarkExceeded (% disk space): When the disk usage is above the percentage that you specify, LPM sends out an alarm message to syslog and an alert to RTMT Alert central. To save the log files and regain disk space, you can use trace and log central option in RTMT.
- LogPartitionHighWaterMarkExceeded (% disk space): When the disk usage is above the percentage that you specify, LPM sends an alarm message to syslog and an alert to RTMT Alert central.
- SparePartitionLowWaterMarkExceeded (% disk space): When the disk usage is above the percentage that you specify, LPM sends out an alarm message to syslog and an alert to RTMT Alert central. To save the log files and regain disk space, you can use trace and log central option in RTMT.
- SparePartitionHighWaterMarkExceeded (% disk space): When the disk usage is above the percentage that you specify, LPM sends a n alarm message to syslog and an alert to RTMT Alert central.

In addition, Cisco Log Partitioning Monitoring Tool service checks the server every 5 seconds for newly created core dump files. If new core dump files exist, Cisco Log Partitioning Monitoring Tool service sends a CoreDumpFileFound alarm and an alert to Alert Central with information on each new core file.

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

When the log partition monitoring services starts at system startup, the service checks the current disk space utilization. If the percentage of disk usage is above the low water mark, but less than the high water mark, the service sends a alarm message to syslog and generates a corresponding alert in RTMT Alert central.

To configure Log Partitioning Monitoring, set the alert properties for the LogPartitionLowWaterMarkExceeded and LogPartitionHighWaterMarkExceeded alerts in Alert Central.

To offload the log files and regain disk space on the server, you should collect the traces that you are interested in saving by using the Real-Time Monitoring tool.

If the percentage of disk usage is above the high water mark that you configured, the system sends an alarm message to syslog, generates a corresponding alert in RTMT Alert Central, and automatically purges log files until the value reaches the low water mark.

Note Log Partition Monitoring automatically identifies the common partition that contains an active directory and inactive directory. The active directory contains the log files for the current installed version of the software (Unified Communications Manager or Cisco Unity Connection), and the inactive directory contains the log files for the previous installed version of the software. If necessary, the service deletes log files in the inactive directory first. The service then deletes log files in the active directory, starting with the oldest log file for every application until the disk space percentage drops below the configured low water mark. The service does not send an e-mail when log partition monitoring purges the log files.

After the system determines the disk usage and performs the necessary tasks (sending alarms, generating alerts, or purging logs), log partition monitoring occurs at regular 5 minute intervals.

Cisco Unified Analysis Manager

The Cisco Unified Analysis Manager, a tool included with the Cisco Unified Real-Time Monitoring Tool, is used to perform troubleshooting operations. When the Unified Analysis Manager is launched, it collects troubleshooting information from your system and provides an analysis of that information. You can use this information to perform your own troubleshooting operation or to send the information to Cisco Technical Assistance for analysis.

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

After it is installed, the application can identify the supported Unified Communications (UC) products and applications that you have in your system and troubleshoot call failures across these UC applications, collecting trace and log files.

The Unified Analysis Manager supports the following products:

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

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

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

Related Topics

View Trace and Log Central Options

Services, Servlets, and Service Parameters

To support the Unified RTMT client, there are a number of services that needs to be active and running on the server. Unified RTMT uses the following services and servlets:

- Cisco AMC service: This service starts up automatically after the installation and allows Unified RTMT to retrieve real-time information that exists on nodes in the cluster. The IM and Presence service automatically assigns the first node as the primary collector. For Unified RTMT to continue to retrieve information when the primary collector fails, you must configure a subsequent node as the failover collector in Service Parameters in the administration interface.

  The following list comprises some Cisco AMC service parameters that are associated with Unified RTMT. For the latest list of parameters, select **System** > **Service Parameters** in the administrative interface. Then, select the server and the Cisco AMC service.

  - Primary Collector
  - Failover Collector
  - Data Collection Enabled
  - Data Collection Polling Rate
  - Server Synchronization Period
  - RMI Registry Port Number
  - RMI Object Port Number
  - Logger Enabled
  - Unified Communications Manager: Alarm Enabled
  - Unified Communications Manager: AlertMgr Enabled
  - Cisco Unity Connection: PerfMon Log Deletion Age
  - Cisco Unity Connection: AlertMgr Enabled

  For information about these service parameters, select the **?** button that displays in the Service Parameter configuration window of the administrative interface.

The following list comprises some network services and servlets that are associated with Unified RTMT. In Cisco Unified Serviceability, select **Tools** > **Control Center - Network Services** to view these services.

- Cisco CallManager Serviceability RTMT: Supports the Unified RTMT; this service starts up automatically after the installation.
- Cisco RIS Data Collector: The Real-time Information Server (RIS) maintains real-time information such as performance counter statistics, critical alarms generated, and so on. The Cisco RIS Data Collector service provides an interface for applications, such as Real-Time Monitoring Tool, SOAP applications, and AlertMgrCollector (AMC) to retrieve the information that is stored on the server.

- Cisco Tomcat Stats Servlet: The Cisco Tomcat Stats Servlet allows you to monitor the Tomcat perfmon counters by using Unified RTMT or the CLI. Do not stop this service unless you suspect that this service is using too many resources, such as CPU time.
- Cisco Trace Collection Servlet: The Cisco Trace Collection Servlet, along with the Cisco Trace Collection Service, supports trace collection and allows users to view traces by using the Unified RTMT client. If you stop this service on a server, you cannot collect or view traces on that server.
- Cisco Trace Collection Service: The Cisco Trace Collection Service, along with the Cisco Trace Collection Servlet, supports trace collection and allows users to view traces by using the Unified RTMT client. If you stop this service on a server, you cannot collect or view traces on that server.
- Cisco Log Partition Monitoring Tool: This service which starts up automatically after the installation, monitors the disk usage of the log partition on a server.
- Cisco SOAP-Real-Time Service APIs: The Cisco SOAP-Real-Time Service APIs, which start automatically after the installation, allow Unified RTMT to collect real-time information for devices and CTI applications.
- Cisco SOAP-Performance Monitoring APIs: This service, which starts up automatically after the installation, allows Unified RTMT to use performance monitoring counters for various applications through SOAP APIs.
- Cisco RTMT Reporter servlet: This service, which starts up automatically after the installation, allows you to publish reports for Unified RTMT.

Nonconfigurable Components

RTMTCollector, a component that is automatically installed with the application, logs preconfigured monitoring objects information while Alert Manager, also automatically installed, logs alert histories into log files. Each preconfigured object belongs to one of several categories: devices, services, nodes, call activities, and PPR. Each category uses a separate log file, and alert details are also logged in a separate file.

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

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

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

You can display log files, except an alert log file, by using the Performance log viewer in Unified RTMT or by using the native Microsoft Performance viewer. You can view an alert log file by using any text editor.

To download log files to a local machine, you can use the collect files option in Trace and Log Central in Unified RTMT.

Alternatively, from the CLI, you can use the file list command to display a list of files and the file get command to download files by SFTP. For more information about using CLI commands, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Log files exist in CSV format. New log files are created every day at 00:00 hours on the local system. For Unified Communications Manager clusters, new logs for devices, services, nodes, and calls are created when the time zone changes, when a new node is added to the cluster, or during failover/fallback scenarios. The first column of all these logs comprises the time zone information and the number of minutes from the Greenwich Meridian Time (GMT). RTMT Reporter uses these log files as a data source to generate daily summary reports. The report, which is based on the default monitoring objects, is generated every 24 hours for the following information:

- Call Activity Status: Number of calls attempted and number of calls completed for each Unified Communications Manager, each gateway, trunk, and overall cluster (if applicable). Number of channels available, in-service for each gateway.
- Device Status: Number of registered phones, gateways, and trunks per each node and overall cluster (if applicable).
- Server Status: percentage CPU load, percentage memory that is used, percentage disk space that is used per node.
- Service Status: (Unified Communications Manager) For each CTI Manager, number of opened devices and lines. For each TFTP server, number attempted and failed requests.
- Alert Status: Number of alerts per node. For Unified Communications Manager clusters, number of alerts per severity level for the cluster, including the top 10 alerts in the cluster.
- Performance Protection Report: Trend analysis information about default monitoring objects that allows you to track overall system health. The report includes information for the last 7 days for each node.

Tip The Unified RTMT reports appear in English only.

The following service parameters apply to Unified RTMT report generation: RTMT Reporter Designated node, RTMT Report Generation Time, and RTMT Report Deletion Age. For information about these parameters, go to the service parameter Help for your configuration:

Unified Communications Manager and **Unified Communications Manager IM and Presence Service**	Choose **Cisco Serviceability Reporter in the Service Parameter** window in Unified Communications Manager Administration and click the ? button.
Cisco Business Edition 5000	Choose **Cisco Serviceability Reporter in the Service Parameter** window in Unified Communications Manager IM and Presence Administration and click the ? button.
Cisco Unity Connection	On the **Service Parameters** window, in the Service drop-down list box, click a service and click **Help** > **This Page**.

For more information about the Serviceability reports, see the "Serviceability Reports" chapter in the *Cisco Unified Serviceability Administration Guide*.

Java Requirements for SAML SSO Login to RTMT via Okta

If you have SAML SSO configured with Okta as the identity Provider, and you want to use SSO to log in to the Cisco Unified Real-Time Monitoring Tool, you must be running a minimum Java version of 8.221. This requirement applies to 12.5(x) releases of Cisco Unified Communications Manager and the IM and Presence Service.