Monitoring Cisco Unified Communications Manager IM and Presence, Release 9.1(1)

First Published: February 04, 2013
Last Modified: February 04, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided "as is" with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice.

In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2013 Cisco Systems, Inc. All rights reserved.
CONTENTS

Preface vii

CHAPTER 1 Alerts and alarms 1

Monitor alerts using Cisco Prime Unified Operations Manager 1
Monitor alerts using Unified RTMT 2
List of alerts 3

IM and Presence Service alerts 3

CTIGWProviderDown 3
CTIGWProviderFailedToOpen 4
DbmonQueueWorkerExistWithError 4
ESPSharedMemAllocFailed 5
ESPSharedMemCreateFailed 5
ESPSharedMemSetPermFailed 5
ESPStopped 6
ICSACertificateFingerPrintMisMatch 6
ICSACertificateValidationFailure 6
InterclusterSyncAgentAXLConnectionFailed 7
InterclusterSyncAgentFailedToCleanUpPeer 7
InterclusterSyncAgentFailedToSendCN 7
InterclusterSyncAgentPeerDuplicate 8
InterclusterSyncAgentPeerSyncFailed 8
NotInCucmAppServerListError 9
PEConfigNotificationFailure 9
PEDatabaseError 9
PEIDSQueryError 10
PEIDSSubscribeError 10
PEIDStoIMDBDatabaseSyncError 10
PEOamInitialConfigFileError 11
PEOamInvalidInitialConfigFile 11
PEOamConfigFileError 11
PEPeerNodeFailure 12
PESipSgHostUnavailable 12
PESipSocketBindFailure 12
SRMFailed 13
SRMFailover 13
SyncAgentAXLConnectionFailed 13
SyncAgentCucmDbmonConnectionFailed 14
XCPConfigMgrConfigurationFailure 14
XCPConfigMgrHostNameResolutionFailed 14
XCPConfigMgrJabberRestartRequired 15
XCPConfigMgrQueueAtCriticalLevel 15
XCPConfigMgrR2RPasswordEncryptionFailed 15
XcpSIPGWStackResourceError 16
Cisco Prime Unified Operations Manager Alerts 16
   DevicePartiallyMonitored 17
   HighUtilization 17
   HTTPInaccessible 17
   InsufficientFreeVirtualMemory 18
   ServerUnreachable 18
   Unresponsive 19
System Alerts 19
   CiscoDRFFailure 19
   CpuPegging 20
   CriticalServiceDown 20
   HardwareFailure 21
   LogPartitionHighWaterMarkExceeded 21
   LogPartitionLowWaterMarkExceeded 21
   LowActivePartitionAvailableDiskSpace 22
   LowAvailableVirtualMemory 22
   LowSwapPartitionAvailableDiskSpace 23
   ServerDown 23
   SystemVersionMismatched 24
CHAPTER 2

High CPU and virtual memory issues 25

Monitor high CPU and virtual memory issues using Unified Operations Manager 25
Monitor high CPU and virtual memory issues using Unified RTMT 26
High CPU issues 27
High virtual memory issues 29

CHAPTER 3

Performance counters 31

Monitor performance counters using Unified Operations Manager 31
Client connections 31
Database 31
Instant messaging 32
Presence 32
Process CPU usage 33
Process Memory usage 33
SIP federation 34
Text conferencing 34
Monitor performance counters using Unified RTMT 35
Archive performance counters in Unified RTMT 40
List of recommended performance counters 44
Client connections 44
WebCMConnectedSockets 44
ConnectedSockets 44
Database 44
CcmDbSpace_Used 44
ReplicationQueueDepth 44
Replicate_state 44
Instant messaging 45
JsmMsgsInLastSlice 45
JsmSessionMessagesOut 45
JsmSessionMessagesIn 46
JsmIMSessions 46
Cisco XCP JSM Session Counters 46
JsmTotalMessagePackets 47
Contents

Presence 47
  ActiveCalendarSubscriptions 47
  ActiveJsmSessions 47
SIP federation 47
  SIPS2SSubscriptionsIn 47
  SIPS2SSubscriptionsOut 48
  NumIdleSipdWorkers 48
  SIPInviteRequestIn 48
  SIPMessageRequestIn 48
  SIPNotifyRequestIn 49
  SIPS2SInviteIn 49
  SIPS2SInviteOut 49
  Number of SIP MESSAGES Received (Cisco XCP SIP S2S - SIPS2SMessagesIn) 50
  SIPS2SMessagesOut 50
  SIPS2SNotifyIn 50
  SIPS2SNotifyOut 50
  SIPSubscribeRequestIn 50
  Sip_Tcp_Requests 51

Text conferencing 51
  TCRoomMsgPacketsRecv 51
  TCRoomNumOccupants 51
  Cisco XCP TC Room Counters 51
  TcAdHocRooms 52
  TcPersistentRooms 52
  TcTotalRooms 52
Preface

The following document details a series of best practices for monitoring a IM and Presence Service server.
Alerts and alarms

- Monitor alerts using Cisco Prime Unified Operations Manager, page 1
- Monitor alerts using Unified RTMT, page 2
- List of alerts, page 3

Monitor alerts using Cisco Prime Unified Operations Manager

Cisco Prime Unified Operations Manager (Unified Operations Manager) 8.6 is capable of raising system alerts only for IM and Presence Service. Unified Operations Manager 8.7 and later include a custom syslog feature. This feature makes it possible to add syslog messages that are not in the Unified Operations Manager default list. These alerts will be raised based on their Cisco Unified Real-Time Monitoring Tool (Unified RTMT) default thresholds.

Complete the following procedure to monitor alerts using Unified Operations Manager.

Procedure

**Step 1**  
First on IM and Presence.  
a) On the IM and Presence Administration GUI navigate to System > Enterprise Parameters.  
b) For Remote Syslog Server Name, add your Unified Operations Manager node name or IP address and click Save.

**Step 2**  
Then on Unified Operations Manager.  
a) On Unified Operations Manager, navigate to Administration > System Settings > Syslog Support and click Add.  
b) Specify the name of the alert you wish to monitor in Syslog Name.  
Here you can specify which IM and Presence alerts you want Unified Operations Manager to monitor.
Monitor alerts using Unified RTMT

You can monitor both system and IM and Presence-specific alerts for an IM and Presence server using Cisco Unified Real-Time Monitoring Tool.

Procedure

**Step 1**  To monitor both System and IM and Presence Service-specific alerts on IM and Presence Service Server.

- a) Choose **Tools > Alert Central**.
- b) Right-click on each alert and choose **Set alert > Properties** to view alert descriptions, change default thresholds, and configure email notifications.

**Step 2**  To view the recent alarm history on the IM and Presence Service Server.
a) Choose Tools > System summary.

**Figure 2: Real Time Monitoring Tool window**

List of alerts
Alert messages are generated to notify administrators when a predefined condition is met, such as when an activated service goes from up to down. Cisco recommends that you monitor the following IM and Presence, Unified Operations Manager, and System alerts.

**IM and Presence Service alerts**
The following is a list of common IM and Presence Service alerts.

**CTIGWProviderDown**
Type
IM and Presence Service
Alert Description
This alert indicates that the CTI provider is currently unavailable.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Check the connection to the configured Cisco Unified Communications Manager nodes and verify that the Cisco CTI Gateway application is enabled on the Administration GUI CTI Settings page.

**CTIGWProviderFailedToOpen**

Type
IM and Presence Service

Alert Description
This alert indicates that the CTI Provider failed to open due to a configuration error.

Unified RTMT Default Threshold
Not Applicable.

Recommended Actions
Verify the Cisco Unified Communications Manager addresses and application user credentials on the Administration GUI CTI Settings page.

**DbmonQueueWorkerExistWithError**

Type
IM and Presence Service

Alert Description
This alert indicates that the Cisco Sync Agent service is no longer processing change notifications from the Cisco Unified Communications Manager cluster. This error can cause the data on the IM and Presence Service cluster to get out of sync with the data on the Cisco Unified Communications Manager cluster.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Verify that the Cisco Unified Communications Manager server is active. You might need to restart the Cisco Sync Agent service.
**ESPSharedMemAllocFailed**

**Type**
IM and Presence Service

**Alert Description**
This alert indicates that the Cisco SIP Proxy service failed to allocate shared memory segments while trying to initialize tables.

**Unified RTMT Default Threshold**
Not Applicable

**Recommended Actions**
Use Unified RTMT to check system shared memory, check the Cisco SIP Proxy service trace log file for any detailed error messages and contact Cisco TAC for assistance.

**ESPSharedMemCreateFailed**

**Type**
IM and Presence Service

**Alert Description**
This alert indicates that the Cisco SIP Proxy service failed to create shared memory segments while trying to initialize tables.

**Unified RTMT Default Threshold**
Not Applicable

**Recommended Actions**
Use Unified RTMT to check system shared memory, check the Cisco SIP Proxy service trace log file for any detailed error messages, and contact Cisco TAC for assistance.

**ESPSharedMemSetPermFailed**

**Type**
IM and Presence Service

**Alert Description**
This alert indicates that the Cisco SIP Proxy service failed to set permissions on shared memory segments while trying to initialize tables.

**Unified RTMT Default Threshold**
Not Applicable
Recommended Actions
Use Unified RTMT to check system shared memory, check the Cisco SIP Proxy service trace log file for any detailed error messages, and contact Cisco TAC for assistance.

**ESPStopped**

**Type**
IM and Presence Service

**Alert Description**
This alert indicates that the Cisco SIP Proxy service child process has stopped.

**Unified RTMT Default Threshold**
Not Applicable

**Recommended Actions**
If the administrator has not manually stopped the Proxy service, this may indicate a problem. Use Unified RTMT to check for any related alarms and contact Cisco TAC for assistance.

**ICSACertificateFingerPrintMisMatch**

**Type**
IM and Presence Service

**Alert Description**
This alert indicates that the Cisco Intercluster Sync Agent service detected a fingerprint mismatch on the certificate being processed.

**Unified RTMT Default Threshold**
Not Applicable

**Recommended Actions**
Use the IM and Presence Service OS Administration GUI to compare the certificates that are loaded on this server with the certificates on the source server. You might need to delete the problem certificates and reload them.

**ICSACertificateValidationFailure**

**Type**
IM and Presence Service

**Alert Description**
This alert indicates that the Cisco Intercluster Sync Agent service detected a validation error on the certificate being processed.
Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Use the IM and Presence Service OS Administration GUI to compare the certificates that are loaded on this server with the certificates on the source server. You might need to delete the problem certificates and reload them.

InterclusterSyncAgentAXLConnectionFailed

Type
IM and Presence Service

Alert Description
This alert indicates that the Cisco Intercluster Sync Agent service failed authentication to the remote IM and Presence Service cluster and therefore is unable to connect.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Verify that the AXL credentials are correct and whether the Cisco AXL Web service is running on the remote IM and Presence Service cluster.

InterclusterSyncAgentFailedToCleanUpPeer

Type
IM and Presence Service

Alert Description
This alert indicates that the Cisco Intercluster Sync Agent service failed to successfully clean up data after a peer was removed during a sync.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Verify that the Cisco DB service is still up and accepting connections. See Cisco Inter Cluster Sync Agent logs for the root cause and contact Cisco TAC for assistance.

InterclusterSyncAgentFailedToSendCN

Type
IM and Presence Service
Alert Description
This alert indicates that the Cisco Intercluster Sync Agent service failed to send change notifications to the remote IM and Presence Service cluster.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Verify that the AXL credentials are correct and whether the Cisco AXL Web service is running on the remote IM and Presence Service cluster.

InterclusterSyncAgentPeerDuplicate
Type
IM and Presence Service

Alert Description
This alert indicates that the Cisco Intercluster Sync Agent service failed to sync user location data from a remote peer. The remote peer is from an IM and Presence Service cluster which already has a peer in the local cluster.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Verify that the hostname of the remote peer is not a secondary node from the identified existing peer. If the new peer is a secondary node, then remove this peer from the IM and Presence Service Administration GUI Inter-cluster details page. You can also run the System Troubleshooter for more details.

InterclusterSyncAgentPeerSyncFailed
Type
IM and Presence Service

Alert Description
This alert indicates that the Cisco Intercluster Sync Agent service failed to sync user location data from the remote IM and Presence Service cluster.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Verify that the remote IM and Presence Service peer is not also configured as a node in the local cluster, and on the Administration GUI run the System Troubleshooter for more information about this issue.
**NotInCucmAppServerListError**

**Type**
IM and Presence Service

**Alert Description**
This alert indicates that the Cisco Sync Agent failed to start because the IM and Presence Service Server node is not in the application server list on the Cisco Unified Communications Manager publisher.

**Unified RTMT Default Threshold**
Not Applicable

**Recommended Actions**
Add IM and Presence Service Server node to the application server list on the Cisco Unified Communications Manager server and start the Cisco Sync Agent service.

**PEConfigNotificationFailure**

**Type**
IM and Presence Service

**Alert Description**
This alert indicates that the Cisco Presence Engine service cannot bind to the socket that is used for communication with the IM and Presence Service OAM Agent service through XML-RPC.

**Unified RTMT Default Threshold**
Not Applicable

**Recommended Actions**
Verify that the IM and Presence Service OAM Agent service listen interface is configured correctly on the IM and Presence Service Administration GUI Application Listener page. Verify that no other process is listening on the same port using netstat.

**PEDatabaseError**

**Type**
IM and Presence Service

**Alert Description**
This alert indicates that the Cisco Presence Engine service encountered an error while retrieving information from the database. This may indicate a problem with the Cisco DB service.

**Unified RTMT Default Threshold**
Not Applicable
Recommended Actions

Verify that the Cisco DB service is running. Use Unified RTMT to check the Cisco Presence Engine service logs for errors. Consult Cisco TAC for guidance.

PEIDSQueryError

Type
IM and Presence Service

Alert Description
This alert indicates that the Cisco Presence Engine service has detected an error while querying the IM and Presence Service database.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Restart the Cisco Presence Engine service when convenient. See the associated error message and log files and consult Cisco TAC if the problem persists.

PEIDSSubscribeError

Type
IM and Presence Service

Alert Description
This alert indicates that the Cisco Presence Engine service was unable to subscribe for IM and Presence Service database change notifications.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Restart the Cisco Presence Engine service when convenient. See the associated error message and log files and consult Cisco TAC if the problem persists.

PEIDStoIMDBDatabaseSyncError

Type
IM and Presence Service

Alert Description
This alert indicates that synchronization between the IM and Presence database and the Cisco Presence Engine and a database service has failed (Cisco Login Datastore, Cisco Route Datastore, Cisco Presence Datastore, and Cisco SIP Registration Datastore).
Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Restart the Cisco Presence Engine service when convenient. See associated error message and log files and consult Cisco TAC if the problem persists.

PEOamInitialConfigFileError

Type
IM and Presence Service

Alert Description
This alert indicates that the Cisco Presence Engine service configuration file is missing or malformed.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Verify that the IM and Presence Service OAM Agent service is running through the Serviceability GUI.

PEOamInvalidInitialConfigFile

Type
IM and Presence Service

Alert Description
This alert indicates that the Cisco Presence Engine service configuration file is missing or malformed.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Verify that the OAM Agent service is running.

PEOamConfigFileError

Type
IM and Presence Service

Alert Description
This alert indicates that the Cisco Presence Engine service configuration file is missing or malformed.

Unified RTMT Default Threshold
Not Applicable
Recommended Actions
Verify that the IM and Presence Service OAM Agent service is running through the Serviceability GUI.

PEPeerNodeFailure

Type
IM and Presence Service

Alert Description
This alert indicates that Cisco Presence Engine service on the peer node of a subcluster has failed.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Use Cisco Unified Serviceability to verify that the Cisco Presence Engine service is running. Consult Cisco TAC for further assistance

PESipSgHostUnavailable

Type
IM and Presence Service

Alert Description
This alert indicates that the Cisco Presence Engine service could not contact the indicated outbound proxy server group.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Verify that the outbound proxy is configured correctly and listening on the configured ports.

PESipSocketBindFailure

Type
IM and Presence Service

Alert Description
This alert indicates that the Cisco Presence Engine service was unable to connect to the indicated configured interface. No SIP traffic can be processed on this interface.

Unified RTMT Default Threshold
Not Applicable
Recommended Actions
Verify that the Cisco Presence Engine service listen interface is configured correctly on the IM and Presence Service Administration GUI Application Listener page. Verify that no other process is listening on the same port using netstat.

SRMFailed

Type
IM and Presence Service

Alert Description
This alert indicates that the Server Recovery Manager is in the Failed state.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
When it is convenient restart the Server Recovery Manager.

SRMFailover

Type
IM and Presence Service

Alert Description
This alert indicates that the Server Recovery Manager is performing an automatic failover.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Verify that the failed node is up and that critical services are running.

SyncAgentAXLConnectionFailed

Type
IM and Presence Service

Alert Description
This alert indicates that the Cisco Sync Agent service failed authentication to the remote Cisco Unified Communications Manager publisher and therefore is unable to connect.

Unified RTMT Default Threshold
Not Applicable
**Recommended Actions**

Verify that the AXL credentials are correct and whether the Cisco AXL Web service is running on the remote Cisco Unified Communications Manager publisher.

---

**SyncAgentCucmDbmonConnectionFailed**

**Type**  
IM and Presence Service

**Alert Description**

This alert indicates that the Cisco Sync Agent service lost the connection to the Cisco Database Layer Monitor service. This error can cause the data on the IM and Presence Service cluster to get out of sync with the data on the Cisco Unified Communications Manager cluster.

**Unified RTMT Default Threshold**

Not Applicable

**Recommended Actions**

Verify that the Cisco Unified Communications Manager server is active and that the Cisco Unified Communications Manager publisher has opened port 8001.

---

**XCPConfigMgrConfigurationFailure**

**Type**  
IM and Presence Service

**Alert Description**

This alert indicates that the Cisco XCP Config Manager failed to successfully update XCP configuration.

**Unified RTMT Default Threshold**

Not Applicable

**Recommended Actions**

See the Cisco XCP Config Manager logs for the root cause. Contact Cisco TAC for assistance.

---

**XCPConfigMgrHostNameResolutionFailed**

**Type**  
IM and Presence Service

**Alert Description**

This alert indicates that the Cisco XCP Config Manager could not resolve a DNS name to allow Cisco XCP Routers to connect to that node.
Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Verify DNS resolvability of all hostnames and FQDNs in both local and remote clusters. Restart the Cisco XCP Config Manager and then restart the Cisco XCP Router after DNS is resolvable.

XCPConfigMgrJabberRestartRequired

Type
IM and Presence Service

Alert Description
This alert indicates that the Cisco XCP Config Manager has regenerated XCP XML files after system halt due to buffer size. The Cisco XCP Router must now be restarted to apply changes.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
When it is convenient to do so, restart the Cisco XCP Router.

XCPConfigMgrQueueAtCriticalLevel

Type
IM and Presence Service

Alert Description
This alert indicates that the Cisco XCP Config Manager buffer has reached critical levels. The system will halt until configuration stabilizes, and then it will regenerate all files. The Cisco XCP Router will need to be restarted to apply these changes.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Restart the Cisco XCP Router after the alarm is sent that indicates that configuration has been regenerated successfully.

XCPConfigMgrR2RPasswordEncryptionFailed

Type
IM and Presence Service
Alert Description
This alert indicates that the Cisco XCP Config Manager was unable to encrypt the password that is associated with an Inter-cluster Router-to-Router configuration.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
When it is convenient to do so, restart the Cisco XCP Config Manager and then restart the Cisco XCP Router.

XcpSIPGWSStackResourceError

Type
IM and Presence Service

Alert Description
This alert indicates that the maximum supported concurrent SIP Federation subscriptions or SIP Federation IM sessions has been reached, and the Cisco XCP SIP Federation Connection Manager does not have the resources that are required to handle any addition subscriptions or IM sessions.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Increase the Pre-allocated SIP stack memory Service Parameter for the Cisco XCP SIP Federation Connection Manager. Note: If you are changing this setting, make sure that you have the memory available. If you do not have enough memory, you may have reached the limit of your hardware capability.

Cisco Prime Unified Operations Manager Alerts

The following is a list of common Unified Operations Manager alerts.

Note
Unified Operations Manager maintains its own set of alerts that are related to IM and Presence Service. Some of these mirror existing native alerts. For example, the native alert LowAvailableVirtualMemory and the Unified Operations Manager alert InsufficientFreeVirtualMemory both alert on the same item and are based on the same data, yet the default threshold is different on Unified Operations Manager (< 15%) and Unified RTMT (< 25%).
DevicePartiallyMonitored

Type
Unified Operations Manager

Alert Description
This alert is generated based on polling Unified RTMT precanned counters and is raised when Unified Operations Manager is not able to collect Unified RTMT data for Unified RTMT polling supported devices. Unified RTMT data collection can fail if there are HTTP communication failures or network issues or if the Unified RTMT application on the device has issues and is unable to provide the data to Unified Operations Manager.

Default Threshold
Not Applicable

Recommended Actions
- Check for any HTTP communication or network failures from the Operations Manager to the device.
- Check whether Cisco RIS Data Collector network service is running on the device. This service should be running in all the nodes of the cluster.

HighUtilization

Type
Unified Operations Manager

Alert Description
Current utilization exceeds the utilization threshold that is configured for this processor.

Default Threshold
> 90%

Recommended Actions
Identify the processes that are using excessive CPU space. You may want to take action, which may include restarting the identified process or processes.

HTTPInaccessible

Type
Unified Operations Manager
**Alert Description**

HTTP service cannot be used to communicate to all servers in the cluster. This might be due to one or both of the following:

- The Web Services for a server in the cluster is down.
- The credentials (HTTP username, password) for at least one of the running Web Services were not found or are incorrect.

**Default Threshold**

Not Applicable

**Recommended Actions**

Verify that all servers are accessible through Web Service with the credentials that are provided in Unified Operations Manager. Provide the correct username and password if the credentials are wrong. You might need to restart the web server if Web Service is down.

---

**InsufficientFreeVirtualMemory**

**Type**

Unified Operations Manager

**Alert Description**

System is running out of virtual memory resources. This may degrade the performance of the device.

**Default Threshold**

< 15%

**Recommended Actions**

Verify insufficient memory using the CPU and Memory tool in Unified RTMT. This alert may be due to a memory leak. It is important to identify which process is using excessive memory. This can be done using the Process tool. After the process is identified, if you suspect a memory leak (for example, if the memory usage for a process increases continually, or a process is using more memory than it should), you may want to restart that process.

---

**ServerUnreachable**

**Type**

Unified Operations Manager

**Alert Description**

Host is not reachable through Unified RTMT polling. This alert is generated based on polling Unified RTMT pre canned counters.

**Default Threshold**

Not Applicable
Recommended Actions

Investigate whether the indicated host is running and whether a network problem exists.

Unresponsive

Type
Unified Operations Manager

Alert Description
Device does not respond to ICMP or SNMP requests. Probable causes are:

- On a system: ICMP ping requests and SNMP queries to the device timeout receive no response.
- On an SNMP Agent: Device ICMP ping requests are successful, but SNMP requests time out with no response.

A system might also be reported as unresponsive if the only link (for example, an interface) to the system goes down. Unified Operations Manager performs root cause analysis for any unresponsive events.

If Unified Operations Manager receives a device unresponsive event, it will clear any interface unresponsive events from that device until the device is recognized as responsive.

Default Threshold
Not Applicable

Recommended Actions
Check whether the device is reachable from Unified Operations Manager.

System Alerts

The following is a list of common System alerts.

CiscoDRFFailure

Type
System

Alert Description
This alert indicates that the Disaster Recovery Failure (DRF) backup or restore process encountered errors. The alert is generated by monitoring the syslog messages that are received from the IM and Presence Service Server.

Unified RTMT Default Threshold
Not Applicable
Recommended Actions

Verify whether /common/drf has the required permission and enough space for the DRF user. Check the application logs for further details. Consult Cisco TAC for assistance.

CpuPegging

Type
System

Alert Description
This alert occurs when the percentage of CPU load on a presence server is over the configured percentage for the configured period of time. This alert is generated based on polling Unified RTMT performance counters. To view the threshold, right-click the alert and select Set Alert/Properties.

Unified RTMT Default Threshold
99%

Recommended Actions
The most common reason for this alert is that one or more processes are using excessive CPU space. The alert has information about which process is using the most CPU. After the process is identified, you may want to take action, which could include restarting the process. You can also verify the current CPU usage of the problem process using the Process tool.

It is helpful to check the trace setting for that process. Using the detailed/debug trace level is known to take up excessive CPU space. If so, you may want to take more drastic measures, such as stopping nonessential services or scheduling a restart of IM and Presence Server during off hours.

CriticalServiceDown

Type
System

Alert Description
This alert is generated when one of the critical services (any of the services in the Critical Services tool in Unified RTMT) is not running. The problem could be due to someone manually stopping the service. If you intend to stop the service for a long period of time, you should deactivate it on the Serviceability GUI: Cisco Unified Serviceability > Tools > Service Activation.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Identify which services are not running. You can start the service manually from the Serviceability GUI: Cisco Unified Serviceability > Tools > Feature Services/Network Services.

Also, check to see whether there are any core files. Download the core files, if any, as well as service trace files.
HardwareFailure

Type
System

Alert Description
This alert indicates that a hardware failure has occurred in a presence server. This event is generated by monitoring the syslog messages received from the IM and Presence server.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Check the Unified RTMT Syslog Viewer tool for further details.

LogPartitionHighWaterMarkExceeded

Type
System

Alert Description
This alert indicates that the percentage of used disk space in the log partition has exceeded the configured high water mark. This alert is generated based on polling Unified RTMT performance counters. To view the threshold, right-click the alert and select Set Alert/Properties.

Unified RTMT Default Threshold
> 95%

Recommended Actions
Log partition usage can be monitored from the Unified RTMT Disk Usage page. It appears as Common Partition. Check trace settings and also check for core dump files. Note that core dump files are fairly large. Typically, a core dump file is 200 to 300 MB in size, but it can also be 1 GB or 2 GB. Note that after the log partition disk usage goes above the high water mark threshold, Cisco Log Partition Monitoring Tool (LPM) starts deleting files to put log partition disk usage under the low water mark threshold. Because LPM may delete the trace/log/core dump files you want to keep, it is very important to act when you receive a LogPartitionLowWaterMarkExceeded alert. You can use Trace and Log Central (TLC) in Unified RTMT to download files and delete them from the server.

LogPartitionLowWaterMarkExceeded

Type
System
Alert Description

This alert indicates that the percentage of used disk space in the log partition has exceeded the configured low water mark. This alert is generated based on polling Unified RTMT performance counters. To view the threshold, right-click the alert and select Set Alert/Properties.

Unified RTMT Default Threshold

> 90%

Recommended Actions

See LogPartitionHighWaterMarkExceeded.

**LowActivePartitionAvailableDiskSpace**

**Type**

System

**Alert Description**

This alert indicates that the percentage of available disk space in the active partition is lower than the configured value. This alert is generated based on polling Unified RTMT performance counters. To view the threshold, right-click the alert and select Set Alert/Properties.

**Unified RTMT Default Threshold**

< 4%

**Recommended Actions**

Some of the symptoms of low active disk space are:

- Administration GUI does not operate correctly.
- Cisco Unified Communications Manager Bulk Administration Tool (BAT) does not operate correctly.
- Unified RTMT does not operate correctly.

Because there are no user-manageable files in Active Partition, check the alert threshold. If the alert threshold is at the Cisco default, contact Cisco TAC for guidance.

**LowAvailableVirtualMemory**

**Type**

System
Alert Description

This alert occurs when the percentage of available virtual memory is lower than the configured value. This alert indicates that the available virtual memory is running low. This alert is generated based on polling Unified RTMT performance counters. To view the threshold, right-click the alert and select Set Alert/Properties. A LowAvailableVirtualMemory alert generally means that the server has allocated all of its physical memory and has begun using its Swap Space on disk more intensively. This will lead to higher CPU usage and longer I/O wait times.

Unified RTMT Default Threshold

< 25%

Recommended Actions

Verify insufficient memory using the CPU and Memory tool in Unified RTMT. This alert may be due to a memory leak. It is important to identify which process is using excessive memory. This can be done using the Process tool. After the process is identified, if you suspect a memory leak (for example, if the memory usage for a process increases continually, or a process is using more memory than it should), you may want to restart that process.

LowSwapPartitionAvailableDiskSpace

Type

System

Alert Description

This alert occurs when the percentage of available disk space of the swap partition is lower than the configured value. This alert indicates that available swap partition is running low. Note that the swap partition is part of virtual memory. Therefore, low available swap partition disk space also means low virtual memory. This alert is generated based on polling Unified RTMT performance counters. To view the threshold, right-click the alert and select Set Alert/Properties.

Unified RTMT Default Threshold

< 10%

Recommended Actions

When you receive this alert, you should find out how much swap space and virtual memory are still available. You should also find out find out which process is using the most memory. This alert may be due to a memory leak. After you determine that there is a memory leak and virtual memory is running low, you may want to restart the service after saving the necessary troubleshooting information. Consult Cisco TAC for further information.

ServerDown

Type

System
Alert Description
This alert indicates that the host is not reachable through Unified RTMT polling. This alert is generated based on polling Unified RTMT performance counters.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Investigate whether the indicated host is running and whether a network problem exists.

SystemVersionMismatched

Type
System

Alert Description
This alert occurs when there is a mismatch in the system version among all servers in the cluster. This alert is generated by monitoring the syslog messages that are received from the IM and Presence server.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Make sure that all servers in the cluster are running the same system version.

TotalProcessesAndThreadsExceededThreshold

Type
System

Alert Description
This alert indicates that the current total number of processes or threads has exceeded the maximum number of tasks. This situation could indicate that some processes or threads are not being shut down correctly. System access must stop thread counter update to avoid CPU pegging, and only provide process counter information for up to the maximum number of processes. This alert is generated by monitoring the syslog messages that are received from the IM and Presence Server.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Check the alert detail for the process that has the highest number of threads and the process that has the most instances. If the process has an unusual number of threads or process instances, save the trace for the service and perhaps restart the service. Make sure to download trace files that are associated with the service. Note that the Cisco SIP Proxy process sipd and the Database process cmoninit can each have over 20 instances. This is expected behavior.
High CPU and virtual memory issues

- Monitor high CPU and virtual memory issues using Unified Operations Manager, page 25
- Monitor high CPU and virtual memory issues using Unified RTMT, page 26
- High CPU issues, page 27
- High virtual memory issues, page 29

Monitor high CPU and virtual memory issues using Unified Operations Manager

Unified Operations Manager 8.6 and 8.7 provides an overview of CPU and virtual memory usage on your IM and Presence Service node. If usage is high, debug further using Unified RTMT.

Unified Operations Manager 9.0 reports on the memory usage of the IM and Presence Service node A Cisco DB service or cmoninit processes, the system overview, and also the CPU usage of the following services:

- Cisco Tomcat
- Cisco Presence Engine
- Cisco SIP Proxy
- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP Web Connection Manager
- Cisco XCP SIP Federation Connection Manager
- Cisco XCP XMPP Federation Connection Manager
Monitor high CPU and virtual memory issues using Unified RTMT

Unified RTMT provides an overview of CPU and Virtual Memory usage using the CPU and Memory tool. This provides overall system usage statistics for all nodes in an IM and Presence cluster.

Unified RTMT allows monitoring of usage statistics, and individual processes using the Process tool. Every process on the server reports data for the following:

**PID**
- The task's unique process ID, which periodically wraps, though never restarts at zero.

**% CPU**
- The task’s share of the elapsed CPU time since the last update.

**Status**
- The task's process status: 0 - Running, 1 - Sleeping, 2 - Uninterruptible disk sleep, 3 - Zombie, 4 - Traced or stopped (on a signal), 5 - Paging, 6 - Unknown.

**Shared Memory (KB)**
- The amount of shared memory, in kilobytes (KB), that a task is using. Other processes could potentially share the same memory.

**Nice (Level)**
- The nice value of the task. A negative nice value indicates that the process has a higher priority, while a positive nice value indicates that the process has a lower priority. If the nice value equals zero, do not adjust the priority when you are determining if the task can be dispatched.

**VmRSS (KB)**
- The virtual memory (Vm) resident set size (RSS) that is currently in physical memory in KB, including Code, Data, and Stack.

**VmSize (KB)**
- The total amount of virtual memory, in KB, that the task is using. It includes all code, data, shared libraries, and pages that have been swapped out: Virtual Image = swapped size + resident size.

**VmData (KB)**
- The virtual memory usage of the heap for the task in KB.

**Thread Count**
- The number of threads that are currently grouped with the task. The negative value -1 indicates that this counter is currently not available because thread statistics (including all performance counters in the Thread object as well as the Thread Count counter in the Process object) have been turned off because the system's total processes and threads have exceeded the default threshold value.

**Data Stack Size**
- The stack size for task memory status.
Page Fault Count

The number of major page faults that a task encountered that required the data to be loaded into memory.

High CPU issues

On IM and Presence Service, when you experience high overall CPU usage, Cisco recommends that you check the usage of the following processes that have historically caused high CPU on IM and Presence:

<table>
<thead>
<tr>
<th>Process</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>tomcat</td>
<td>Cisco Tomcat</td>
</tr>
<tr>
<td>jabberd</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>pe</td>
<td>Cisco Presence Engine</td>
</tr>
<tr>
<td>cm</td>
<td>Cisco XCP Connection Manager</td>
</tr>
<tr>
<td>cm_web</td>
<td>Cisco XCP Web Connection Manager</td>
</tr>
<tr>
<td>cm_sip_fed</td>
<td>Cisco XCP SIP Federation Manager</td>
</tr>
<tr>
<td>cm_xmpp_fed</td>
<td>Cisco XCP XMPP Federation Manager</td>
</tr>
<tr>
<td>cmoninit</td>
<td>A Cisco DB</td>
</tr>
<tr>
<td>sipd</td>
<td>Cisco SIP Proxy</td>
</tr>
</tbody>
</table>

The cmoninit and sipd processes will both have 20+ individual instances, any one of which could be responsible for high CPU usage.

If the process consuming CPU is not in the preceding table, consult the following table for a list of other processes and their corresponding services. If the process causing high CPU is not in either table, the problem may reside with a system or platform service. Consult Cisco TAC for further assistance.

<table>
<thead>
<tr>
<th>Process</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>amc</td>
<td>Cisco AMC Service</td>
</tr>
<tr>
<td>AuditLog</td>
<td>Cisco Audit Event Service</td>
</tr>
<tr>
<td>auth</td>
<td>Cisco XCP Authentication Service</td>
</tr>
<tr>
<td>BPS</td>
<td>Cisco Bulk Provisioning Service</td>
</tr>
<tr>
<td>cdpd</td>
<td>Cisco CDP</td>
</tr>
<tr>
<td>cdpAgt</td>
<td>Cisco CDP Agent</td>
</tr>
<tr>
<td>certM</td>
<td>Cisco Certificate Expiry Monitor</td>
</tr>
<tr>
<td>CiscoDRFLocal</td>
<td>Cisco DRF Local</td>
</tr>
<tr>
<td>Process</td>
<td>Service</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>CiscoDRFMaster</td>
<td>Cisco DRF Master</td>
</tr>
<tr>
<td>CiscoLicenseMgr</td>
<td>Cisco License Manager</td>
</tr>
<tr>
<td>CiscoSyslogSubAgt</td>
<td>Cisco Syslog Agent</td>
</tr>
<tr>
<td>db1rpc</td>
<td>A Cisco DB Replicator</td>
</tr>
<tr>
<td>dbmon</td>
<td>Cisco Database Layer Monitor</td>
</tr>
<tr>
<td>EspConfigAgent</td>
<td>Cisco Config Agent</td>
</tr>
<tr>
<td>hostagt</td>
<td>Host Resources Agent</td>
</tr>
<tr>
<td>interClusterSyncAgent</td>
<td>Cisco Intercluster Sync Agent</td>
</tr>
<tr>
<td>jds</td>
<td>Cisco XCP Directory Service</td>
</tr>
<tr>
<td>LpmTool</td>
<td>Cisco Log Partition Monitoring Tool</td>
</tr>
<tr>
<td>ma</td>
<td>Cisco XCP Message Archiver</td>
</tr>
<tr>
<td>Mib2agt</td>
<td>MIB2 Agent</td>
</tr>
<tr>
<td>oamagent</td>
<td>Cisco OAM Agent</td>
</tr>
<tr>
<td>replWatcher</td>
<td>Cisco Replication Watcher</td>
</tr>
<tr>
<td>RisDC</td>
<td>Cisco RIS Data Collector</td>
</tr>
<tr>
<td>rtmreporter</td>
<td>Cisco Serviceability Reporter</td>
</tr>
<tr>
<td>sappagt</td>
<td>System Application Agent</td>
</tr>
<tr>
<td>snmpdm</td>
<td>SNMP Master Agent</td>
</tr>
<tr>
<td>srm</td>
<td>Cisco Server Recovery Manager</td>
</tr>
<tr>
<td>syncAgent</td>
<td>Cisco Sync Agent</td>
</tr>
<tr>
<td>tc</td>
<td>Cisco XCP Text Conference Manager</td>
</tr>
<tr>
<td>tracecollectionservice</td>
<td>Cisco Trace Collection Service</td>
</tr>
<tr>
<td>ttlogin</td>
<td>Cisco Login Datastore</td>
</tr>
<tr>
<td>ttreg</td>
<td>Cisco SIP Registration Datastore</td>
</tr>
<tr>
<td>ttroute</td>
<td>Cisco Route Datastore</td>
</tr>
<tr>
<td>ttsoft</td>
<td>Cisco Presence Datastore</td>
</tr>
<tr>
<td>xcpConfigManager</td>
<td>Cisco XCP Config Manager</td>
</tr>
</tbody>
</table>
High virtual memory issues

When experiencing high Virtual Memory usage on IM and Presence, Cisco recommends that you monitor the VmSize of the following processes:

- tomcat
- jabberd
- pe
- all of the Connection Manager processes (cm, cm_web, cm_sip_fed & cm_xmpp_fed)
- all of the sipd processes
- all of the cmoninit processes
High CPU and virtual memory issues

High virtual memory issues
Performance counters

- Monitor performance counters using Unified Operations Manager, page 31
- Monitor performance counters using Unified RTMT, page 35
- Archive performance counters in Unified RTMT, page 40
- List of recommended performance counters, page 44

Monitor performance counters using Unified Operations Manager

Unified Operations Manager 9.0 allows the monitoring of the following counters in the following categories.

### Client connections

<table>
<thead>
<tr>
<th>Counter Value</th>
<th>Counter Name</th>
<th>Folder Location</th>
<th>Default Alert Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of connected XMPP clients</td>
<td>ConnectedSockets, on page 44</td>
<td>Cisco XCP CM</td>
<td>None</td>
</tr>
<tr>
<td>Number of connected CAXL clients</td>
<td>WebCMConnectedSockets, on page 44</td>
<td>Cisco XCP WebCM</td>
<td>None</td>
</tr>
</tbody>
</table>

### Database

<table>
<thead>
<tr>
<th>Counter Value</th>
<th>Counter Name</th>
<th>Folder Location</th>
<th>Default Alert Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Space Used</td>
<td>CcmDbSpace_Used, on page 44</td>
<td>DB Local_DSN</td>
<td>Yes (&gt; 90%)</td>
</tr>
</tbody>
</table>
### Instant messaging

<table>
<thead>
<tr>
<th>Counter Attribute</th>
<th>Counter Name</th>
<th>Folder Location</th>
<th>Default Alert Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Instant Message Sessions</td>
<td>JsmIMSessions, on page 46</td>
<td>Cisco XCP JSM</td>
<td>None</td>
</tr>
<tr>
<td>Total Instant Message Packets</td>
<td>JsmTotalMessagePackets, on page 47</td>
<td>Cisco XCP JSM</td>
<td>None</td>
</tr>
<tr>
<td>Instant Message Packets in the last 60 seconds</td>
<td>JsmMsgsInLastSlice, on page 45</td>
<td>Cisco XCP JSM</td>
<td>None</td>
</tr>
<tr>
<td>Message Packets Received per Session</td>
<td>JsmSessionMessagesIn, on page 46</td>
<td>Cisco XCP JSM Session Counters</td>
<td>None</td>
</tr>
<tr>
<td>Messages Sent per Session</td>
<td>JsmSessionMessagesOut, on page 45</td>
<td>Cisco XCP JSM Session Counters</td>
<td>None</td>
</tr>
<tr>
<td>Per User/Per Session counters existing for the duration of an IM session or user login.</td>
<td>Cisco XCP JSM Session Counters, on page 46</td>
<td>Cisco XCP JSM Session Counters</td>
<td>None</td>
</tr>
</tbody>
</table>

---

### Presence

<table>
<thead>
<tr>
<th>Counter Attribute</th>
<th>Counter Name</th>
<th>Folder Location</th>
<th>Default Alert Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Active JSM Sessions</td>
<td>ActiveJsmSessions, on page 47</td>
<td>Cisco Presence Engine</td>
<td>None</td>
</tr>
<tr>
<td>Number of Active Calendar Subscriptions</td>
<td>ActiveCalendarSubscriptions, on page 47</td>
<td>Cisco Presence Engine</td>
<td>None</td>
</tr>
</tbody>
</table>
## Process CPU usage

<table>
<thead>
<tr>
<th>Counter Attribute</th>
<th>Counter Name</th>
<th>Folder Location</th>
<th>Default Alert Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Cisco DB CPU Usage</td>
<td>cmoninit</td>
<td>% CPU Time</td>
<td>Yes (CPU &gt; 90%)</td>
</tr>
<tr>
<td>Cisco SIP Proxy CPU Usage</td>
<td>sipd</td>
<td>% CPU Time</td>
<td>Yes (CPU &gt; 90%)</td>
</tr>
<tr>
<td>Cisco Tomcat CPU Usage</td>
<td>tomcat</td>
<td>% CPU Time</td>
<td>Yes (CPU &gt; 90%)</td>
</tr>
<tr>
<td>Cisco Presence Engine CPU Usage</td>
<td>pe</td>
<td>% CPU Time</td>
<td>Yes (CPU &gt; 90%)</td>
</tr>
<tr>
<td>Cisco XCP Router CPU Usage</td>
<td>jabberd</td>
<td>% CPU Time</td>
<td>Yes (CPU &gt; 90%)</td>
</tr>
<tr>
<td>Cisco XCP Connection Manager CPU usage</td>
<td>cm</td>
<td>% CPU Time</td>
<td>Yes (CPU &gt; 90%)</td>
</tr>
<tr>
<td>Cisco XCP SIP Federation Connection Manager CPU usage</td>
<td>cm#2</td>
<td>% CPU Time</td>
<td>Yes (CPU &gt; 90%)</td>
</tr>
<tr>
<td>Cisco XCP XMPP Federation Connection Manager CPU usage</td>
<td>cm#3</td>
<td>% CPU Time</td>
<td>Yes (CPU &gt; 90%)</td>
</tr>
<tr>
<td>Cisco XCP Web Connection Manager CPU usage</td>
<td>cm#1</td>
<td>% CPU Time</td>
<td>Yes (CPU &gt; 90%)</td>
</tr>
</tbody>
</table>

## Process Memory usage

<table>
<thead>
<tr>
<th>Counter Attribute</th>
<th>Counter Name</th>
<th>Folder Location</th>
<th>Default Alert Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Memory Usage</td>
<td>cmoninit</td>
<td>VmSize</td>
<td>None</td>
</tr>
</tbody>
</table>
### SIP federation

<table>
<thead>
<tr>
<th>Counter Attribute</th>
<th>Counter Name</th>
<th>Folder Location</th>
<th>Default Alert Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Active SIP Subscriptions</td>
<td>SIPS2SSubscriptionsOut, on page 48</td>
<td>Cisco XCP SIP S2S</td>
<td>Yes (&gt; 260,000)</td>
</tr>
<tr>
<td></td>
<td>SIPS2SSubscriptionsIn, on page 47</td>
<td>Cisco XCP SIP S2S</td>
<td></td>
</tr>
<tr>
<td>Number of Idle SIP Proxy Worker Processes</td>
<td>NumIdleSipdWorkers, on page 48</td>
<td>Cisco SIP Proxy</td>
<td>Yes (&lt; 5 for 60 minutes)</td>
</tr>
</tbody>
</table>

### Text conferencing

<table>
<thead>
<tr>
<th>Counter Attribute</th>
<th>Counter Name</th>
<th>Folder Location</th>
<th>Default Alert Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Text Conferencing Rooms</td>
<td>TcTotalRooms, on page 52</td>
<td>Cisco XCP TC</td>
<td>None</td>
</tr>
<tr>
<td>Total AdHoc Group Chat rooms</td>
<td>TcAdHocRooms, on page 52</td>
<td>Cisco XCP TC</td>
<td>None</td>
</tr>
<tr>
<td>Total Persistent Chat Rooms</td>
<td>TcPersistentRooms, on page 52</td>
<td>Cisco XCP TC</td>
<td>None</td>
</tr>
<tr>
<td>Room Message Packets Received</td>
<td>TCRoomMsgPacketsRecv, on page 51</td>
<td>Cisco XCP TC Room Counters</td>
<td>None</td>
</tr>
<tr>
<td>Room Number of Occupants</td>
<td>TCRoomNumOccupants, on page 51</td>
<td>Cisco XCP TC Room Counters</td>
<td>None</td>
</tr>
</tbody>
</table>
Monitor performance counters using Unified RTMT

All IM and Presence Service counters are monitored in Unified RTMT through the **Performance** menu item, under the **System** tools:

**Figure 3: Real Time Monitoring Tool window**

Using Unified RTMT it is possible to create custom alerts based on the values of any Performance Counter. The following procedure is an example of creating a custom alert for Cisco SIP Proxy – NumIdleSipdWorkers.
Procedure

**Step 1** Select **Performance** from the **Performance** menu item in Unified RTMT.

**Step 2** Double-click the **NumIdleSipdWorkers** counter.

**Step 3** Select the counter graph in the main Unified RTMT pane.

**Figure 4: Counter graph**

![Counter graph](image)

**Step 4** Right-click, select **Set Alert/Properties**
The **Alert Properties: General** window opens.

**Figure 5: Alert Properties: General window**

![Alert Properties: General window](image)

- **Step 5** Ensure the **Enable Alert** check box is checked.
- **Step 6** In the **Description** field, enter a brief description for the alert.
- **Step 7** In the **Recommended Action** field, enter a brief action for the alert.
- **Step 8** Choose a severity from the **Severity** drop-down menu.
- **Step 9** Click **Next**.
The **Alert Properties: Threshold & Duration** window opens.

*Figure 6: Alert Properties: Threshold & Duration window*

**Step 10** In the **Threshold** field, specify the alerting threshold for the counter.

**Step 11** In the **Value Calculated As** field, specify how this threshold is calculated.

**Step 12** In the **Duration** field, specify duration of time that the counter value must be above or below the specified threshold before the alert is triggered.

**Note** Cisco recommends that on IM and Presence Service this counter should not remain below a value of 5 for a period of 60 minutes (or 3600 seconds). For more details about this counter, see the List of recommended performance counters.

**Step 13** Click Next.
The **Alert Properties: Frequency & Schedule** window opens.

*Figure 7: Alert Properties: Frequency & Schedule window*

![Alert Properties: Frequency & Schedule window](image)

**Step 14** In the **Frequency** field, specify the amount of times the custom alert is triggered. The default is: “Trigger alert on every poll.”

**Step 15** In the **Schedule** field, specify when the alert is triggered. The default is: “Trigger Alert when it occurs (Non-Stop Monitoring).”

**Step 16** Click **Next**
The Alert Properties: Email Notification window opens.

![Alert Properties: Email Notification window](image)

**Figure 8: Alert Properties: Email Notification window**

**Step 17** To receive email notifications, ensure the Enable Email check box is checked.

*Note* If you do not wish to receive email notifications, uncheck the Enable Email check box and proceed to Step 20, on page 40.

**Step 18** In the Trigger Alert Action field, use the drop-down menu to select the profile this alert will use.

**Step 19** In the User-defined email text field, enter a brief message for the alert.

**Step 20** Click Save.

---

### Archive performance counters in Unified RTMT

The Trace and Log Collection tool in Unified RTMT collects and pushes Perfmon Counter CSV files out to an external server. The following procedure describes how to archive Perfmon Counter CSV files using Cisco RIS Data Collector PerfMon Log.

**Procedure**

**Step 1** Open Trace and Log Collection.

**Step 2** Double-click Schedule Collection.
The Schedule Collection window opens to the Select System Services/Applications table.

**Figure 9: Schedule Collection window**

---

**Step 3** Choose the Cisco RIS Data CollectorPerfMon Log service.

**Step 4** To download the PerfMon logs:

<table>
<thead>
<tr>
<th>From...</th>
<th>... take this action:</th>
</tr>
</thead>
<tbody>
<tr>
<td>All nodes in the cluster</td>
<td>Check All Servers.</td>
</tr>
<tr>
<td>A single node</td>
<td>Select the node name.</td>
</tr>
</tbody>
</table>

**Step 5** Choose Next.
The **Schedule Collection Options** window opens.

### Figure 10: Schedule Collection Options window

**Step 6** In the **Schedule Options** field, configure the following drop-down menus, as desired:

- Select task **Server Time Zone**
- Schedule Start Date/Time
- Schedule End Date/Time
- Scheduler Frequency
- Collect Files generated in the last

**Step 7** In the **Action Options** field, check the **Download Files** check box.
The Trace Download Configuration window opens.

**Figure 11: Trace Download Configuration window**

![Trace Download Configuration window](image)

**Step 8** Choose the archive location for the PerfMon logs. The default is **Localhost**.

**Note** When choosing an SFTP/FTP server, you must choose **Test Connection** to ensure your setup is correct.

**Step 9** Click **OK**.

The Trace Download Configuration window closes.

**Step 10** Click **Finish**.

The Schedule Collection window closes.

---

**Note** You can find the CSV files by navigating down the directory structure to `cm/log/ris/csv`. This unusual directory structure is necessary as it is possible to use Unified RTMT to archive many different logs in one query. It is possible to use Trace and Log collection to archive every log the server generates. Each log will have its own specific path for the sake of organization.
List of recommended performance counters

Client connections

**WebCMConnectedSockets**

The WebCMConnectedSockets performance counter in the Cisco XCP WebCM folder contains the current number of CAXL web clients that are connected to the Cisco XCP Web Connection Manager on an individual IM and Presence Service server. This number rises and falls based on the usage patterns of your deployment. Further investigation may be required if this number is higher than expected for your user base.

**ConnectedSockets**

The ConnectedSockets performance counter in the Cisco XCP CM folder contains the current number of XMPP clients that are connected to the Cisco XCP Connection Manager on an individual IM and Presence Service server. This number rises and falls based on the usage patterns of your deployment. Further investigation may be required if this number is higher than expected for your user base.

Database

**CcmDbSpace_Used**

The Database Space Used performance counter contains the percentage of ccm dbspace used. Monitor this counter for an indication of when you will run out of database space.

**ReplicationQueueDepth**

The Replication Queue Depth performance counter contains the replication queue depth. A high value is an indication of replication issues.

**Replicate_state**

The Replication Status performance counter represents the current state of database replication. This is applicable for multinode IM and Presence Service Distributions. It has five potential values:

- **0**
  
  Initializing. The counter equals 0 when the server is not defined or when the server is defined but the realize template has not completed.

- **1**
  
  The system that is created replicates of some tables but not all tables. Cisco recommends that you run `utils dbreplication status` on the CLI to determine the location and cause of the failure.
Replication is good, replication is set up correctly, and most of the tables in the database should be in sync for all nodes of the cluster.

Bad replication. When the counter displays a value of 3, consider replication in the cluster as bad. It does not mean that replication failed on a particular node. Cisco recommends that you run `utils dbreplication status` on the CLI to determine the location and cause of the failure.

Replication set up did not succeed.

**Instant messaging**

**JsmMsgsInLastSlice**

The total number of IM packets handled by the IM and Presence Service node across all users in the past 60 seconds. This counter is reset to zero every 60 seconds. The same rules for counting IM packets apply as for TotalMessagePackets. Monitoring of this counter helps identify the busy IM hours in your organization.

**JsmSessionMessagesOut**

The IM Packets received per session performance counter contains the total number of IMs that are sent by the user from the user's IM client or session. Note that the term `SessionMessagesIn` is defined from the perspective of IM and Presence Service: the IM packet that was sent by the client is an *inbound* IM packet to IM and Presence Service. On large deployments of IM and Presence Service there can be many instances of this counter, and viewing individual counters in Unified RTMT can be time consuming. To get a long list of the value of this counter for every user on IM and Presence Service, use the CLI command:

```
show perf query counter "Cisco XCP JSM Session Counters" JsmSessionMessagesOut
```

`JsmTotalMessagePackets, JsmMsgsInLastSlice, JsmSessionMessagesIn and JsmSessionMessagesOut` each represent instant message packets being sent to IM and Presence Service and are not exact figures of Instant Messages on the system. The amount of IM packets that are sent to IM and Presence Service per IM can vary depending on the client in use.

**Example**

If Alice and Bob are both using Cisco Unified Personal Communicator 8.5, when Alice sends Bob a single instant message, Cisco Unified Personal Communicator 8.5 will send to IM and Presence Service:

- A composed packet to indicate Alice is typing a new message.
- The instant message packet containing the message body.
- A paused packet to indicate the end of the communication.

In this scenario JSM counters will increment by three.
**JsmSessionMessagesIn**

The IM Packets sent per session performance counter counts the total number of IM packets that are sent to the user on the user's IM client or session. Note that the term SessionMessagesOut is defined from the perspective of IM and Presence Service: the IM packet is sent to the client and is an outbound IM packet from IM and Presence Service. On large deployments of IM and Presence Service there can be many instances of this counter, and viewing individual counters in Unified RTMT can be time consuming. To get a long list of the value of this counter for every user on IM and Presence Service use the CLI command:

```
show perf query counter "Cisco XCP JSM Session Counters" JsmSessionMessagesIn
```

**JsmIMSessions**

The Number of IM Sessions performance counter contains the total number of IM sessions on the IM and Presence Service node across all users. The Cisco Presence Engine, which provides presence composition services and rich, always-on network presence, creates an IM session on behalf of all users at Presence Engine (PE) startup time. This is necessary so that network presence events such as Cisco Unified Communications Manager Telephony Presence and Exchange Calendar notifications are reflected in a user's presence even if that user is not logged in on any of their IM clients. Every licensed user that is assigned to an IM and Presence Service node will have one IM Session for PE rich presence composition in addition to one IM Session for any logged-in clients.

**Example**

If:

- 100 licensed users are assigned to the IM and Presence Service node.
- 50 users are not logged in.
- 40 users are logged in on one IM client.
- 10 users are logged in on two IM clients.

Then IM Sessions will total 160:

- 100 x 1 for rich Presence Engine sessions, *plus*
- 40 x 1 for users logged in on a single client, *plus*
- 10 x 2 for users logged in on two clients

**Cisco XCP JSM Session Counters**

The Per User/Per Session counters exist only for the duration of an IM session or user login. One set of these counters exists per Presence Engine network presence session, and one set of these counters exists per client login session. In the example given above for IM Sessions, 160 different sets of Cisco XCP JSM Session Counters would exist. When a user logs out, or when the Cisco Presence Engine is stopped, the associated Cisco XCP JSM Session Counters instance is deleted.

Administrators can use these counters to get a snapshot of all users that are currently logged in. These can be accessed by entering the following command on the CLI:

```
show perf list instances "Cisco XCP JSM Session Counters"
```
Every user that is assigned to an IM and Presence Service node that is logged in to the system will have a set of JSM session counters for their current logged-in client session and also their Presence Engine network session. On an IM and Presence Service node with 5000 users logged in, this would result in a minimum of 10,000 sets of JSM Session counters. Updating these counters with new values as they change would place the system under stress. To combat this problem, JSM Session counter values are cached locally by the system and are only updated to Unified RTMT every 30 minutes.

**JsmTotalMessagePackets**

The Total IM Packets performance counter gives the total number of IM packets that are handled by the IM and Presence Service node across all users.

**Example**

If user Alice sends an IM packet to user Bob, and both users are assigned to the same IM and Presence Service node, then this IM packet will be counted twice. This is because The Cisco XCP Router and Jabber Session Manager treat the two users separately. For example, Alice’s privacy rules will be applied to the IM packet before it is delivered to Bob, and then Bob’s privacy rules will be applied to the IM packet before it is delivered to Bob’s client. Whenever IM and Presence Service handles an IM packet, it is counted once for the originator and once for the terminator.

If Alice and Bob are assigned to different IM and Presence Service nodes and Alice sends an IM packet to Bob, then the IM packet will be counted once on Alice’s node and once on Bob’s node.

**Presence**

**ActiveCalendarSubscriptions**

The Number of Active Calendar Subscriptions performance counter contains the number of calendar subscriptions that are currently active on the box.

**ActiveJsmSessions**

The Number of Active JSM Sessions performance counter contains the number of client emulation sessions between the Cisco Presence Engine and Cisco XCP Router. The value of this counter should always equal the number of licensed users on the box.

**SIP federation**

**SIPS2SSubscriptionsIn**

The Number of Active Inbound SIP Subscriptions performance counter contains the current number of active inbound SIP Subscriptions that are maintained by the Cisco XCP SIP Federation Connection Manager service on the IM and Presence Service server. Monitor this counter if the IM and Presence Service server is configured for SIP Interdomain Federation or SIP Intradomain Federation.
The total combined count of SubscriptionsOut and SubscriptionsIn must not rise above 260,000 on any single IM and Presence Service server.

**SIPS2SSubscriptionsOut**

The Number of Active Outbound SIP Subscriptions performance counter contains the current number of active outgoing SIP Subscriptions being maintained by the Cisco XCP SIP Federation Connection Manager service on the IM and Presence Service server. Monitor this counter if IM and Presence Service server is configured for SIP Interdomain Federation or SIP Intradomain Federation.

The sum of the values of the SubscriptionsOut and SubscriptionsIn performance counters must not rise above 260,000 on any single IM and Presence Service server.

**NumIdleSipdWorkers**

The Number of Idle SIP Proxy Worker Processes performance counter contains the current number of idle/free SIP worker processes on the IM and Presence Service SIP Proxy. This counter gives a good indication of the load being applied to the Cisco SIP Proxy on each IM and Presence Service server. Monitor this counter if IM and Presence Service server is configured for SIP Interdomain Federation or SIP Intradomain Federation.

The number of idle processes can drop to zero on occasion and is not a cause for concern. However, if the number of idle processes is consistently below five processes, then it is an indication that the IM and Presence Service Server is being heavily loaded and requires further investigation.

**SIPInviteRequestIn**

The Number of INVITE Requests Received performance counter is a cumulative count of the number of SIP INVITE requests arriving into the Cisco SIP Proxy service since the service was last started. Depending on the Role of the IM and Presence Service server, these SIP INVITE requests can come from multiple sources:

- On a Routing IM and Presence Service server this count captures outbound INVITE requests to federated SIP contacts from IM and Presence Service users.
- On an IM and Presence Service server with users provisioned, this count captures:
  - All inbound INVITEs from federated SIP contacts to users that are provisioned on the IM and Presence Service server.
  - All outbound INVITEs to federated SIP contacts from users that are provisioned on the IM and Presence Service server.
  - All outbound INVITEs to local SIP clients from users that are provisioned on the IM and Presence Service server.

**SIPMessageRequestIn**

The Number of MESSAGE Requests Received performance counter is a cumulative count of the number of SIP MESSAGE requests arriving into the Cisco SIP Proxy service since the service was last started. This is useful on the Routing IM and Presence Service server in terms of understanding the rate of IMs that are associated with SIP and federated SIP conversations. Depending on the role of the IM and Presence Service server, these SIP MESSAGE requests can come from multiple sources.
• On a Routing IM and Presence Service server this count captures outbound MESSAGE requests to federated SIP contacts from IM and Presence Service users.

• On an IM and Presence Service server with users provisioned, this count captures:
  ◦ All inbound MESSAGE requests from federated SIP contacts to users that are provisioned on the IM and Presence Service server.
  ◦ All outbound MESSAGE requests to federated SIP contacts from users that are provisioned on the IM and Presence Service server.
  ◦ All outbound MESSAGE requests to local SIP clients from users that are provisioned on the IM and Presence Service server.

**SIPNotifyRequestIn**

The Number of NOTIFY Requests Received performance counter is a cumulative count of the number of SIP NOTIFY requests arriving into the Cisco SIP Proxy service since the service was last started. Depending on the role of the IM and Presence Service server, these SIP NOTIFY requests can come from multiple sources:

• On a Routing IM and Presence Service server this count captures Outbound NOTIFY to federated SIP contacts from IM and Presence Service users.

• On an IM and Presence Service server with users provisioned, this count captures:
  ◦ All inbound NOTIFY requests from federated SIP contacts to users that are provisioned on the IM and Presence Service server.
  ◦ All outbound NOTIFY requests to federated SIP contacts from users that are provisioned on the IM and Presence Service server.
  ◦ All outbound NOTIFY requests to local SIP clients from users that are provisioned on the IM and Presence Service server.

**SIPS2SInviteIn**

The Number of SIP INVITE Messages Received performance counter is a cumulative total of the number of SIP INVITE messages that were received by the Cisco XCP SIP Federation Connection Manager service since the service was last started. A SIP INVITE message arrives from each IM conversation that is initiated by a federated SIP user. So this count equates to the number of inbound IM conversations that were established since the Cisco XCP SIP Federation Connection Manager was last started.

**SIPS2SInviteOut**

The Number of SIP INVITE Messages Sent performance counter contains the total number of SIP INVITE messages that were sent out by the Cisco XCP SIP Federation Connection Manager since the service was last started. A SIP INVITE message is sent out for each IM conversation that is initiated by a Cisco Unified Personal Communicator user to a federated SIP user. So this count equates to the number of outbound IM conversations that were established since the Cisco XCP SIP Federation Connection Manager was last started.
Number of SIP MESSAGES Received (Cisco XCP SIP S2S - SIPS2SMessagesIn)
The Number of SIP MESSAGES Received performance counter contains the total number of SIP MESSAGE packets that were received by the Cisco XCP SIP Federation Connection Manager service since the service was last started. Each Instant Message is sent in a SIP MESSAGE packet. So this count equates to the number of inbound IMs since the Cisco XCP SIP Federation Connection Manager was last started.

SIPS2SMessagesOut
The Number of SIP MESSAGES Sent performance counter contains the total number of SIP MESSAGE packets that were sent out by the Cisco XCP SIP Federation Connection Manager since the service was last started. Each Instant Message is sent in a SIP MESSAGE packet. So this count equates to the number of inbound IMs since the Cisco XCP SIP Federation Connection Manager was last started.

SIPS2SNotifyIn
The Number of SIP NOTIFY Messages Received performance counter contains the total number of SIP NOTIFY messages that were received by the Cisco XCP SIP Federation Connection Manager service since the service was last started.

SIPS2SNotifyOut
The Number of SIP NOTIFY Messages Sent performance counter contains the total number of SIP NOTIFY messages that were sent out from the Cisco XCP SIP Federation Connection Manager service since the service was last started.

SIPSubscribeRequestIn
The Number of SUBSCRIBE Requests Received performance counter contains the total number of SIP SUBSCRIBE requests arriving at the Cisco SIP Proxy service since the service was last started. This counter captures all SUBSCRIBE requests, including refresh SUBSCRIBE requests (sent every 2 hours to keep a SIP Subscription alive) and unSUBSCRIBE requests (to terminate the subscription). Depending on the role of the IM and Presence Service server, these SIP SUBSCRIBE requests can come from multiple sources.

- On a Routing IM and Presence server, this count captures outbound SUBSCRIBE requests to federated SIP contacts from IM and Presence users.
- On an IM and Presence server with users provisioned, this count captures:
  - All inbound SUBSCRIBE requests from federated SIP contacts to users that are provisioned on the IM and Presence server.
  - All outbound SUBSCRIBE requests to federated SIP contacts from users that are provisioned on the IM and Presence server.
  - All outbound SUBSCRIBE requests to local SIP clients from users that are provisioned on the IM and Presence server.
**Sip_Tcp_Requests**

The Number of TCP Requests Received performance counter contains a time-sliced count of the number of generic SIP packets arriving per second at the Cisco SIP Proxy over TCP connections, regardless of type. This includes any SIP requests (SUBSCRIBE/INVITE/MESSAGE/NOTIFY/INFO, etc.) and any SIP responses (100: Trying, 200: OK, 404: Not Found, etc.). You can use it to check for spikes in activity on the IM and Presence Service SIP Proxy.

**Text conferencing**

**TCRoomMsgPacketsRecv**

The IMs received per room performance counter contains the number of IMs that are received by the room. On large deployments of IM and Presence Service there can be many instances of this counter, and viewing individual counters in Unified RTMT can be time consuming. To get a long list of the value of this counter for every user on IM and Presence Service, use the CLI command:

```
show perf query counter "Cisco XCP TC Room Counters" TCRoomMsgPacketsRecv
```

**TCRoomNumOccupants**

The Number of occupants per room performance counter contains the current number of occupants of the chat room. For Persistent Chat rooms, monitoring the Number of occupants per room performance counter will give an indication of the room's usage trend. On large deployments of IM and Presence there can be many instances of this counter and viewing individual counters in Unified RTMT can be time consuming. To get a long list of the value of this counter for every user on IM and Presence use the CLI command:

```
show perf query counter "Cisco XCP TC Room Counters" TCRoomNumOccupants
```

It is possible to have a maximum of 16,500 Text Conferencing rooms on a IM and Presence Service node. Each of these rooms will have its own set of Per Chat Room counters. In a similar fashion to JSM Session counters, updating these with new values as they change would place the system under stress. To reduce the stress, Per Chat Room counter values are cached locally by the system and only updated to Unified RTMT every 30 minutes.

**Cisco XCP TC Room Counters**

Per Chat Room performance counters only exist for the lifetime of a chat room. For ad hoc chat rooms, these counter instances will be destroyed when the ad hoc chat room is destroyed. For persistent chat rooms, the counter instances will also be destroyed when the persistent chat room is destroyed; however, persistent chat rooms are long lived, so they should rarely be destroyed.

Per Chat Room counters can be used to monitor the usage and participants in persistent (and ad hoc) chat rooms over their lifetime and can help identify persistent chat rooms that are no longer being used frequently. Administrators can use Per Chat Room counters to get a snapshot of all rooms that are currently hosted on the node. These can be accessed by using the following CLI command:

```
show perf list instances "Cisco XCP TC Room Counters"
```
**TcAdHocRooms**

The Total ad hoc Group Chat Rooms performance counter contains the total number of ad hoc chat rooms that are currently hosted on the node. Note that ad hoc chat rooms are automatically destroyed when all users leave the room, so this counter should rise and fall in value regularly.

**TcPersistentRooms**

The Total Persistent Chat Rooms performance counter contains the total number of persistent chat rooms hosted on the node. Persistent chat rooms must be explicitly destroyed by the room owner. This counter can be monitored to identify if the total number of persistent chat rooms is very large and also to help identify if some persistent chat rooms are not being used regularly anymore.

**TcTotalRooms**

The Total Text Conferencing Rooms performance counter contains the total number of Text Conferencing rooms that are hosted on the node. This includes both ad hoc rooms and persistent chat rooms.