Troubleshooting Voice Application Components

Cisco Emergency Responder

Logs

The following logs provide information for debugging database related issues:

- Install or Upgrade logs: `/var/log/install/`
- Install DB logs: `/var/log/active/er/trace/dbl/sdi/`
- CERDbMon logs: `/var/log/install/`
- CLI logs: `/var/log/active/platform/log/`

For more information, go to:

https://www.cisco.com/c/en/us/support/unified-communications/emergency-responder/products-troubleshooting-guides-list.html.

Cisco Emergency Responder License Compliance

Cisco Emergency Responder sends licensing requirements to Cisco Prime License Manager and attempts to discover all phones on Cisco Unified Communications Manager, excluding subnets not tracked by Cisco

Emergency Responder. Cisco Prime License Manager computes the license requirements for all connected Cisco Emergency Responder product instances and compares the total license requirements to the total available installed licenses.

When upgrading from Cisco Emergency Responder Release 10.0 to 10.5(1) or higher, also upgrade the Cisco Emergency Responder license from Release 10.x to Release 10.5 or higher as appropriate. If these new licenses are not installed within 60 days of upgrading, the Cisco Emergency Responder system is affected in the following ways:

- Does not track or update unlicensed phone locations.
- Does not support unlicensed phones.
- Enters noncompliance mode.
- Generates email alerts and GUI warnings.

Important Failure to upgrade licenses does not impact 911 calls.

For more information, see the *Cisco Emergency Responder Administration Guide* : https://www.cisco.com/c/en/us/support/unified-communications/emergency-responder/products-troubleshooting-guides-list.html.

Cisco Unified Attendant Console-Premium Edition

Logs

The Logging Management option on the Engineering menu is used to enable or disable real-time logging of the following:

- Cisco Unified Attendant Console server
- Cisco Unified Attendant LDAP plug-in
- Cisco Unified Attendant CUPS plug-in
- Cisco Unified Attendant BLF plug-in

For more information, see Cisco Unified Attendant Console Premium Edition Web Admin, and Installation Guide, at:

https://www.cisco.com/c/en/us/support/unified-communications/unified-attendant-consoles/products-maintenance-guides-list.html

Troubleshooting Cisco Unified CM Modes Management

The following table provides the information on various cluster assignment scenarios of Cisco Unified CM modes management.

Table 1: Cisco Unified CM Modes Management Scenarios in Cluster Assignment

Error Message	Recommended Steps
Job status message: Assigning cluster <*clusterName*> to LM <*elmName*> failed.	Check the IP address of the specified cluster application.
Job status message: Assigning cluster <*clusterName*> to LM <*elmName*> failed.	Check if PLM is active, and reachable from the Cisco HCM-F node.
Job status message: Assigning cluster <*clusterName*> to LM <*elmName*> failed: no platform credential is configured.	Either add, or update the platform credentials of the specified cluster application in Cisco HCM-F.
Job status message: Assigning cluster <*clusterName*> to LM <*elmName*> failed: cluster is not allowed to be assigned.	Unassign the specified cluster, and then try to reassign.
Job status message: Assigning cluster <*clusterName*> to LM <*elmName*> failed: cluster is not allowed to be assigned.	Either try unassigning a cluster from PLM using the HCM-F GUI, or try assigning the specified cluster to some other PLM.
Job status message: Assigning cluster <*clusterName*> to LM <*elmName*> failed: cluster is not eligible to be assigned.	Add the publisher node information to the specified cluster application.

The following table provides the information on various cluster unassignment scenarios of Cisco Unified CM modes management.

Table 2: Cisco Unified CM Modes Management Scenarios in Cluster Unassignment

Error Messages	Recommended Steps
Job status message: Unassigning cluster <*clusterName*> from LM <*elmName*> failed.	Check if the specified cluster is present in PLM.
Job status message: Unassigning cluster <*clusterName*> from LM <*elmName*> failed.	Check if PLM is active, and reachable from the Cisco HCM-F node.
Job status message: Unassigning cluster <*clusterName*> from LM <*elmName*> failed: no platform credential is configured.	Either add, or update the platform credentials of the specified cluster in Cisco HCM-F.
Job status message: Unassigning cluster <*clusterName*> from LM <*elmName*> failed: LM does not exist.	Check the Cisco HCM-F logs for the detailed error message.

Cisco Unified Communications Manager IM and Presence Service

This section applies to Cisco Unified Communications Manager IM and Presence Service.

Troubleshoot Cisco Unified IM and Presence Service

From the Cisco Unified Communications Manager IM and Presence Administration page, select **Diagnostics** > **System Troubleshooter**. A GUI displays all the issues, and you can click to go through each error and resolve it.

Configure Cisco Unified IM and Presence Service Trace Settings

The Cisco Unified IM and Presence Service trace settings are normally set to Default. Follow the procedure below to change the settings if required for troubleshooting.

Procedure

Step 1 Select **Trace** > **Configuration**.

Step 2 From the Server drop-down list, select the server that is running the service for which you want to configure trace and click **Go**.

Step 3 From the Server Group drop-down list, select the service group for the service that you want to configure trace and click **Go**.

This table lists the services and trace libraries that correspond to the options that display in the Service Group list box.

Step 4 From the Service drop-down list, select the service for which you want to configure trace and click **Go**.

If you configure Troubleshooting Trace for this service, a message displays at the top of the window that indicates that Troubleshooting Traces have been set. The system disables all fields on the window except the Output Settings. To configure the Trace Output Settings, go to Step 10.

Step 5 Check **Apply to All Nodes** if you want trace to apply to all Cisco Unified IM and Presence Service servers in the cluster.

Step 6 Check **Trace On**.

Step 7 Select the level of information that you want traced from the Debug Trace Level list box. The Debug Trace Level options that display vary depending on which service you are tracing.

Step 8 Check the relevant trace check boxes for the service that you chose; for example, Cisco UP SIP Proxy Trace Fields.

Step 9 Check the trace fields that you want to enable if the service that you chose has multiple trace fields. Check **All Traces** to enable all trace fields.

Step 10 Specify the trace output setting to limit the number and size of the trace files.

Step 11 Perform one of the following actions:

- Select **Save** to save your trace parameters configuration.
- Select **Set Default** to set the default.

Unable to Delete a Voice Gateway

Symptoms: Unified CDM throws the error message `Macro function error - list index out of range` while deleting the voice gateway.

Resolution: Use Unified CDM bulk loader sheet to delete the voice gateway.

Troubleshooting Tips

- When you change either the Maximum No. of Files parameter or Maximum File Size (MB) parameter and the service is running, the system deletes all the service log files except the current file. If the service is not running, the system deletes the files when the service is initially turned on. To keep a record of the log files, download and save the service log files to another server before changing the Maximum No. of Files parameter or the Maximum File Size parameter.
- The changes to trace configuration take effect immediately for all services.
- The section in the Trace Filter Settings area that relates to devices is not relevant to Cisco IM and Presence Service.
- Depending on the service that you select and the traces that are generated by the service, some trace fields may be disabled or selected by default on the Trace Configuration screen.

For more information on serviceability configuration for Cisco IM and Presence Service, see the *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Cisco Unified Communications Manager Serviceability Trace

The traces for the Cisco Unified Communications Manager are normally set to Default. Cisco recommends that you change the trace setting for the Unified Communications Manager service to Detailed. Leave all other traces at Default for all call processing nodes.

Set the Unified Communications Manager Service Trace

Set the trace settings for the Unified Communications Manager service to **detailed**. Confirm that the maximum number of signaling distribution layer (SDL) files is 1500 and the file size is 10 MB. Make sure that the number of files and file size are the same for both the SDL and system diagnostic interface (SDI).

Procedure

Step 1 Log in to Cisco Unified Communications Manager Administration console.

Step 2 From the Navigation drop-down list on the top right of the screen, select **Cisco Unified Serviceability** and click **Go**.

Step 3 Select **Trace** > **Configuration**.

Step 4 From the Server drop-down list, select the Primary CallProcessing Node and click **Go**.

Step 5 From the Server Group drop-down list, select **CM Services** and click **Go**.

Step 6 From the Service drop-down list, select **Cisco CallManager (Active)** and click **Go**.

Step 7 On the UCM SDI Trace Page, confirm that the Debug Trace Level is set to the default of Detailed.

Step 8 Click **Apply to All Nodes**, and then **Save**.

Step 9 Select the SDL Configuration (top right).

Step 10 Make sure that the following defaults are in place: maximum number of files = 1500 and file size = 10 MB.

Step 11 Click **Apply to All Nodes**, and then **Save**.

SDI and SDL are interleaved. SDI traces are written to the SDL trace location, which is at /var/log/active/cm/trace/ccm/sdl/.

Trace Collection

Use the trace and log central feature, an option in the Cisco Unified Real-Time Monitoring Tool, to collect, view, and zip various service traces and other log files. With the Trace and Log Central option, you can collect SDL and SDI traces, application logs, system logs (such as Event View Application, Security, and System logs), and crash dump files.

Note Do not use the Notepad application to view collected trace files, because Notepad does not properly display line breaks.

For more information on trace collection, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Trace Field Descriptions

For some services, you can activate trace for specific components instead of enabling all trace for the service. The following list includes the services for which you can activate trace for specific components. Click the cross-reference to go to the applicable section where a description displays for each trace field for the service. If a service does not exist in the following list, the Enable All Trace check box displays for the service in the Trace Configuration window.

The following services apply to Cisco Unified Communications Manager and Cisco Unity Connection:

- Database Layer Monitor Trace Fields
- Cisco RIS Data Collector Trace Fields

The following services apply to Cisco Unified Communications Manager only:

- Cisco CallManager SDI trace fields
- Cisco CallManager SDL trace fields
- Cisco CTIManager SDL trace fields
- Cisco Extended Functions trace fields
- Cisco Extension Mobility trace fields

- Cisco IP manager assistant trace fields
- Cisco IP voice media streaming app trace fields
- Cisco TFTP trace fields
- Cisco Web Dialer Web Service Trace fields
- Database layer monitor trace fields
- Cisco RIS data collector trace fields
- Cisco CallManager SDI trace fields
- Cisco CallManager SDL trace fields
- Cisco CTIManager SDL trace fields
- Cisco Extended Functions trace fields
- Cisco Extension Mobility trace fields
- Cisco IP manager assistant trace fields
- Cisco IP voice media streaming app trace fields
- Cisco TFTP Trace fields
- Cisco Web Dialer Web Service Trace fields

For more information on serviceability configuration for Cisco IM and Presence Service, see the *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Enable Translation Pattern Printing for HCS Looping Dial Plan

Configure the translation patterns in Cisco Unified Communications Manager to allow the generation of SDL logs when performing the digit analysis of HCS looping dial plan. The SDL logs capture the looping dial plan translation pattern during call processing. For more information about the HCS Looping Dial Plan, see the Cisco Hosted Collaboration Solution, *Cisco Hosted Collaboration Solution Dial Plan Management Guide for Cisco Unified Communications Domain Manager, Release 10.x/11.5*

Note

- The Route List, Route Group, and Trunk information are not printed in SDL logs.
- Call Identifier (CI) and SIP Call ID are not printed in the Digit Analysis Results (DaRes).

Procedure

Step 1 Log in to Cisco Unified Communications Manager as a customer administrator.

Step 2 Choose **System > Service Parameters**.

Step 3 Select the following options:

- From the **Server** drop-down menu, select either**CUCM PUB server** or **CUCM SUB server**.
- From the **Service** drop-down menu, select **Cisco Call Manager (Active)**.

The **Cisco Call Manager (Active) Parameters** page is displayed.

Step 4 From the **System** group, click the drop-down menu next to **Digit Analysis Complexity** , and then select the **CompleteTranslationAndAlternatePatternAnalysis** parameter.

Step 5 Click Save.
The SDL logs are generated when you perform digit analysis of the HCS Looping dial plan.

Step 6 Configure and deploy the Serviceability Connector on Expressway C to collect logs for analysis. For more information on Serviceability Connector deployment, see Deployment Guide for Cisco Webex Serviceablity Connector.

Step 7 Add HCM-F as a managed device in Serviceability Connector and sync with HCM-F.
This configuration ensures to use the Serviceability Connector debugging capability for HCS Looping dial plan by the Cisco Support team.

Cisco Unity Connection Serviceability Trace

Cisco Unity Connection Serviceability provides both micro traces and macro traces that you enable individually or in any combination. After you enable the traces, access the trace log files through the Real-Time Monitoring Tool (RTMT) or the command line interface (CLI).

Note Before trace information is written to the log files, you must enable the micro traces or macro traces that provide the troubleshooting information in the areas that you select.

Configure Trace Log Files in Cisco Unity Connection

Procedure

Step 1 In Cisco Unity Connection Serviceability, select **Trace** > **Configuration**.

Step 2 On the Trace Configuration page, in the Server drop-down list, select the applicable Cisco Unity Connection server and click **Go**.

Step 3 From the Component drop-down list, select the component for which you want to configure trace log files and click **Go**.

Step 4 In the Maximum No. of Files field, enter the maximum number of trace log files that are created for this component.

Step 5 In the Maximum File Size field, enter the size limit (in megabytes) for the trace log files that are created for this component.

Step 6 To return to the default settings, select Set Default. Otherwise, proceed to the next step.

Step 7 Click **Save**.

Step 8 To have the new trace log files replace the old trace log files for this component, select Restart Log Files.

Enable Micro Traces in Cisco Unity Connection

Enable micro traces to troubleshoot problems with specific Cisco Unity Connection components. For example, if the Alert Central tool in the RTMT has notification errors, enable the Notifier trace. However, keep in mind that running traces can affect the system performance and hard-disk space.

Note Enabling micro traces decreases the system performance. Enable traces only for troubleshooting purposes.

Procedure

Step 1 In Cisco Unity Connection Serviceability, select **Trace** > **Micro Traces**.

Step 2 On the Micro Traces page, in the Server drop-down list, select the applicable Cisco Unity Connection server and click **Go**.

Step 3 From the Micro Trace drop-down list, select the microtrace that you want to enable and click **Go**.

Step 4 Under Micro-Trace Levels, check the check boxes for the microtrace levels that you want to enable.

Step 5 Click **Save**.

What to do next

You may need to enable traces in Cisco Unity Connection Serviceability and Cisco Unified Serviceability to troubleshoot Cisco Unity Connection issues. To troubleshoot Cisco Unity Connection components, enable traces in Cisco Unity Connection Serviceability. Similarly, to troubleshoot services that are supported in Cisco Unified Serviceability, enable traces in Cisco Unified Serviceability. For information on how to enable traces in Cisco Unified Serviceability, see the *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Enable Macro Traces in Cisco Unity Connection

Enable macro traces, which are preselected sets of micro traces, to troubleshoot general areas of Cisco Unity Connection functionality. For example, if there are MWI problems, enable the Traces for the MWI Problems macro trace. However, keep in mind that running traces can affect the system performance and hard-disk space.

Note Enabling macro traces decreases the system performance. Enable traces only for troubleshooting purposes.

Procedure

Step 1 In Cisco Unity Connection Serviceability, select **Trace** > **Macro Traces**.

Step 2 On the Macro Traces page, in the Server drop-down list, select the applicable Connection server and click **Go**.

Step 3 Check the check box of the macro trace that you want to enable.

Step 4 Expand the macro trace and check the check boxes for the levels that you want to enable.

Step 5 Click **Save.**

What to do next

You may need to enable traces in Cisco Unity Connection Serviceability and Cisco Unified Serviceability to troubleshoot Cisco Unity Connection issues. To troubleshoot Cisco Unity Connection components, enable traces in Cisco Unity Connection Serviceability. Similarly, to troubleshoot services that are supported in Cisco Unified Serviceability, enable traces in Cisco Unified Serviceability. For information on how to enable traces in Cisco Unified Serviceability, see the *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Recommended Traces

Look for a relevant macro trace. Always include the following:

- Conversation traces
- Call flow diagnostics

The following additional traces are available to focus on a specific problem:

- AvRdbSvr 11 (SQL query Generation)
- DOH 10+ & MALEx 10+ (Exchange Mailbox issues)
- notescommon 10+ & MALLn 10+ (Domino Issues)
- AvSaDbConn 10+ (SAWeb add/modify/delete issues)
- NodeMgr 10+ (failover issues)
- DSAD 10+ (Local Unity Objects to/from AD Sync)
- DSGlobalCatalog 10+ (Object not local to Unity to/from AD sync)
- DSDomino 10+ (Unity/from to Domino Sync)

For More Information

For more information on traces in Cisco Unity Connection, see the following:

- Diagnostic Traces in the *Troubleshooting Guide for Cisco Unity Connection* at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-troubleshooting-guides-list.html
- Using Traces in the *Administration Guide for Cisco Unity Connection Serviceability* at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html

Troubleshoot Dial Plan Without E.164 Mapping with Internal Numbers

The E.164 Number Association configuration is necessary in all the cases to support Direct Dial-In (DDI). However, if you plan to use a Type 4 dial plan and configure all the DNs with +E.164 numbers, you can avoid the E.164 Number Association configuration. Before deploying the site dial plan, update the dial plan schema with the following changes to bypass Directory Number (DN) Routing:

- Add Cu<cid>-DirNum-PT to the phone Line CSS.
- Add the Cu<cid>-DirNum-PT to the Cu<cid>-IngressFromUnity-CSS calling search space.

Ensure the following configuration in your system:

- Cisco Unity Connection must NOT be multitenant.
- Unified CM Multitenant must NOT share the same Cisco Unity Connection.
- The **Multi Tenant MWI mode** is turned off in the Unified CM **Service Parameters**.

Note You will face issues with the Message Waiting Indicator (MWI) if you do not follow the steps.

Cisco Webex Meetings

For more information, see *Cisco Webex Meetings Server Troubleshooting Guide*, at:

http://www.cisco.com/en/US/products/ps12732/prod_troubleshooting_guides_list.html

Note Cisco HCS 10.0(1) does not support on-premises Cisco Webex Meetings.

Troubleshoot Call Failures with RTMT

Cisco Unified Communications Manager is the core call processor. Unified Communications Manager can provide most of the data that is needed for all voice applications. However, there are instances where you must capture information from the respective applications.

Configure the PerfMon Log Settings

Procedure

Step 1 Log in to Cisco Unified CM Administration.

Step 2 Select **System** > **Service Parameters**.

Step 3 From the Server drop-down list, select the server for which you want to configure the PerfMon log settings.

Step 4 From the Service drop-down list, select **Cisco RIS Data Collector**.

Step 5 Specify the maximum number of log files to store on the disk. The system automatically purges files that exceed this limit by removing the oldest log file. The default value is 50 files.

Step 6 Specify the rollover criteria of the log file based on the maximum size of the file in megabytes. The default value is 5 MB.

Step 7 Repeat Step 3 to Step 6 for each server.

Step 8 Use the Trace and Log Central feature of the RTMT or CLI to collect the Cisco RIS Data Collector PerfMon log file.

The suggested polling rate is 5 seconds for RTMT and Cisco RIS Data Collector in Unified Communications Manager for RISDC in Service Parameters. The default settings for RISDC are 15 seconds polling rate and 10 seconds polling rate for RTMT. Change this setting to 5 seconds for On Demand Capture to troubleshoot memory, CPU, or any other performance degradation or issue. The default values are not granular enough for analysis, except for longevity-test captures of two or more days, in which case 15 seconds is acceptable.

RTMT Performance Monitoring

Benefits of using RTMT for performance monitoring include the following:

- RTMT integrates with existing software for performance monitoring.
- RTMT integrates with the administration and serviceability software for both Cisco Unified Communications Manager and Cisco Unity Connection.
- RTMT displays performance information for all Cisco Unified Communications Manager and Cisco Unity Connection components.

RTMT provides alert notifications for troubleshooting performance. RTMT also periodically polls the counters to display data for the counters.

Through performance monitoring you can perform the following tasks:

- Continuously monitor a set of preconfigured objects and receive notification in the form of an email message.
- Associate counter threshold settings with an alert notification. An email or pop-up message notifies the administrator.
- Save and restore settings, such as the counters being monitored, threshold settings, and alert notifications, for customized troubleshooting tasks.
- Display up to six performance counters in one chart for performance comparisons.
- Use performance queries to add a counter to monitor.

Performance Counter Interface

RTMT contains ready-to-view, predefined performance counters. You can also select, and add counters to monitor in RTMT. See the Performance Monitoring section in the *Cisco Unified Real-Time Monitoring Tool Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html for the following views and task information:

- To view predefined system counters, see Monitoring Predefined System Objects.
- To view predefined Cisco Unified Communications Manager counters, see Monitoring Predefined Cisco Unified Communications Manager Objects.
- To add a counter to monitor, see Working with Performance Queries.

RTMT displays performance counters in chart or table format. Chart format looks like a miniature window of information. Double click the counter in the PerfMon monitoring pane to display a particular counter.

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

Category Tabs

A category is 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. The 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 performance counters, devices, and alerts within that tab and then save your custom category by using Profile.

For More Information

For more information, see the following:

- *Cisco Unified Real-Time Monitoring Tool Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html
- *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html
- *Windows PerfMon Guide*
- Windows PerfMon is a useful tool for importing PerfMon files from either the RISDC Directory or RTMT OnDemand capture files.

Cisco Unified Communications Manager RTMT PerfMon Counters

- Cisco CallManager\CallManagerHeartBeat
- Cisco CallManager\CallsActive
- Cisco CallManager\CallsAttempted
- Cisco CallManager\CallsCompleted
- Cisco CallManager\CallsInProgress
- Cisco CallManager\InitializationState
- Cisco CallManager\RegisteredHardwarePhones
- Cisco CallManager\PartiallyRegisteredPhone
- Cisco CallManager\EncryptedCallsActive
- Cisco CallManager\EncryptedCallsCompleted
- Cisco CallManager\EncryptedRegisteredPhones
- Cisco CallManager\EncryptedPartiallyRegisteredPhones
- Cisco CallManager System Performance\AverageExpectedDelay
- Cisco CallManager System Performance\CallsRejectedDueToThrottling
- Cisco CallManager System Performance\CodeRedEntryExit
- Cisco CallManager System Performance\CodeYellowEntryExit
- Cisco CallManager System Performance\TotalCodeYellowEntry
- Process(ccm)\% CPU Time
- Process(ccm)\% Memory Usage
- Process(ccm)\VmSize
- Memory\Used Swap KBytes
- Memory\% Mem Used
- Memory\% Page Usage
- Memory\% VM Used
- Memory\Used VM KBytes
- Processor(_Total)\% CPU Time
- Processor(_Total)\IOwait Percentage
- Number of Replicates Created and State of Replication(ReplicateCount)\Replicate_State
- Number of Replicates Created and State of Replication(ReplicateCount)
- Number of Replicates Created

- Partition(Common)\Write Bytes Per Sec
- Partition(Common)\Read Bytes Per Sec
- System/IOPerSecond
- /System/IOKBytesReadPerSecond
- /System/IOKBytesWrittenPerSecond

Cisco Unity Connection RTMT PerfMon Counters

The Cisco Unity Connection RTMT PerfMon counters are the key server performance metrics, which are monitored together or separately. The platform key performance indicators (KPIs) show that a server is under load. You can add sections to narrow the focus to a particular area. The KPIs provide the information to get to the root cause of an issue. You can apply the KPIs to any server in any tier of the server lines.

System KPIs (Linux VOS)

The following Linux system KPIs deal with core subsystems such as disk, processor, memory, and network:

- \PROCESSOR(_TOTAL)\USER PERCENTAGE
- \PROCESSOR(_TOTAL)\IRQ PERCENTAGE
- \PROCESSOR(_TOTAL)\IOWAIT PERCENTAGE
- \PROCESSOR(_TOTAL)% CPU TIME
- \PARTITION(SWAP)\USED MBYTES
- \PARTITION(SWAP)\TOTAL MBYTES
- \PARTITION(SPARE)\WRITE BYTES PER SEC
- \PARTITION(SPARE)\READ BYTES PER SEC
- \PARTITION(SPARE)\QUEUE LENGTH
- \PARTITION(SPARE)%WAIT IN WRITE
- \PARTITION(SPARE)% WAIT IN READ
- \PARTITION(SPARE)% USED
- \PARTITION(COMMON)\WRITE BYTES PER SEC
- \PARTITION(COMMON)\READ BYTES PER SEC
- \PARTITION(COMMON)\QUEUE LENGTH
- \PARTITION(COMMON)% WAIT IN WRITE
- \PARTITION(COMMON)% WAIT IN READ
- \PARTITION(COMMON)% USED
- \PARTITION(ACTIVE)\WRITE BYTES PER SEC

- \PARTITION(ACTIVE)\READ BYTES PER SEC
- \PARTITION(ACTIVE)\QUEUE LENGTH
- \PARTITION(ACTIVE)% WAIT IN WRITE
- \PARTITION(ACTIVE)% WAIT IN READ
- \PARTITION(ACTIVE)% USED
- \NETWORK INTERFACE(ETH0)\TX ERRORS
- \NETWORK INTERFACE(ETH0)\TX BYTES
- \NETWORK INTERFACE(ETH0)\TOTAL BYTES
- \NETWORK INTERFACE(ETH0)\RX ERRORS
- \NETWORK INTERFACE(ETH0)\RX BYTES
- \MEMORY\USED VM KBYTES
- \MEMORY\USED SWAP KBYTES
- \MEMORY\USED KBYTES
- \MEMORY\TOTAL VM KBYTES
- \MEMORY\TOTAL SWAP KBYTES
- \MEMORY\TOTAL KBYTES
- \MEMORY\PAGES OUTPUT PER SEC
- \MEMORY\PAGES INPUT PER SEC
- \MEMORY\PAGES
- \MEMORY\PAGE FAULTS PER SEC
- \MEMORY%VM USED
- \MEMORY% PAGE USAGE
- \MEMORY% MEM USED

System KPIs (Windows)

The following Windows system KPIs deal with core subsystems such as disk, processor, memory, and network:

- LOGICAL DISK (% DISK TIME, % FREE DISK SPACE, AVG. DISK QUEUE LENGTH)
- MEMORY (AVAILABLE BYTES, CACHE FAULTS/SEC, COMMITTED BYTES, PAGE FAULTS/SEC, PAGE READS/SEC, PAGES/SEC, TRANSITION FAULTS/SEC)
- PAGING FILE (% USAGE PEAK)
- PHYSICAL DISK (% DISK TIME, AVG. DISK QUEUE LENGTH, AVG. DISK/SEC TRANSFER, DISK READS/SEC, DISK WRITES/SEC)
- PROCESSOR (% INTERRUPT TIME, % PROCESSOR TIME, % USER TIME)

- REDIRECTOR (NETWORK ERRORS/SEC)
- SERVER (BYTES RECEIVED/SEC, BYTES TOTAL/SEC, BYTES TRANSMITTED/SEC, ERRORS LOGON)
- SYSTEM (CONTEXT SWITCHES/SEC, PROCESSOR QUEUE LENGTH)

Core Process KPIs

The following core process KPIs deal with core architecture items (for example, Cisco UCS Manager):

- \PROCESS(PROCESSNAME)% CPU TIME
- \PROCESS(PROCESSNAME)% MEMORY USAGE
- \PROCESS(PROCESSNAME)\THREAD COUNT
- \PROCESS(PROCESSNAME)\VMDATA *
- \PROCESS(PROCESSNAME)\VMRSS *
- \PROCESS(PROCESSNAME)\VMSIZE *
- VmSize = Virtual memory usage of entire process = VmLib + VmExe + VmData + VmStk (bytes)
- VmRss = Resident Set currently in physical memory including Code, Data, Stack (bytes)
- VmData = Virtual memory usage of Heap (bytes)
- VmLib = Virtual memory usage by dlls loaded (bytes)

Application KPIs

The following application KPIs deal with the application as a whole (for example, phone system, IMAP) and include counters related to feature sets:

- \CUC MESSAGE STORE\MESSAGE SIZE AVERAGE (KB)
- \CUC MESSAGE STORE\MESSAGES DELIVERED TOTAL
- \CUC MESSAGE STORE\MESSAGES RECEIVED TOTAL
- \CUC MESSAGE STORE\NON-DELIVERY RECEIPTS TOTAL
- \CUC MESSAGE STORE\RETRIES TOTAL
- \CUC PHONE SYSTEM\CALL COUNT TOTAL
- \CUC PHONE SYSTEM\CALL DURATION AVERAGE (S)
- \CUC PHONE SYSTEM\CALL DURATION TOTAL (S)
- \CUC PHONE SYSTEM\INCOMING CALLS CFB TOTAL
- \CUC PHONE SYSTEM\INCOMING CALLS CFNA TOTAL
- \CUC PHONE SYSTEM\INCOMING CALLS DURATION AVERAGE (S)
- \CUC PHONE SYSTEM\INCOMING CALLS DURATION TOTAL (S)

- \CUC PHONE SYSTEM\MESSAGE NOTIFICATION DURATION TOTAL (S)
- \CUC PHONE SYSTEM\MESSAGE NOTIFICATIONS FAILED
- \CUC PHONE SYSTEM\MESSAGE NOTIFICATIONS TOTAL
- \CUC PHONE SYSTEM\MWI REQUESTS FAILED TOTAL
- \CUC PHONE SYSTEM\MWI REQUESTS TOTAL
- \CUC PHONE SYSTEM\OUTGOING CALLS RELEASE TRANSFERS FAILED
- \CUC PHONE SYSTEM\OUTGOING CALLS RELEASE TRANSFERS TOTAL
- \CUC PHONE SYSTEM\OUTGOING CALLS SUPERVISED TRANSFERS FAILED
- \CUC PHONE SYSTEM\OUTGOING CALLS SUPERVISED TRANSFERS TOTAL
- \CUC PHONE SYSTEM\PORT IDLE DURATION AVERAGE (S)
- \CUC PHONE SYSTEM\PORTS LOCKED
- \CUC REPLICATION\FILE REPLICATION LATENCY MAX (S)
- \CUC REPLICATION\TRANSFER RATE (BYTES/S)
- \CUC SESSIONS: IMAP SERVER\COMMANDS PER MINUTE
- \CUC SESSIONS: IMAP SERVER\CONNECTION LENGTH AVERAGE (S)
- \CUC SESSIONS: IMAP SERVER\ERRORS TOTAL
- \CUC SESSIONS: IMAP SERVER\LOGIN REQUESTS TOTAL
- \CUC SESSIONS: IMAP SERVER\LOGOUT REQUESTS TOTAL
- \CUC SESSIONS: IMAP SERVER\MESSAGES READ/HOUR
- \CUC SESSIONS: IMAP SERVER\MESSAGES/FETCH AVERAGE
- \CUC SESSIONS: IMAP SERVER\RESPONSE TIME (MS)
- \CUC SESSIONS: IMAP SERVER\TLS ERRORS TOTAL
- \CUC SESSIONS: VOICE\DELAY - OPENING GREETING (MS)
- \CUC SESSIONS: VOICE\DELAY - SUBSCRIBER LOGON (MS)
- \CUC SESSIONS: VOICE\FAILSAFES TOTAL
- \CUC SESSIONS: VOICE\MEETING SEARCH DELAY (MS)
- \CUC SESSIONS: VOICE\MESSAGES DELETED
- \CUC SESSIONS: VOICE\MESSAGES FORWARDED
- \CUC SESSIONS: VOICE\MESSAGES READ
- \CUC SESSIONS: VOICE\MESSAGES REPLIED
- \CUC SESSIONS: VOICE\MESSAGES SENT
- \CUC SESSIONS: VOICE\MRCP DEFINE GRAMMAR DELAY (MS)

- \CUC SESSIONS: VOICE\MRCP DEFINE GRAMMAR DELAY AVERAGE (MS)
- \CUC SESSIONS: VOICE\MRCP DELAY (MS)
- \CUC SESSIONS: VOICE\MRCP DELAY AVERAGE (MS)
- \CUC SESSIONS: VOICE\SESSIONS TOTAL
- \CUC SESSIONS: VUI\MATCHES TOTAL
- \CUC SESSIONS: VUI\NO-MATCHES TOTAL
- \CUC SESSIONS: VUI\SESSIONS DURATION AVERAGE/CALL (S)

Database KPIs

Database KPIs deal with the same set of core subsystem counters as the Core Process KPIs and the database-specific counters.

Web KPIs

The following Web KPIs deal with the same set of core subsystem counters as the Core Process KPIs and the web-specific counters:

- \CUC SESSIONS: WEB\CPCA AUTHENTICATION DELAY MAX (S)
- \CUC SESSIONS: WEB\CPCA PAGES SERVED TOTAL
- \CUC SESSIONS: WEB\CPCA SERVER BUSY PAGES TOTAL
- \CUC SESSIONS: WEB\CUCA AUTHENTICATION DELAY MAX (S)
- \CUC SESSIONS: WEB\CUCA RESPONSE TIME MAX (S)
- \CISCO TOMCAT JVM\KBYTESMEMORYFREE
- \CISCO TOMCAT JVM\KBYTESMEMORYMAX
- \CISCO TOMCAT JVM\KBYTESMEMORYTOTAL

Unified RTMT Trace File Collection

Through the Trace and Log Central feature in the Cisco Unified Real-Time Monitoring Tool (Unified RTMT), you can configure on-demand trace collection. RTMT is available for Cisco Unified Communications Manager, Cisco Unified IM and Presence Service, and Cisco Unity Connection.

Collect Trace Files

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

Procedure

Step 1 Open Trace and Log Central.

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

Step 3 Collect traces for the all services and all nodes, normally the call processing nodes of the application. Check the name of the server.

Step 4 Collect traces for particular system logs on particular servers and check the traces that apply.

For example, to collect CSA logs, check **Cisco Security Agent**. To access user logs that provide information about users who are signing in and out, check **Security Logs**.

Step 5 Continue the Trace Collection wizard without collecting traces for system logs.

Step 6 Select the time, date, or relative time that you need.

Step 7 Continue the Trace Collection wizard without collecting traces for services or applications.

Step 8 Select **Next**.

Step 9 Specify the time zone and time range for which you want to collect traces in the Collection Time group box.

Step 10 Select the partition that contains the logs for which you want to collect traces from the Select Partition list box.

Step 11 Perform one of the following actions to download trace files:

- Specify the directory in which you want to download the trace files.
- Select **Browse** next to the Download File Directory field. Navigate to the directory and select **Open**.

Step 12 To create a zip file of the trace files that you collected, select **Zip File**, otherwise select **Do Not Zip Files**.

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

Step 14 Click **Finish**.

The files start to download from all the nodes or cluster that you have defined.

Trace Levels, Parameters, and Fields

The following tables describe trace levels, parameters, and fields.

Table 3: Trace levels

Level	Description
Arbitrary	Traces all Entry and Exit conditions and provides low-level debugging information. **Note:** Do not use this trace level with the Cisco IP Voice Media Streaming Application service during normal operation.

Debug	Traces all State Transition conditions plus media layer events that occur during normal operation. **Note:** Do not use Debug logging with IM and Presence Service because this trace level degrades system performance. Cisco strongly recommends that you use the Info trace level to debug issues during normal operation.
Detailed	Traces all Arbitrary conditions and provides detailed debugging information. **Note:**Do not use Debug logging with the Cisco IP Voice Media Streaming Application service because this trace level degrades system performance. Cisco strongly recommends that you use the Info trace level to debug issues during normal operation.
Entry/Exit	Traces all significant conditions plus entry and exit points of routines. Not all services use this trace level (for example, Cisco Unified IM and Presence Service does not).
Error	Traces alarm conditions and events. Used for all traces that are generated in the abnormal path. Uses minimum number of CPU cycles.
Fatal	Traces severe error events that may cause the application to stop working.
Info	Traces most of servlet problems and has a minimal effect on system performance.
Significant	Traces all State Transition conditions plus media layer events that occur during normal operation.
Special	Traces all Error conditions plus process and device initialization messages.
State Transition	Traces all Special conditions plus subsystem state transitions that occur during normal operation.
Warn	Traces potentially harmful situations.

Table 4: Trace Parameters

Parameter	**Description**
Enable CTI Gateway Trace	This parameter enables tracing for the CTI Gateway.
Enable Parser Trace	This parameter enables tracing of parser information that is related to the operation of the persipd child SIP parser.

Enable SIP TLS Trace	This parameter enables tracing for information that is related to the TLS transport of SIP messages by TCP services.
Enable Privacy Trace	This parameter enables tracing for information about processing of PAI, RPID, and Diversion headers in relation to privacy requests.
Enable Routing Trace	This parameter enables tracing for the Routing module.
Enable IPPM Trace	This parameter enables tracing for IP Phone Messenger.
Enable SIPUA Trace	This parameter enables tracing for the SIP UA application module.
Enable Number Expansion Trace	This parameter enables tracing for the Number expansion module.
Enable Presence Web Service Trace	This parameter enables tracing for the Presence Web Service.
Enable SIP Message and State Machine Trace	This parameter enables tracing for information that is related to the operation of the per-sipd SIP state machine.
Enable SIP TCP Trace	This parameter enables tracing for information that is related to the TCP transport of SIP messages by TCP services.
Enable Authentication Trace	This parameter enables tracing for the Authentication module.
Enable Enum Trace	This parameter enables tracing for the Enum module.
Enable Registry Trace	This parameter enables tracing for the Registry module.
Enable Method/Event Routing Trace	This parameter enables tracing for the Method/Event routing module.
Enable CALENDAR Trace	This parameter enables tracing for the Calendar module.
Enable Server Trace	This parameter enables tracing for the Server.
Enable Access Log Trace	This parameter enables the proxy access log trace; the first line of each SIP message received by the proxy is logged.
Enable SIP XMPP IM Gateway Trace	This parameter enables tracing for the SIP XMPP IM Gateway.

Table 5: Trace Fields

Field	Description
Maximum No. of files	This field specifies the total number of trace files for a given service. Cisco Unified IM and Presence Service automatically append a sequence number to the filename to indicate which file it is; for example, esp000005. When the last file in the sequence is full, the trace data begins writing over the first file. The default varies by service.
Maximum File Size (MB)	This field specifies the maximum size of the trace file in megabytes. The default varies by service.

Common Logs and Traces

The following are commonly collected Cisco Unified Communications Manager logs and traces:

- CM SDL: /var/log/active/cm/trace /ccm/sdl/
- CM SDI: /var/log/active/cm/trace /ccm/sdi
- CTI SDL: /var/log/active/cm/trace /cti/sdl
- CTI SDI: /var/log/active/cm/trace /cti/sdi
- Install Logs: /common/log/install
- DRF Logs: /var/log/active/platform/drf/log
- PerfMon: /var/log/active/cm/log/ris/csv/
- CORE: /var/log/active/core/
- SYSLOGS: /var/log/active/syslog/
- TOMCAT logs: /var/log/active/tomcat/logs/
- Platform: /var/log/active/platform/log/

Alarms

Cisco Unified Communications Manager Alarms

Table 6: Cisco Unified Communications Manager Alarms

CallManager Alarm Catalog	
Name	**Description**
CallManager	All Cisco CallManager service alarm definitions

CDRRepAlarmCatalog	All CDRRep alarm definitions
CARAlarmCatalog	All CDR analysis and reporting alarm definitions
CEFAlarmCatalog	All Cisco Extended Functions alarm definitions
CMIAlarmCatalog	All Cisco messaging interface alarm definitions
CtiManagerAlarmCatalog	All Cisco computer telephony integration (CTI) manager alarm definitions
IpVmsAlarmCatalog	All IP voice media streaming applications alarm definitions
TCDSRVAlarm Catalog	All Cisco telephony call dispatcher service alarm definitions
Phone	Alarms for phone-related tasks, such as downloads
CAPFAlarmCatalog	Alarms for Certificate Authority Proxy Function (CAPF) service
Cisco Unified CallManager System Catalogs	
ClusterManagerAlarmCatalog	All cluster manager alarm definitions that are related to the establishment of security associations between servers in a
DBAlarmCatalog	All Cisco database (aupair) alarm definitions
DRFAlarmCatalog	All Disaster Recovery System alarm definitions
GenericAlarmCatalog	All generic alarm definitions that all applications share
JavaApplications	All Java Applications alarm definitions. Cisco License Manager, which supports Cisco Unified Communications Manager, uses this catalog. You cannot configure JavaApplications alarms through the alarm configuration GUI. For Cisco Unified Communications Manager and Cisco Unity Connection, you generally configure these alarms to go to the Event Logs. For Cisco Unified Communications Manager, you can configure these alarms to generate SNMP traps to integrate with CiscoWorks LAN Management Solution. Use the registry editor that is provided with your operating system to view or change alarm definitions and parameters.
E MAlarmCatalog	Alarms for Extension Mobility
LoginAlarmCatalog	Alarms for Extension Mobility

LpmTctCatalog	All log partition monitoring and trace collection alarm definitions
RTMTAlarmCatalog	All Cisco Unified Real-Time Monitoring Tool alarm definitions
SystemAccessCatalog	All alarm definitions that are used for tracking whether SystemAccess provides all thread statistic counters together with all the process statistic counters
ServiceManagerAlarmCatalogs	All service manager alarm definitions that are related to the activation, deactivation, starting, restarting, and stopping of services
TFTPAlarmCatalog	All Cisco TFTP alarm definitions
TVSAlarmCatalog	Alarms for Trust Verification Service
TestAlarmCatalog	All alarm definitions that are used for sending test alarms through SNMP traps from the CLI. For information on the CLI, see the *Command Line Interface Reference Guide for Cisco Unified Solutions*. Cisco Unified Communications Manager supports SNMP traps in Unified CM systems. Cisco Unity Connection SNMP does not support traps in Cisco Unity Connection systems.
CertMonitorAlarmCatalog	All certificate expiration definitions
CTLproviderAlarmCatalo g	Alarms for Certificate Trust List (CTL) Provider service
CDPAlarmCatalo g	Alarms for Cisco Discovery Protocol (CDP) service
IMSAlarmCatalog	All user authentication and credential definitions

Cisco Unity Connection Alarms

Cisco Unity Connection Serviceability alarms provide information on runtime status and the state of the system so you can troubleshoot problems that are associated with the system. For example, you can use alarms to determine whether there are any ports that are enabled to set MWIs. Alarm information includes the catalog, name, severity, explanation, recommended action, routing list, and parameters.

You can enable or disable alarms to appear as syslog messages on the local server or on a remote server that you specify. You can also set the severity level that you want to appear.

You use the trace and log central option in the Real-Time Monitoring Tool (RTMT) to collect alarms. You use the SysLog Viewer in RTMT to view alarms.

Alarm definitions

You can search for and view alarm definitions in *Alarm Message Definitions for Cisco Unity Connection* at:

http://www.cisco.com/en/US/products/ps6509/products_system_message_guides_list.html.

Enable alarms

Procedure

Step 1 In Cisco Unity Connection Serviceability, select **Alarm** > **Configurations**.

Step 2 In the Alarm Configurations window, perform one of the following actions:

- To enable the system to log the alarms in the application logs area in the SysLog Viewer, under Local Syslogs, check the **Enable Alarm** check box.
- To enable the system to store the alarms on a remote syslog server, under Remote Syslogs, check the **Enable Alarm** check box and, in the Server Name field, enter the IP address or hostname of the remote syslog server.

Step 3 Under the syslog for which you have enabled alarms, in the Alarm Event Level field, select the severity level that you want.

Step 4 Select **Save**.

Disable alarms

Procedure

Step 1 In Cisco Unity Connection Serviceability, select **Alarm** > **Configurations**.

Step 2 In the Alarm Configurations windows, uncheck the applicable **Enable Alarm** check box.

Step 3 Select **Save**.

Cisco Unified IM and Presence Service Alarms

For details of Cisco Unified IM and Presence Service alarms, see *System Error Messages for IM and Presence Service on Cisco Unified Communications Manager*, at :

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-system-message-guides-list.html.

Alarms and CiscoLog Messages

- CiscoLog Format
- Log File and Syslog Outputs
- Standard Syslog Server Implementations
- Clock Synchronization
- Multipart Messages

- CiscoLog Message Format
- Message Length Limit
- SEQNUM Field
- HOST Field
- TIMESTAMP Field
- HEADER Field
- TAGS Field
- MESSAGE Field
- Internationalization
- Versioning

Preconfigured System Alarm Notifications

- AuthenticationFailed
- CiscoDRFFailure
- CoreDumpFileFound
- CpuPegging
- CriticalServiceDown
- HardwareFailure
- LogFileSearchStringFound
- LogPartitionHighWaterMarkExceeded
- LogPartitionLowWaterMarkExceeded
- LowActivePartitionAvailableDiskSpace
- LowAvailableVirtualMemory
- LowInactivePartitionAvailableDiskSpace
- LowSwapPartitionAvailableDiskSpace
- ServerDown
- SparePartitionHighWaterMarkExceeded
- SparePartitionLowWaterMarkExceeded
- SyslogSeverityMatchFound
- SyslogStringMatchFound
- SystemVersionMismatched
- TotalProcessesAndThreadsExceededThreshold

Troubleshooting with RTMT

You can use the Cisco Unified Real-Time Monitoring Tool (RTMT) to troubleshoot call failures by selecting **Systems** > **Tools** > **Trace & Log Central**.

For more information on RTMT, see: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

For information on troubleshooting in HCM-F, see: *Cisco Hosted Collaboration Mediation Fulfillment Troubleshooting Guide*.

Troubleshooting FAX for Long Distance Call

Unified CM Forced Authorization Code (FAC) Interactions and Restrictions

- The FAC and CMC tones play only on Cisco Unified IP Phones that are running SCCP or SIP, TAPI/JTAPI ports, and MGCP FXS ports.
- Calls that originate from a SIP trunk, H.323, or MGCP gateway fail if they encounter a route pattern that requires FAC or CMC and the caller is not configured as Cisco Unified Mobility.
- H.323 analog gateways do not support FAC or CMC because these gateways cannot play tones.

1. Verify if the FXS port of Voice Gateway is configured as SIP trunk. If yes, disable the FAC for those FXS ports that are cofigured as SIP. SIP trunk doesn't support FAC.
2. In Unified CDM, navigate to **Device Management** > **CUCM** > **Route Patterns** > **Require Forced Authorization Codes**, and disable the FAC.

Note

- Use MGCP or SCCP to implement FAC.
- Use a CSS that allows calls without FAC on SIP trunk since SIP trunk doesn't support FAC.