Cisco Unified Communications Manager Systems Management and Monitoring

This chapter describes how to manage and monitor the health of Cisco Unified Communications Manager (Cisco Unified CM) systems.

Note Serviceability APIs (AXL/SOAP) that are used for serviceability queries and Administrative XML (AXL) that are used as a provisioning read and write APIs are not covered in this document.

Supported Interfaces

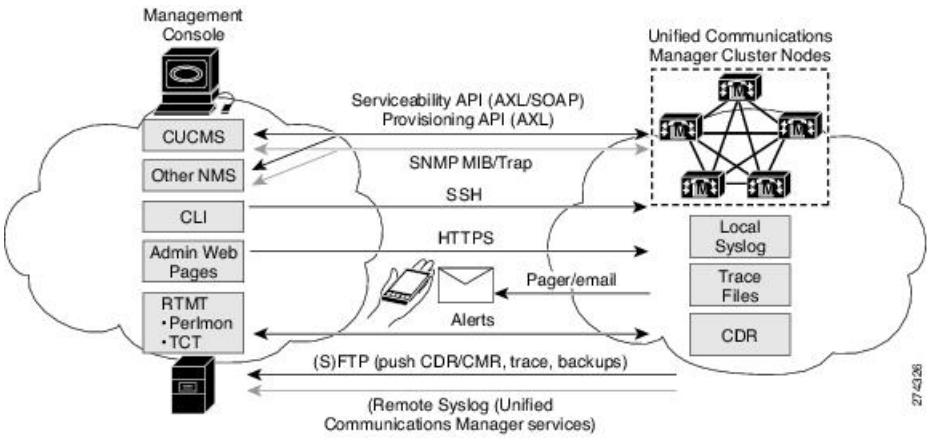
The following interfaces are supported on Cisco Unified CM servers:

- SNMP MIB/Trap—Supports polling and traps by using select MIBs from Cisco and the native platforms.
- SSH Secure Shell Client— Replaces telnet and ftp clients by using a more secure protocol. This application encrypts the entire network session and can use public-key authentication.

- Local and Remote Syslog—Contains types of platform and Cisco Unified CM application events, alerts, and alarms are written to syslog servers.
- HTTPS—Displays the following web pages by using HTTPS—Cisco Unified CM Administration, Cisco Unified Serviceability, Disaster Recovery System, and Unified OS Administration.
- Command Line Interface (CLI)—Used for a subset of functions available by using the web browser interfaces and primarily used to re-establish these interfaces if inoperable. The CLI is accessible by using SSH or a serial console port on the appliance. The complete set of CLI commands is described in the *Command Line Interface Guide for Cisco Unified Communications Solutions*.
- Native Hardware Out of Band Management (OOB)—Supports select features of HP iLO and IBM RSA II.
- Secure FTP (SFTP)—Used for secure file push from or pull to the appliance, including CDR/CMR push, trace file push, push of backups or pull or restores, and pull of upgrade files.
- Third-party Network Management Systems (NMS)—Monitors appliances by leveraging the exact same interfaces exposed to Cisco network management applications. Certain functions of these applications may not be supported on the appliance if native platform access is required, such as account management, software configuration management, or other forms of native platform manipulation. For example, the system management portal web page on HP servers is not supported, but polling and alerting by using the HP System Insight Manager and the appliance MIB is supported.
- Cisco Unified Communications Real-Time Management Tool—Used for perfmon and TCT functions.

The following figure shows the supported interfaces in Cisco Unified CM Release 5.0 and later releases.

Figure 1: Supported Management Interfaces in Cisco Unified CM Release 5.0 and Later Releases



Critical Processes to Monitor

Cisco Unified Communications Manager Critical Processes

The following tables describe Cisco Unified Communications Manager critical processes that require monitoring. Be aware of the following items while monitoring the processes:

- Any of the services, process names, or process sets could change at any time with newer Cisco Unified CM releases without notice.
- HOST-RESOURCES-MIB could be deprecated in any future Cisco Unified CM release.
- Whether a process is auto-restarted or the maximum number of restarts could change for any newer Cisco Unified CM releases without notice.
- Process names represent value shown in HOST-RESOURCES-MIB::hrSWRUNName.
- Any processes not included in this list are transient or not critical for system operation. Those processes should be ignored and they can change without notice.
- Services Cisco CallManager through Cisco CDR Agent can be monitored by using SYSAPPL-MIB.

The following table describes Cisco Unified Communications Manager critical services that require monitoring.

Table 1: Cisco Unified Communications Manager Critical Services to Monitor

Service	Stop | Start | Restart Instruction	Process Name	Auto Restart	Description
Cisco CallManager	**Serviceability/Tools** > **Control Center - Feature Services** *****	ccm	3	The Cisco CallManager service provides software-only call processing as well as signaling and call control functionality for Cisco Unified Communications Manager.
Cisco TFTP	**Serviceability/Tools** > **Control Center - Feature Services** *****	ctftp	3	The Cisco Trivial File Transfer Protocol (TFTP) builds and serves files that are consistent with the trivial file transfer protocol, a simplified version of FTP. Cisco TFTP serves embedded component executable, ringer files, and device configuration files.
Cisco IP Voice Media Streaming App	**Serviceability/Tools** > **Control Center - Feature Services** *****	ipvmsd	3	The Cisco IP Voice Media Streaming Application service provides voice media streaming functionality for the Cisco Unified Communications Manager for use with MTP, conferencing, music on hold (MOH), and annunciator. The Cisco IP Voice Media Streaming Application relays messages from the Cisco Unified Communications Manager to the IP voice media streaming driver, which handles RTP streaming.

Service	Stop | Start | Restart Instruction	Process Name	Auto Restart	Description
Cisco CTIManager	**Serviceability/Tools** > **Control Center - Feature Services** *****	CTI Manager	3	The CTI Manager contains the CTI components that interface with applications. With CTI Manager, applications can access resources and functionality of all Cisco Unified Communications Manager in the cluster and have improved failover capability. Although one or more CTI Managers can be active in a cluster, only one CTI Manager can exist on an individual server. An application (JTAPI/TAPI) can have simultaneous connections to multiple CTI Managers; however, an application can only use one connection at a time to open a device with media termination.
Cisco DHCP Monitor Service	**Serviceability/Tools** > **Control Center - Feature Services** *****	DHCP Monitor	3	Cisco DHCP Monitor Service monitors IP address changes for IP phones in the database tables. When a change is detected, it modifies the `/etc./dhcpd.conf` file and restarts the DHCPD daemon.
Cisco CallManager SNMP Service	**Serviceability/Tools** > **Control Center - Feature Services** *****	ccmAgt	3	This service provides SNMP access to provisioning and statistics information that is available for Cisco Unified Communications Manager.
Cisco CTL Provider Service Status	**Serviceability/Tools** > **Control Center - Feature Services** *****	CTL Provider	3	The Cisco CTL Provider service, which runs with local system account privileges, works with the Cisco CTL Provider Utility, a client-side plug-in, to change the security mode for the cluster from nonsecure to mixed mode. When you install the plug-in, the Cisco CTL Provider service retrieves a list of all Cisco Unified Communications Manager and Cisco TFTP servers in the cluster for the CTL file, which contains a list of security tokens and servers in the cluster.

Service	Stop | Start | Restart Instruction	Process Name	Auto Restart	Description
Cisco Certificate Authority Proxy Function	**Serviceability/Tools** > **Control Center - Feature Services** *****	capf	3	Working in conjunction with the CAPF application, the Cisco Certificate Authority Proxy Function (CAPF) service can perform the following tasks, depending on your configuration—(1)Issue locally significant certificates to supported Cisco Unified IP Phone models. (2)Using SCEP, request certificates from third-party certificate authorities on behalf of supported Cisco Unified IP Phone models. (3)Upgrade existing certificates on the phones. (4)Retrieve phone certificates for troubleshooting. (5)Delete locally significant certificates on the phone.
Cisco DirSync	**Serviceability/Tools** > **Control Center - Feature Services** *****	CCM DirSync	3	Unlike Windows versions of Cisco Unified Communications Manager, Cisco Unified Communications Manager does not contain an embedded directory. Because of this change, the Cisco Unified Communications Manager database stores all user information. If you use an integrated corporate directory, for example, Microsoft Active Directory or Netscape/iPlanet Directory, with Cisco Unified Communications Manager, the Cisco DirSync service migrates the user data to the Cisco Unified Communications Manager database. The Cisco DirSync service does not synchronize the passwords from the corporate directory.
Cisco CallManager Attendant Console Server	**Serviceability/Tools** > **Control Center - Feature Services** *****	acserver	3	The Cisco CallManager Attendant Console Server service provides centralized services for Cisco Unified Communications Manager Attendant Console clients and pilot points. For Attendant Console clients, this service provides call-control functionality, line state information for any accessible line within the Cisco Unified Communications Manager domain, and caching of directory information. For pilot points, this service provides automatic redirection to directory numbers that are listed in hunt groups and failover during a Cisco Unified Communications Manager failure.
Cisco Extended Functions	**Serviceability/Tools** > **Control Center - Feature Services** *****	cef	3	The Cisco Extended Functions service provides support for some Cisco Unified Communications Manager features, including Quality Report Tool (QRT).

Service	Stop | Start | Restart Instruction	Process Name	Auto Restart	Description
Cisco Bulk Provisioning Service	**Serviceability/Tools** > **Control Center - Feature Services** *****	BPS	3	You can activate the Cisco Bulk Provisioning Service only on the first node. If you use the Cisco Unified Bulk Administration Tool (BAT) to administer phones and users, you must activate this service.
Cisco TAPS Service	**Serviceability/Tools** > **Control Center - Feature Services** *****	TAPS	3	The Cisco TAPS Service supports the Cisco Unified Communications Manager Auto-Registered Phone Tool, which allows a user to upload a customized configuration on an autoregistered phone after a user responds to Interactive Voice Response (IVR) prompts.
Cisco Serviceability Reporter	**Serviceability/Tools** > **Control Center - Feature Services** *****	rtmt reporter	3	The Cisco Serviceability Reporter service generates the following daily reports—Device Statistics, Server Statistics, Service Statistics, Call Activities, Alert, Performance Protection Report.
Cisco CAR Scheduler	**Serviceability/Tools** > **Control Center - Feature Services**	carschlr		The Cisco CAR Scheduler service allows you to schedule CAR-related tasks; for example, you can schedule report generation or CDR file loading into the CAR database. This service starts automatically.
Cisco AMC Service	**Serviceability/Tools** > **Control Center - Feature Services**	amc	3	Used for the real-time monitoring tool (RTMT), this service, Alert Manager and Collector service, existed as a component of the Cisco RIS Data Collector service in previous Windows releases of Cisco Unified Communications Manager. This service allows RTMT to retrieve real-time information that exists on nodes in the cluster.
Cisco Trace Collection Service	**Serviceability/Tools** > **Control Center - Feature Services**	tracecollection	3	The Cisco Trace Collection Service, along with the Cisco Trace Collection Servlet, supports trace collection and allows users to view traces by using the RTMT client. After Cisco Unified Communications Manager installation, this service starts automatically. If you stop this service on a server, you cannot collect or view traces on that server.
A Cisco DB	CLI utils service start | stop A Cisco DB	cmoninit	3	A Cisco DB acts as the Progress database engine.

Service	Stop | Start | Restart Instruction	Process Name	Auto Restart	Description
A Cisco DB Replicator	**Serviceability/Tools** > **Control Center - Feature Services**	dblrpc	3	The A Cisco DB Replicator service ensures database configuration and data synchronization between the first and subsequent nodes in the cluster.
Cisco Tomcat	CLI utils service restart Cisco Tomcat	tomcat	3	The Cisco Tomcat service supports the web server.
SNMP Master Agent	**Serviceability/Tools** > **Control Center - Feature Services** *	snmpdm	3	This service, which acts as the agent protocol engine, provides authentication, authorization, access control, and privacy functions that relate to SNMP requests.
MIB2 Agent	**Serviceability/Tools** > **Control Center - Feature Services** *	mib2agt	3	This service provides SNMP access to variables that are defined in RFC 1213, which read and write variables; for example, system, interfaces, IP, and so on.
Host Resources Agent	**Serviceability/Tools** > **Control Center - Feature Services** *	hostagt	3	This service provides SNMP access to host information, such as storage resources, process tables, device information, and installed software base.
Native Agent Adapter	**Serviceability/Tools** > **Control Center - Feature Services** *	naaagt	3	This service allows you to forward SNMP requests to another SNMP agent that runs on the system.
System Application Agent	**Serviceability/Tools** > **Control Center - Feature Services**	sappagt	3	This service provides SNMP access to the applications that are installed and executing on the system. This implements the SYSAPPL-MIB.
Cisco CDP Agent	**Serviceability/Tools** > **Control Center - Feature Services**	cdpAgt	3	This service uses the Cisco Discovery Protocol to provide SNMP access to network connectivity information on the Cisco Unified Communications Manager node.
Cisco Syslog Agent	**Serviceability/Tools** > **Control Center - Feature Services**	Cisco Syslog SubA	3	This service uses the Cisco Discovery Protocol to provide SNMP access to network connectivity information on the Cisco Unified Communications Manager node.

Service	Stop | Start | Restart Instruction	Process Name	Auto Restart	Description
Cisco Trace Collection Service	**Serviceability/Tools** > **Control Center - Feature Services**	Cisco Syslog SubA	3	Cisco License Manager keeps track of the licenses that a customer purchases and uses. It controls licenses checkins and checkouts, and it takes responsibility for issuing and reclaiming licenses. Cisco License Manager manages the Cisco Unified Communications Manager application and the number of IP phone unit licenses. When the number of phones exceeds the number of licenses, it issues alarms to notify the administrator. This service runs on all the nodes, but the service on the first node has the responsibility for issuing and reclaiming licenses.
A Cisco DB	**Serviceability/Tools** > **Control Center - Feature Services**	Cisco License Mgr	3	This service periodically checks the expiration status of certificates that Cisco Unified Communications Manager generates and sends notification when a certificate gets close to its expiration date.
A Cisco DB Replicator	CLI utils service restart Cisco Database Layer Monitor	certM	3	The Cisco Database Layer Monitor service monitors aspects of the database layer. This server takes responsibility for change notification and monitoring.
Cisco Tomcat	**Serviceability/Tools** > **Control Center - Feature Services**	dbmon	3	The Cisco Log Partition Monitoring Tool service supports the Log Partition Monitoring feature, which monitors the disk usage of the log partition on a server (or all servers in the cluster) by using configured thresholds and a polling interval.
SNMP Master Agent	**Serviceability/Tools** > **Control Center - Feature Services**	Lpm Tool	3	Cisco CDP advertises Cisco Unified Communications Manager to other applications, so the application, for example, SNMP or CiscoWorks2000, can perform network management tasks for Cisco Unified Communications Manager.

Service	Stop | Start | Restart Instruction	Process Name	Auto Restart	Description
MIB2 Agent	**Serviceability/Tools** > **Control Center - Feature Services**	RisDC	3	The Real-time Information Server (RIS) maintains real-time Cisco Unified Communications Manager information such as device registration status, performance counter statistics, critical alarms generated, and so on. The Cisco RIS Data Collector service provides an interface for applications, such as Real-Time Monitoring Tool (RTMT), SOAP applications, Cisco Unified CM Administration and AlertMgrCollector (AMC) to retrieve the information that is stored in all RIS nodes in the cluster.
Host Resources Agent	**Serviceability/Tools** > **Control Center - Feature Services**	CiscoDRFMaster	3	The Cisco DRF Master Agent service supports the DRF Master Agent, which works with the graphical user interface (GUI) or command line interface (CLI) to schedule backups, perform restorations, view dependencies, check status of jobs, and cancel jobs, if necessary. The Cisco DRF Master Agent also provides the storage medium for the backup and restoration process.
Native Agent Adapter	**Serviceability/Tools** > **Control Center - Feature Services**	CiscoDRFLocal	3	The Cisco DRF Local service supports the Cisco DRF Local Agent, which acts as the workhorse for the DRF Master Agent. Components on a node register with the Cisco DRF Local Agent to use the disaster recovery framework. The Cisco DRF Local Agent executes commands that it receives from the Cisco DRF Master Agent. Cisco DRF Local Agent sends the status, logs, and command results to the Cisco DRF Master Agent.
System Application Agent	**Serviceability/Tools** > **Control Center - Feature Services**	cdrrep	3	You can start and stop the Cisco CDR Repository Manager service only on the first node, which contains the Cisco Unified Communications Manager database. This service starts automatically.
Cisco CDP Agent	**Serviceability/Tools** > **Control Center - Feature Services**	cdragent	3	The Cisco CDR Agent service transfers CDR and CMR files that are generated by Cisco Unified CallManager from the local host to the CDR repository node, where the CDR Repository Manager service runs over a SFTP connection. For this service to work, activate the Cisco CallManager service on the first node and ensure that it is running.

Service	Stop | Start | Restart Instruction	Process Name	Auto Restart	Description
Cisco Syslog Agent	CLI utils service restart System SSH	sshd	3	—
Cisco License Manager	Auto-restart being addressed by Cisco	syslogd	—	—
Cisco Certificate Expiry Monitor	CLI utils snmp hardware-agent restart **	—	—	IBM—snmpd, slp_srvreg cimlistener, cimserver, dirsnmpd, ""java... com.tivoli.twg.agent.TWGAgent"" **** HP
Cisco Database Layer Monitor	—	—	—	No API to monitor status of DRF Restoral Condition.
Cisco Log Partition Monitoring Tool	IBM process covered by SNMP Service	cimlistener	—	—
Cisco CDP	IBM process covered by SNMP Service	cimserver	—	—
Cisco RIS Data Collector	IBM process covered by SNMP Service	dirsnmpd	—	—
Cisco DRF Master	HP process covered by SNMP Service	—	—	—
Cisco DRF Local	HP process covered by SNMP Service	—	—	—
Cisco CDR Repository Manager	HP process covered by SNMP Service	—	—	—
Cisco CDR Agent	HP process covered by SNMP Service	—	—	—
SSH Service Status	HP process covered by SNMP Service	—	—	—
Syslog Service Status	HP process covered by SNMP Service	—	—	—
SNMP Service Status	HP process covered by SNMP Service	—	—	—

Service	Stop | Start | Restart Instruction	Process Name	Auto Restart	Description
DRF Restoral Condition	HP process covered by SNMP Service	—	—	—
Cmaperfd	HP process covered by SNMP Service	—	—	—
Cmasm2d	HP process covered by SNMP Service	—	—	—
Cmastdeqd	HP process covered by SNMP Service	—	—	—
Cmathreshd	HP process covered by SNMP Service	—	—	—
hpasm	HP process covered by SNMP Service	hpasm	—	—
hpasmxld	HP process covered by SNMP Service	hpasmxld	—	—
snmpsa-ah	INTEL process covered by SNMP Service	snmpsa-ah	—	—
Cisco Security Agent Service Status	Auto-restart being addressed by Cisco.	—	—	—
ciscosec	Indefinite	—	—	—
Cisco Electronic Notification	**Serviceability/Tools** > **Control Center - Feature Services**	enStart	3	—
Time Synchronization Service	—	ntpd	—	Auto-restarts according to 'init' rules (10 if instantaneous failure, otherwise higher).
Service Manager	CLI utils service restart Service Manager	servM	—	Auto-restarts according to 'init' rules (10 if instantaneous failure, otherwise higher).
Racoon DB	N/A	racoon	—	Internet Key Exchange (IKE) daemon for automatically keying IPsec connections. Auto-restarts according to 'init' rules (10 if instantaneous failure, otherwise higher).

Service	Stop | Start | Restart Instruction	Process Name	Auto Restart	Description
IP Sec Manager	—	ipsec _mgr	—	Auto-restarts according to 'init' rules (10 if instantaneous failure, otherwise higher).

*HOST-RESOURCES-MIB and possibly other MIBS fail to function or respond when this service is stopped.

**Only in Cisco Unified CM Release 5.1(3) and Release 6.1(1) and later releases.

***All of the listed processes may not be running as it is a function of the particular server model or what the service deems appropriate.

****There is more than one process by this name; second argument is relevant for distinction.

*****Feature Services are not activated by default.

The following table lists the critical SysLog test cases for Cisco Unified Communications Manager that require monitoring.

Table 2: Critical SysLog Test Cases

Test Case	Description
MGCPGatewayLostComm	Natively supported alarm—GUI Serviceability/Alarm/Catalog, CallManager, MGCPGatewayLostComm/Find"
SDLLinkOOS	Natively supported alarm—GUI Serviceability/Alarm/Catalog, CallManager, SDLLinkOOS/Find"

The following table lists the critical SNMP trap test cases for Cisco Unified Communications Manager that require monitoring.

Table 3: Critical SNMP Trap Test Cases

Test Case	Description
ccmGatewayFailedEvent	CCM-MIB::ccmGatewayFailed

IM and Presence Service Critical Services

Use Cisco Unified CM Administration to view the status of critical services and self-diagnostic test results for the IM and Presence Service node. The results of these self-diagnostic tests are displayed on the Node Details window:

- Verify IM and Presence Service Installed.
- Verify Node Reachable (pingable).
- Version: The version of the IM and Presence Service that is installed on the selected node.

The status of services that are listed on the Node Details window can be in one of three states:

- Started
- Stopped
- Failed

For more information about services on the IM and Presence Service node, see the *Cisco Unified Serviceability Administration Guide*.

The following table describes the critical services on the IM and Presence Service node that you can monitor on the Node Details window using Cisco Unified CM Administration.

Table 4: IM and Presence Services Node Details

Service Name	Process Name	Description
Cisco SIP Proxy	sipd	The Cisco SIP Proxy service is responsible for providing the SIP registrar and proxy functionality. This includes request routing, requestor identification, and transport interconnection.
Cisco Presence Engine	pe	The Cisco Presence Engine is responsible for presence composition. It takes sources of presence from the XMPP client for the user, on-hook and off-hook status from CUCM and in a meeting status from Microsoft Exchange to generate the users overall composed presence.
Cisco Login Datastore	ttlogin	The Cisco Login Datastore is a real-time database for storing client sessions to the Cisco Client Profile Agent.
Cisco Presence Datastore	ttsoft	The Cisco Presence Datastore caches presence data for users and replicates it between servers in a presence redundancy group for high availability operation.
Cisco Route Datastore	ttroute	This service is used if you configure SIP federation for the IM and Presence Service, or enable Partitioned Intradomain Federation.

Service Name	Process Name	Description
Cisco SIP Registration Datastore	ttreg	The Cisco Presence SIP Registration Datastore is a real-time database for storing SIP Registration data.
A Cisco DB	cmoninit	A Cisco DB acts as the Progress database engine.
Cisco XCP Router	jabberd	The Cisco XCP Router must be running for all availability and messaging services to function properly on IM and Presence. This applies to both SIP-based and XMPP-based client messaging. After IM and Presence Service installation, the system turns on Cisco XCP Router by default.
Cisco XCP Connection Manager	cm	The Cisco XCP Connection Manager enables XMPP clients to connect to the IM and Presence server.
Cisco XCP Authentication Service	auth	The Cisco XCP Authentication Service handles all authentication requests from XMPP clients connecting to IM and Presence Service.
Cisco Sync Agent	syncAgent	The Cisco Sync Agent keeps IM and Presence data synchronized with Cisco Unified Communications Manager data. It sends SOAP requests to the Cisco Unified Communications Manager for data of interest to IM and Presence Service and subscribes to change notifications from Cisco Unified Communications Manager and updates the IM and Presence Service IDS database.
Cisco Client Profile Agent	tomcat	The Cisco Client Profile Agent service provides a secure SOAP interface over HTTPS for external client connections.

Service Name	Process Name	Description
Cisco Intercluster Sync Agent	interClusterSyn	The Cisco Intercluster Sync Agent service provides the following: DND propagation to Cisco Unified Communications Manager and syncs end-user information between IM and Presence Service clusters for intercluster SIP routing.
Cisco XCP Message Archiver	tc	The Cisco XCP Message Archiver service supports the IM Compliance feature. The IM Compliance feature logs all messages sent to and from the IM and Presence server, including point-to-point messages, and messages from instant meeting (temporary) and chat rooms for the Chat feature. Messages are logged to an external Cisco-supported database.
Cisco XCP SIP Federation Connection Manager	cm_sip_fed	The Cisco XCP SIP Federation Connection Manager supports interdomain federation with Microsoft OCS over SIP. You also turn on this service when your deployment contains an intercluster connection between an IM and Presence Service Release 9.0 cluster and a Cisco Unified Presence Release 8.6 cluster.

Related Topics

View Presence Server Status, on page 15

View Presence Server Status

Use Cisco Unified CM Administration to view the status of critical services and self-diagnostic test results for the IM and Presence Service node.

Procedure

Step 1 Select **System** > **Server**.
The **Find and List Servers** window appears.

Step 2 Select the server search parameters, and then click **Find**.
Matching records appear.

Step 3 Select the IM and Presence server that is listed in the **Find and List Servers** window.
The **Server Configuration** window appears.

Step 4 Click on the Presence Server Status link in the IM and Presence Server Information section of the **Server Configuration** window.
The **Node Details** window for the server appears.

Available Supported MIBs

The following MIBs can be reviewed and used for monitoring system health:

- Cisco MIBs
  - CISCO-CCM-MIB
  - CISCO-CCM-CAPABILITY
  - CISCO-CSP-MIB
  - CISCO-SYSLOG-MIB
  - CISCO-SYSLOG-EXT-MIB
- Industry-Standard MIBs
  - SYSAPPL-MIB
  - HOST-RESOURCES-MIB
  - RFC1213-MIB (MIB-II)
  - IF-MIB

Related Topics

Cisco Management Information Base
CISCO-CCM-MIB
CISCO-CCM-CAPABILITY
CISCO-CDP-MIB
CISCO-SYSLOG-MIB
CISCO-SYSLOG-EXT-MIB
Industry-Standard Management Information Base
SYSAPPL-MIB
HOST-RESOURCES-MIB
RFC1213-MIB (MIB-II)
IF-MIB

RTMT Monitoring of Cisco Unified CM System Health

The following topics related to RTM monitoring of Cisco Unified CM system health are provided:

- RTMT summary view
- CPU usage
- %IOwait monitoring
- Virtual memory
- Disk usage
- Database replication and Cisco Unified Communication Manager nodes
- ccm process and CPU usage
- codeYellow
- RIS Data Collectory PerMonLog
- Critical service status
- RTMT syslog viewer
- RTMT alerts as syslog messages and traps

Related Topics

% IOwait Monitoring, on page 20
ccm process and CPU usage
CodeYellow, on page 26
CPU Usage, on page 18
Critical Service Status, on page 29
Database Replication and Cisco Unified Communication Manager Nodes, on page 26
Disk Usage, on page 23
RIS Data Collector PerfMonLog, on page 28
RTMT Alerts as Syslog Messages and Traps, on page 32
RTMT Summary View, on page 17
RTMT Syslog Viewer, on page 31
Virtual Memory, on page 21

RTMT Summary View

The RTMT summary view displays the overall health of the system, which should be monitored daily, including:

- CPU utilization level
- Memory utilization level
- Phone registration status

- Call in progress
- Gateway status

If CPU and memory utilization levels exceeds the 70 percent mark, then the Cisco Unified CM publisher and subscribers that are participating in call processing could be overloaded . Key indicators of system health and performance issues are:

- System Time, User Time, IOWait, soft irq, irq
- CPU Pegging Alerts
- Process using most CPU
- High % iowait
- High % iowait due to common partition
- Process responsible for Disk IO
- CodeYellow

If you do not want the RTMT client running on your workstation or PC all the time, you can configure a threshold for each alert that is of interest to you and how you want to be notified. Then you can close the RTMT client on your workstation or PC.

The RTMT backend, AMC service, which is up and running as soon as the Cisco Unified CM server is up and running, collects and processes all the information needed, and notifies you according to how you configured the notification.

RTMT CPU and memory page reports CPU usage in terms of the following:

- %System—CPU utilization percentage that occurred while executing at the system level (kernel)
- %User—CPU utilization percentage that occurred while executing at the user level (application).
- %IOWait—CPU percentage of time of idle waiting for outstanding disk I/O request.
- %SoftIrq—Percentage of time that the processor is executing deferred IRQ processing (for example, processing of network packets).
- %Irq—Percentage of time that the processor is executing the interrupt request which is assigned to devices for interrupt or sending a signal to the computer when it is finished processing.

CPU Usage

High CPU utilization can impact the call processing by creating delays or interruptions in the service. It could affect the end user service. Sometimes high CPU utilization is indicative of a memory leak. RIS DataCollector PerfMonLog when enabled tracks CPU usage.

Note Cisco recommends that RIS DataCollector PerfMonLog be enabled.

You can also monitor CPU usage by using APIs. Using the SOAP API, you can monitor the following perfmon counters:

- Under Processor object—% CPU Time, System Percentage, User Percentage, IOwait Percentage, Softirq Percentage, Irq Percentage
- Under Process object—% CPU Time

Using the SNMP interface, you can monitor the following perfmon counters:

- Host Resource MIB—hrProcessorLoad, hrSWRunPerfCPU
- CPQHOST-MIB—cpqHoCpuUtilMin, cpqHoCpuUtilFiveMin

If you see high CPU usage, identify which process is causing it. If %system and/or %user is high enough to generate CPUPegging alert, check the alert message to see the processes that are using the most CPU. You can go to the RTMT Process page, sort by %CPU to identify high CPU processes.

Note Cisco Unified Communications Manager VMware installations can experience high CPU usage spikes while performing tasks such as DRF backups and Bulk Administration Tool exports. The processes that are commonly responsible for CPU usage spikes are gzip and DRFLocal.

If your system is generating CallProcessingNodeCpuPegging alarms, add an additional vCPU for the support of 7500 Cisco Unified Communications Manager users following the Open Virtualization Archives (OVA) template specifications for your system.

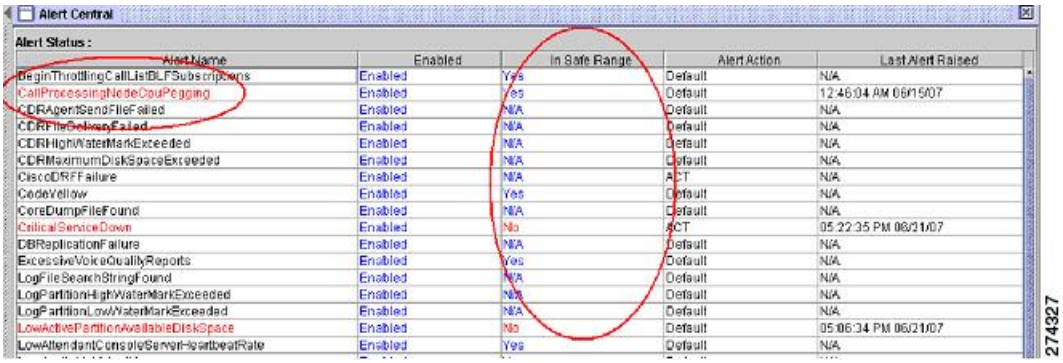
The following figure shows the CPU usage.

Figure 2: Cisco Unified Serviceability CPU Usage

For analysis, RIS Data Collector PerfMonLog tracks processes %CPU usage at system level.

RTMT monitors CPU usage and when CPU usage is above a threshold, RTMT generates CallProcessingNodeCPUPegging alert. The following figure shows the alert status.

Figure 3: RTMT Alert Central with Alert Status



Monitor the “In Safe Range” column often. If it is marked “No,” then the condition is not corrected. For example, if In Safe Range column displays No for CallProcessingNodeCPUPegging, then it means the CPU usage on that node is above the threshold and requires attention.

In addition to CallProcessingNodeCPUPegging, high CPU usage potentially causes the following alerts to trigger:

- CodeYellow
- CodeRed
- CoreDumpFileFound
- CriticalServiceDown
- LowCallManagerHeartbeatRate
- LowTFTPServerHeartbeatRate
- LowAttendantConsoleHeartRate

When a service crashes, the corresponding trace files may have been overwritten. Cisco TAC needs the trace files to troubleshoot the crash. In the case of CoreDumpFileFound, CodeYellow, and CriticalServiceDown, the Enable Trace Download option should be enabled to assist Cisco TAC.

% IOwait Monitoring

High %IOwait indicates high disk input/output (I/O) activities. Consider the following high IOwait conditions:

- Heavy memory swapping—Check %CPU Time for Swap Partition to see if there is high level of memory swapping activity. One potential cause of high memory swapping is memory leak.
- DB activity—Database accesses Active Partition. If %CPU Time for Active Partition is high, then most likely there are a lot of DB activities.
- Common (or Log) Partition in the trace and log files storage location—Check the following:
  - Trace Log Center to see if there is any trace collection activity going on. If call processing is impacted (ie, CodeYellow), then consider adjusting trace collection schedule. If zip option is used, please turning it off.

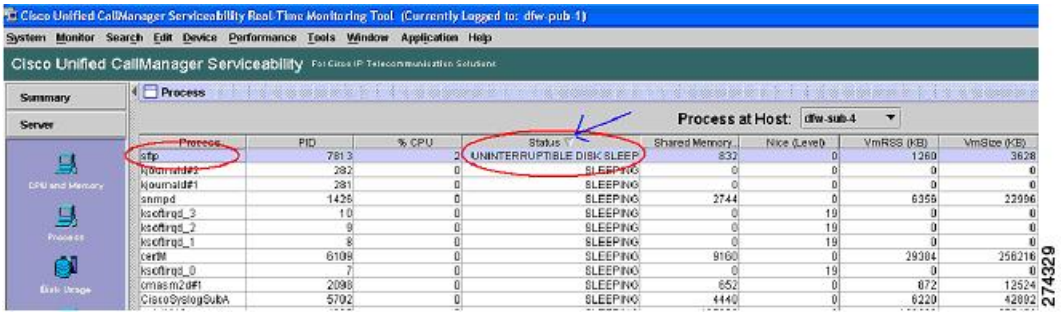
- Trace setting at the detailed level because Cisco Unified CM generates a lot of trace. If high %iowait and/or Cisco Unified CM is in CodeYellow state, and Cisco Unified CM service trace setting is at Detailed, please chance trace setting to “Error” to reduce the trace writing.

You can use RTMT to identify processes that are responsible for high %IOwait:

- If %IOwait is high enough to cause CPUPegging alert, check the alert message to check processes waiting for disk IO.
- Go to RTMT Process page, sort by Status. Check for processes in Uninterruptible Disk Sleep state
- Download RIS Data Collector PerfMonLog file to examine the process status for longer period of time.

The following figure shows an example of RTMT Process window sorted by Status. Check for processes in Uninterruptible Disk Sleep state. The FTP process is in the Uninterruptible Disk Sleep state.

Figure 4: FTP Process in Uninterruptible Disk Sleep State



Virtual Memory

Virtual memory consists of physical memory (RAM) and swap memory (Disk). The RTMT CPU and Memory window has system level memory usage information as the following:

- Total—total amount of physical memory
- Free—amount of free memory
- Shared—amount of shared memory used
- Buffers—amount of memory used for buffering purpose
- Cached—amount of cached memory
- Used—calculated as Total – Free – Buffers – Cached + Shared
- Total Swap—total amount of swap space
- Used Swap—the amount of swap space in use on the system.
- Free Swap—the amount of free swap space available on the system

Note Using SOAP APIs, you can query memory information for the following perfmon counters:

- Under Memory object—% Mem Used, % VM Used, Total Kbytes, Total Swap Kbytes, Total VM Kbytes, Used Kbytes, Used Swap Kbytes, Used VM Kbytes
- Under Process object—VmSize, VmData, VmRSS, % Memory Usage

Using SNMP, you can query the following perfmon counters:

- Host Resource MIB—hrStorageSize, hrStorageUsed, hrStorageAllocationUnits, hrStorageDescr, hrStorageType, hrMemorySize

Note You can download some historical information by using RTMT Trace Log Central. The Cisco AMC Service PerfMonLog is enabled by default. Deprecated in Cisco Unified CM Release 6.0 because Cisco RIS Data Collector PerfMonLog was introduced. The Cisco RIS Data Collector PerfMonLog disabled by default in Cisco Unified CM Release 5.x and enabled by default in Cisco Unified CM Release 6.0.

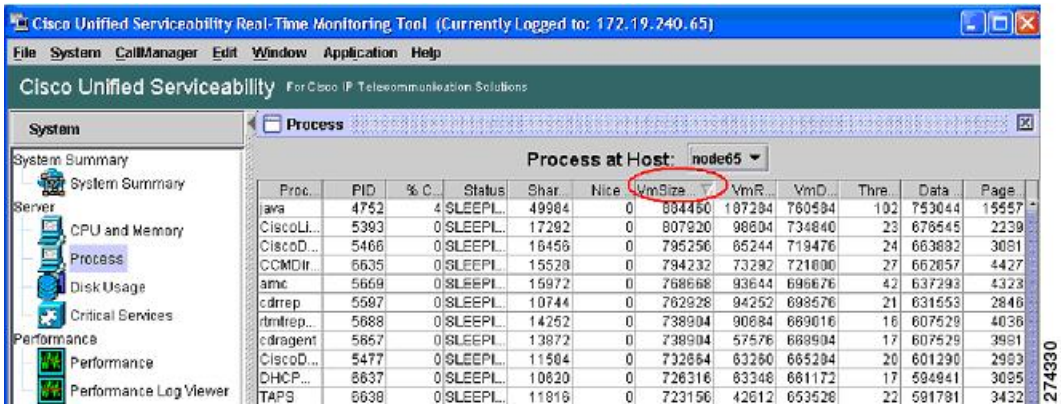
Note Perfmon Virtual Memory refers to Total (Physical + Swap) memory whereas Host Resource MIB Virtual Memory refers to Swap memory only.

The RTMT Process window displays process level memory usage information as follows:

- VmSize—Total virtual memory used by the process
- VmRSS—Resident Set currently in physical memory used by the process including Code, Data and Stack
- VmData—Virtual memory usage of heap by the process
- Page Fault Count—Represents the number of major page faults that a process encountered that required the data to be loaded into physical memory

The following figure shows RTMT Process window. You can sort VmSize by clicking on VmSize tab. Then you can identify which process consumes more memory.

Figure 5: VmSize Listed by RTMT Process



Possible memory leak causes can be from the VmSize continuously increasing.

When a process leaks memory, the system administrator should report it to Cisco and include trace files. Ris Data Collector PerfMonLog collects the data and it contains historical information on memory usage.

Disk Usage

There are four disks or partitions in the Cisco Unified CM hard drive:

- Common partition (log partition)—Contains the trace/log files
- Active partition—Contains files (binaries, libraries and config files) of active OS and the Cisco Unified CM release
- Inactive partition—Contains files for alternative Cisco Unified CM release (for example, an older version that was upgraded from or newer version recently upgraded to but the server has not been toggled to this release).
- Swap partition—Used for swap space.

Using SOAP APIs, you can get partition information for the following perfmon counters:

- Under Partition object—Total Mbytes, Used Mbytes, Queue Length, Write Bytes Per Sec, Read Bytes Per Sec

Using the SNMP MIB, you can query the following information:

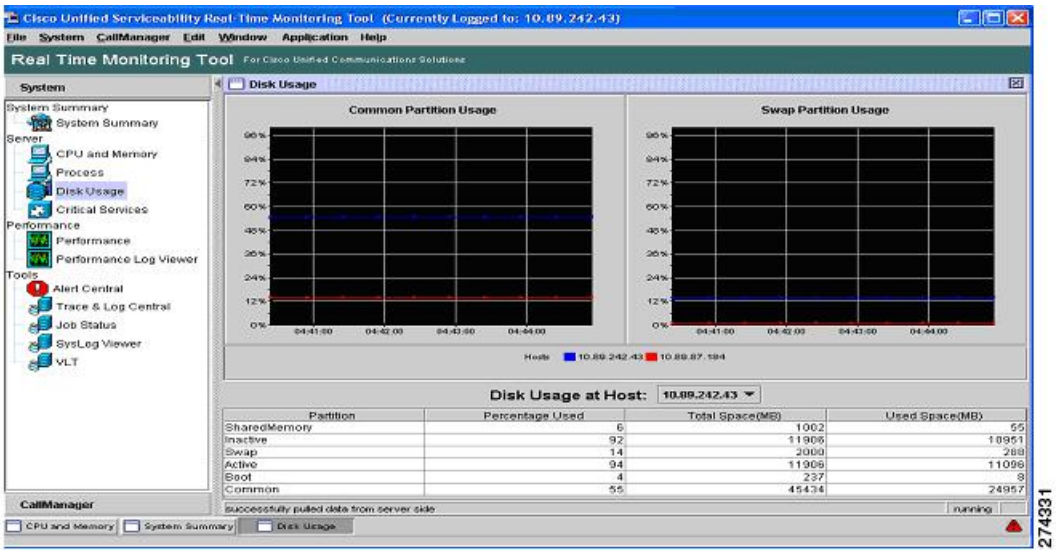
- Host Resource MIB—hrStorageSize, hrStorageUsed hrStorageAllocationUnits, hrStorageDescr, hrStorageType

You can download the following historical information by using RTMT Trace and Log Central:

- Cisco AMC Service PerfMonLog // enabled by default. Deprecated in Cisco Unified CM 6.0, because Cisco RIS Data Collector PerfMonLog is introduced.
- Cisco RIS Data Collector PerfMonLog // disabled by default in Cisco Unified CM 5.x; enabled by default in Cisco Unified CM 6.0

The following figure shows disk usage in RTMT.

Figure 6: Disk Usage by Partition



Disk Name Mapping

Perfmon instance names as shown in RTMT and SOAP are:

- Active
- Inactive
- Common
- Boot
- Swap
- SharedMemory

Names shown in Host Resource MIB hrStorage description are:

- /partB
- /common
- /grub
- Virtual Memory
- /dev/shm

The partition alerts are as follows:

- LogPartitionLowWaterMarkExceeded—Occurs when the percentage of used disk space in the log partition has exceeded the configured low water mark. This alert should be considered as early warning

for an administrator to clean up disk space. You can use RMT Trace/Log Central to collect trace/log files and then delete these trace/log files from the server. In addition to manually clean up the traces/log files, the system administrator should also adjust the number of trace files to be kept to avoid hitting low water mark again.

- LogPartitionHighWaterMarkExceeded—Occurs when the percentage of used disk space in the log partition has exceeded the configured high water mark. When this alert is generated, Log Partition Monitoring (LPM) utility starts to delete files in Log Partition until the Log Partition is down to the low water mark to avoid running out of disk space. Since LPM may delete some files that you want to keep, you need to act upon receiving LogPartitionLowWaterMarkExceed alert.
- LowActivePartitionAvailableDiskSpace—Occurs when the percentage of available disk space of the Active Partition is lower than the configured value. Please use the default threshold that Cisco recommends. At default threshold, this alert should never be generated. If this alert occurs, a system administrator can adjust the threshold as temporary workaround but Cisco TAC should look into this. One place to look is /tmp using remote access. We have seen cases where large files are left there by 3rd party software.
- LowInactivePartitionAvailableDiskSpace—Occurs when the percentage of available disk space of the InActive Partition is lower than the configured value. Please use the default threshold that Cisco recommends. At default threshold, this alert should never be generated. If this alert occurs, a system administrator can adjust the threshold as temporary workaround but Cisco TAC should look into this.

The following table shows a comparison of disk-related perfmon counters between Cisco Unified CM Release 4.x and Cisco Unified CM Release 5.x.

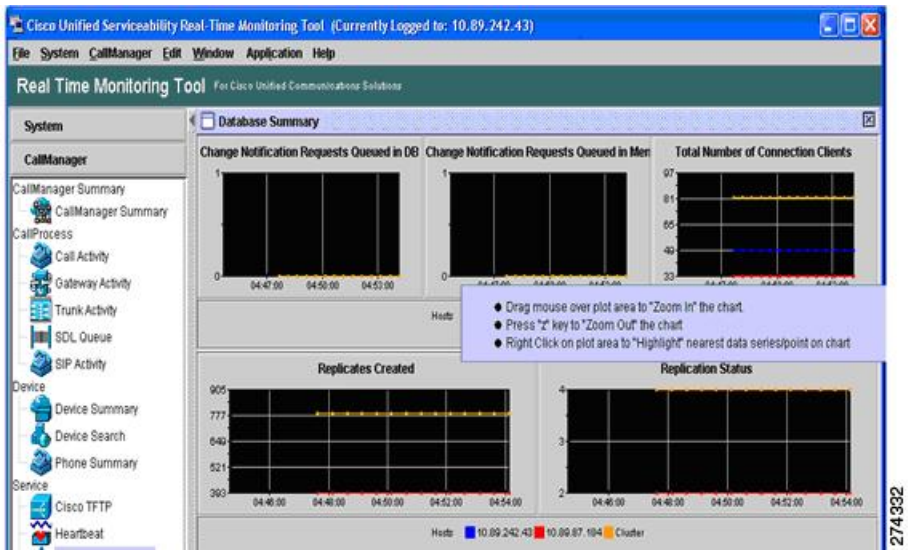
Table 5: Disc-Related Perfmon Counters

Cisco Unified CM Release 4.x Perfmon Counters		Cisco Unified CM Release 5.x Perfmon Counters	
Logical Disk	% Disk Time	Partition	% CPU Time
	Disk Read Bytes/sec		Read Kbytes Per Sec
	Disk Write Bytes/sec		Write Kbytes Per Sec
	Current Disk Queue Length		Queue Length
	Free Megabytes		Used Mbytes
			Total Mbytes
	% Free Space		% Used

Database Replication and Cisco Unified Communication Manager Nodes

You can use RTMT Database Summary to monitor your database activities as shown in the following figure. For example, click **CallManager** > **Service** > **Database Summary**.

Figure 7: Database Summary in RTMT



CodeYellow

CodeYellow state occurs when the ccm process is so overloaded that it cannot process incoming calls anymore. In this case, ccm initiates call throttling.This does not mean that one processor CPU usage is at 100 percent and the remaining processors are operating at 0 percent in RTMT.

Since the main thread can run on processor A for 1/10th of a second and processor B on the next 2/10th of a second, etc., the CPU usage shown in RTMT would be more balanced. By default RTMT shows average CPU usage for a 30-second duration.

You can configure the CodeYellow alert so that once it occurs, the trace files can be downloaded for troubleshooting purposes.

The AverageExpectedDelay counter represents the current average expected delay for handling any incoming message. If the value is above the value specified in “Code Yellow Entry Latency” service parameter, CodeYellow alarm is generated. This counter is one of key indicator of call processing performance issue.

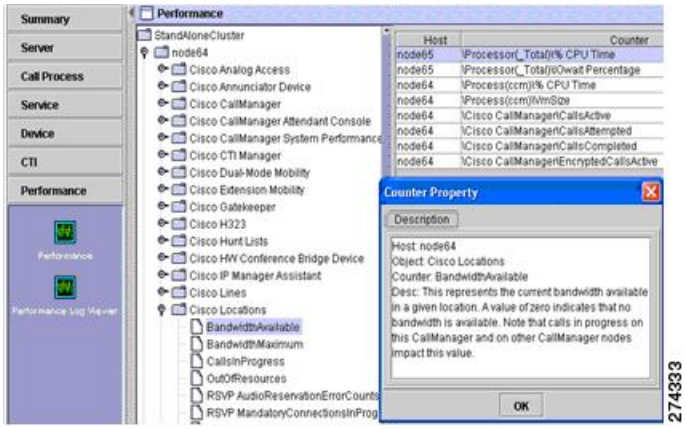
If you see CodeYellow, but the total CPU usage is only 25 percent, it is because Cisco Unified CM needs one processor for call processing. When no processor resource is available, CodeYellow may occur even when the total CPU usage is only around 25 to 30 percent in a 4-virtual processor server. Similarly on a 2 processor server, CodeYellow is possible around 50 percent of total CPU usage.

Other perfmon counters should be monitored are:

- Cisco CallManager\CallsActive, CallsAttempted, EncryptedCallsActive, AuthenticatedCallsActive, VideoCallsActive
- Cisco CallManager\RegisteredHardwarePhones, RegisteredMGCPGateway
- Cisco CallManager\T1ChannelsActive, FXOPortsActive, MTPResourceActive, MOHMulticastResourceActive
- Cisco Locations\BandwidthAvailable
- Cisco CallManager System Performance\AverageExpectedDelay
- CodeYellow
- DBReplicationFailure
- LowCallManagerHeartbeat
- ExcessiveVoiceQualityReports
- MaliciousCallTrace
- CDRFileDeliveryFailure/CDRAgentSendFileFailed
- Critical Service Down
- CoreDumpFileFound

The following figure displays the RTMT performance window.

Figure 8: RTMT Performance of Stand Alone Clusters



Note In general, Cisco Unified CM Release 4.x perfmon counters have been preserved by using the same names and representing the same values.

RIS Data Collector PerfMonLog

In Cisco Unified CM Release 5.x, the RIS Data Collector PerfMonLog file is not enabled by default. It is recommended that RIS Data Collector PerfMonLog is enabled to assist in troubleshooting. It tracks CPU, memory, disk, and the network. If you enable RIS Data Collector PerfMonLog, then you can disable AMC PerfMonLog. In Cisco Unified CM Release 6.x, RIS Data Collector PerfMonLog replaced AMC PerfMonLog.

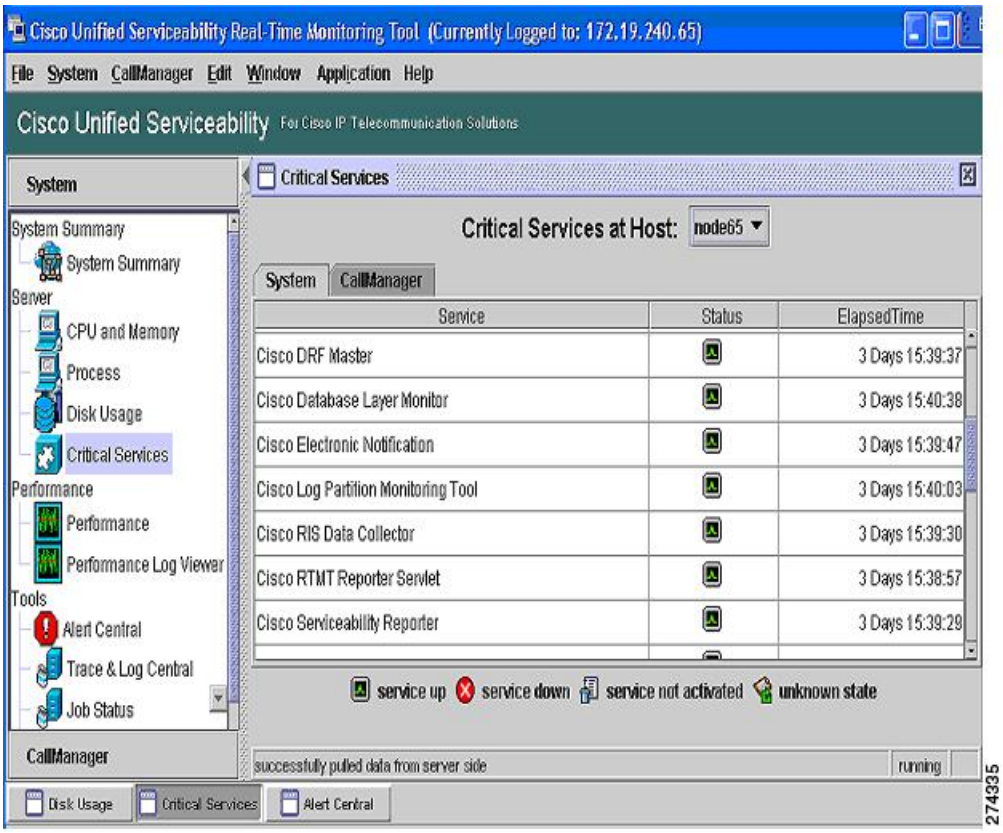
Note With RIS Data Collector PerfMonLog enabled, the impact on the CPU is small, around 1%.

Use RTMT Trace and Log Center to download Cisco RIS Data Collector PerfMonLog files for the time period that you are interested in. Open the log file using Windows Perfmon Viewer (or RTMT Perfmon viewer), then add Performance counters of interest such as:

- CPU usage > Processor or Process % CPU
- Memory usage > Memory %VM Used
- Disk usage > Partition % Used
- Call Processing > Cisco CallManager CallsActive

The following figure shows the output of the Windows Perfmon Viewer.

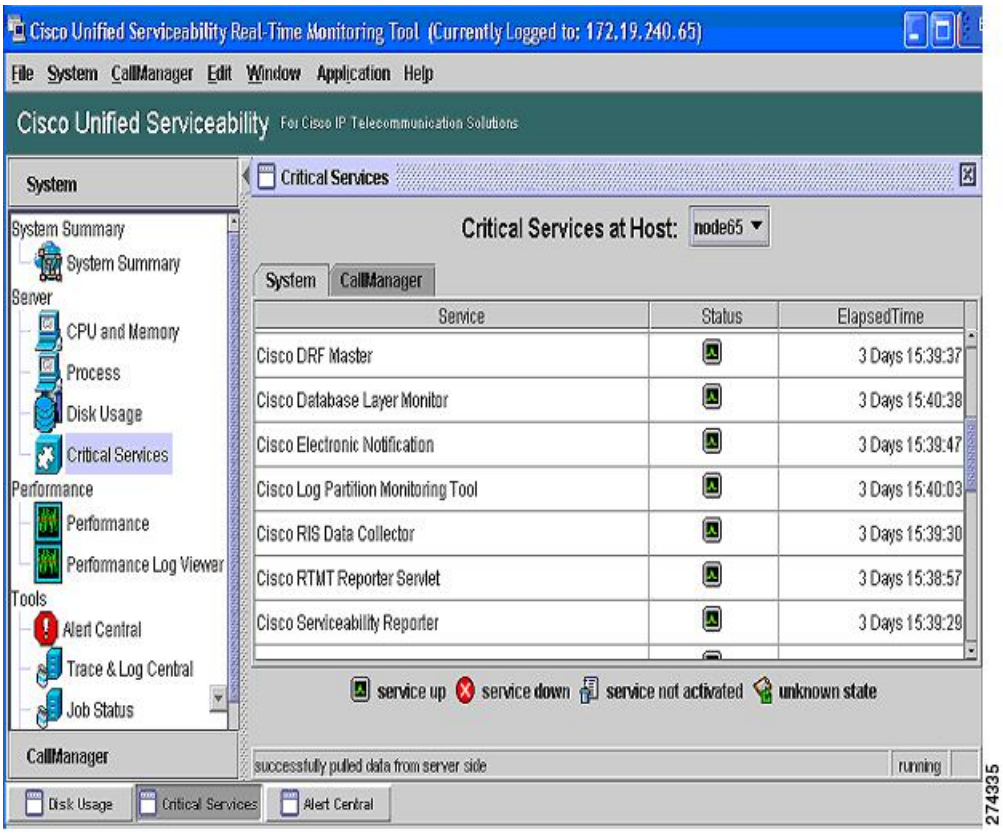
Figure 9: Windows Perfmon Viewer



Critical Service Status

The RTMT Critical Service window provides current status of all critical services as shown in the following figure.

Figure 10: Critical Service Window in RTMT



CriticalServiceDown alert is generated when any of service is down. By default, RTMT back-end service checks for the status every 30 seconds. It is possible if the service goes down and comes back up within that period, the CriticalServiceDown alert may not be generated.

CriticalServiceDown alert monitors only those services listed in RTMT Critical Services page. If you suspect if service got restarted without generating Core files, check the RTMT Critical Service page has elapsed time and Check RIS Troubleshooting perfmon log files and see if PID for service (process) is changed.

The following CLI can be used to check the logs of Service Manager:

- file get activelog platform/servm_startup.log
- file get activelog platform/log/servm*.log

The following CLI can be used to duplicate certain RTMT functions:

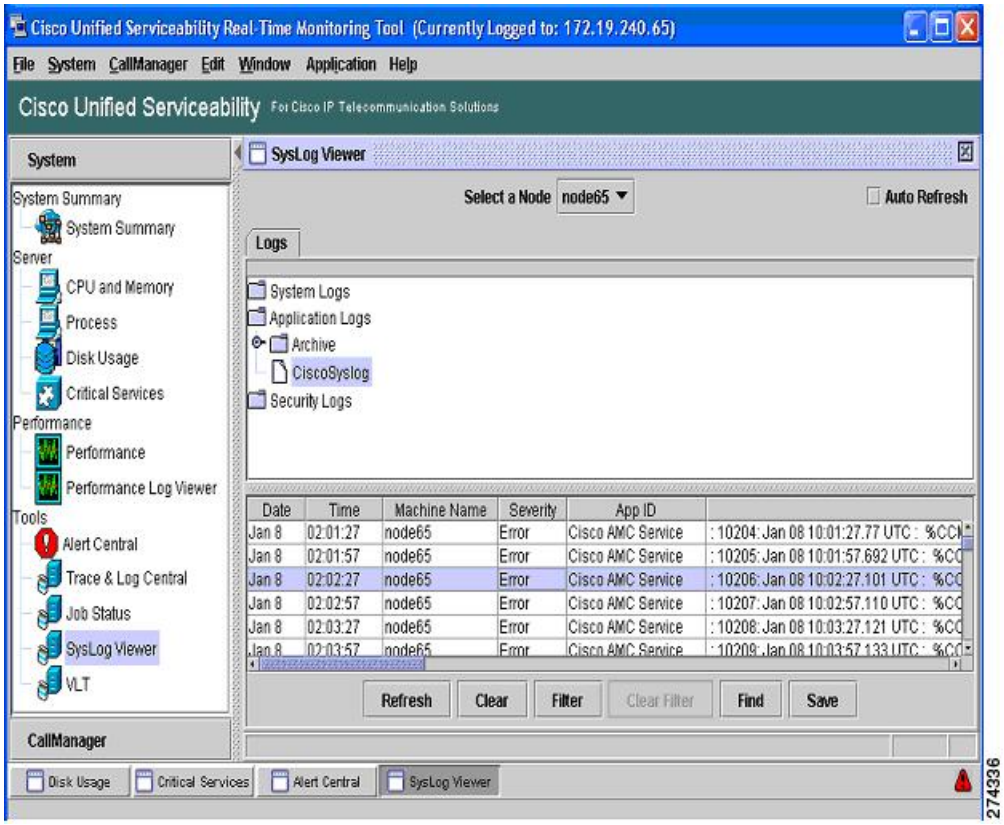
- admin:utils service
- show perf
- show risdb

CoreDumpFileFound alert is generated when RTMT backend service detects new Core Dump file. Both CriticalServiceDown and CoreDumpFileFound alert can be configured to download corresponding trace files for troubleshooting purpose. This helps to preserve trace files at the time of a crash.

RTMT Syslog Viewer

Syslog messages can be viewed using RTMT syslog viewer as shown in the following figure.

Figure 11: Syslog Viewer



Send Syslog Traps to Remote Server

To send syslog traps to a remote server for the CISCO-SYSLOG-MIB follow these steps:

Procedure

Step 1 Setup Trap (Notification) destination in Cisco Unified Serviceability SNMP window.

Step 2 Enable trap generation in CISCO-SYSLOG-MIB.

Step 3 Set the appropriate SysLog level in CISCO-SYSLOG-MIB.
If syslog traps are not being generated for some Cisco Unified CM service alarms, check the RTMT syslog viewer to see if the alarms are shown there. If not, adjust alarm configuration setting to send alarms to local syslog.

Syslogs generated due to hardware failures have an event severity of 4 or higher and contain one of the following patterns:

- *cma*[???]:*
- *cma*[????]:*
- *cma*[?????]:*
- *hp*[???]:*
- *hp*[????]:*
- *hp*[?????]:*

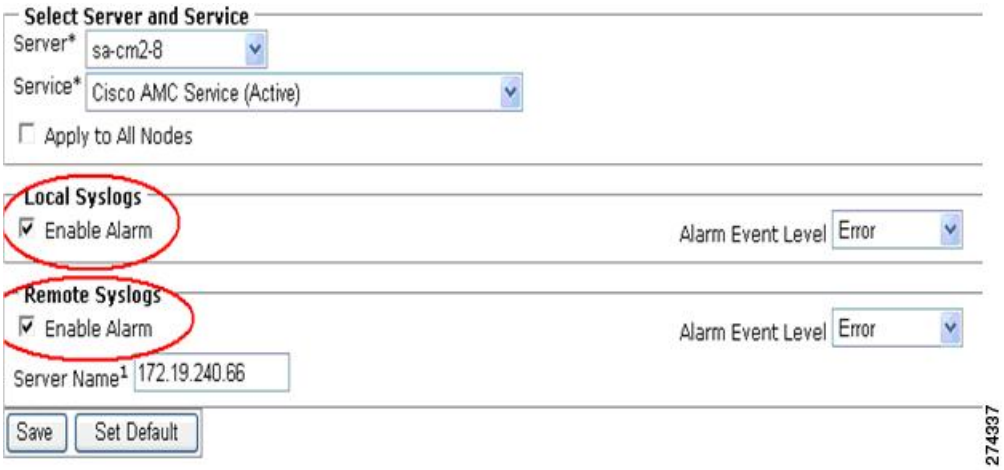
You can search for the above patterns to find hardware failure events in syslog.

For information on alarm configuration, refer to the Alarm Configuration section of the *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/5_1_3/ccmsrva/saalarm.html

RTMT Alerts as Syslog Messages and Traps

RTMT alerts can be sent to a remote syslog server. To send to a local and remote syslog server, configure the AMC alarm in Cisco Unified Serviceability. The following figure shows the window.

Figure 12: Local and Remote Syslog Configuration



Recovery Hardware Migration and Backup/Restore

Backup/Restore

Cisco provides the following backup/restore utilities:

- Cisco Unified CM Release 4.x uses the Backup and Restore System (BARS) application

- Cisco Unified CM Release 5.x uses the Disaster Recovery Framework (DRF)
- Cisco Unified CM Release 6.x uses the Disaster Recovery System (DRS), essentially a renaming of DRF above

These tools support writing backup files to (or reading restore files from) a local tape drive, or a file on a network location. BARS uses Windows shares and DRF/DRS use SFTP to access the network location. If a third-party backup solution is desired, BARS/DRF/DRS can write to a network location for the third-party backup solution to pick up.

DRF/DRS perform a cluster-wide backup, meaning data from all nodes is backed up, but restores are only to the node (s) that need it.

For more details, including what is configured to be included in the backup or what files are created, refer to the following documents depending on release:

- *Disaster Recovery System Administration Guide*
- *Cisco IP Telephony Disaster Recovery Administration Guide*
- *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide*

It is recommended to take a fresh backup every time an install, upgrade or options install is done to the appliance, whether or not configuration data changes were made.

If a catastrophic hardware failure occurs and the hardware must be replaced, reinstall Cisco Unified CM on the new hardware, then perform a restore from your backup.

Note Drive pull/swap is not supported as a fast recovery solution for the appliance.

Refer to the Replacing a Single Server or Cluster for Cisco Unified Communications Manager chapter of your release of *Cisco Unified Communications Manager Install and Upgrade Guide* at this index:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html

Platform Monitoring

This section describes hardware-layer monitoring for system component temperature, fan status, power supply status, RAID and disk status, network status, and operational status. CPU status/utilization and Memory status/utilization are covered in another section.

How to Use Command Line Interface

Hardware BIOS RAID and Firmware View Details Commands

System BIOS is viewable during the server boot sequence. The following commands are useful to view details about hardware, BIOS, RAID, and firmware. These items are included as part of the Cisco Unified CM image and do not need to be managed separately as in Cisco Unified CM Release 4.x, but may need to be inspected during diagnostic activity.

```
show hardwareshow environment [fans | power-supply | temperature]
show tech all
utils create report hardware
```

admin:utils fior CLI

You can also use the admin:utils fior status CLI to isolate which process causes high IOwait.

For example, at the command prompt type admin:utils fior list. This displays the following:

```
2007-05-31 Counters Reset
Time       Process   PID    State   Bytes Read   Bytes Written
17:02:45   rpmq      31206  Done    14173728     0
17:04:51   java      31147  Done    310724       3582
17:04:56   snmpget   31365  Done    989543       0
17:10:22   top       12516  Done    7983360      0
17:21:17   java      31485  Done    313202       2209
17:44:34   java      1194   Done    92483        0
17:44:51   java      1231   Done    192291       0
17:45:09   cdpd      6145   Done    0            2430100
17:45:25   java      1319   Done    192291       0
17:45:31   java      1330   Done    192291       0
17:45:38   java      1346   Done    192291       0
17:45:41   rpmq      1381   Done    14172704     0
17:45:44   java      1478   Done    192291       0
17:46:05   rpmq      1540   Done    14172704     0
17:46:55   cat       1612   Done    2560         165400
17:46:56   troff     1615   Done    244103       0
18:41:52   rpmq      4541   Done    14172704     0
18:42:09   rpmq      4688   Done    14172704     0
```

Use admin:utils fior top CLI for output that is sorted by top disk users. This displays the following:

```
Top processes for interval starting 2007-05-31 15:27:23
Sort by Bytes Written
Process     PID       Bytes Read    Read Rate     Bytes Written   Write Rate
Linuxzip    19556     61019083      15254771      12325229        3081307
Linuxzip    19553     58343109      11668622      9860680         1972136
Linuxzip    19544     55679597      11135919      7390382         1478076
installdb   28786     3764719       83660         6847693         152171
Linuxzip    20150     18963498      6321166       6672927         2224309
Linuxzip    20148     53597311      17865770      5943560         1981187
Linuxzip    19968     9643296       4821648       5438963         2719482
Linuxzip    19965     53107868      10621574      5222659         1044532
Linuxzip    19542     53014605      13253651      4922147         1230537
mv          5048      3458525       3458525       3454941         3454941
```

Related Topics

admin:utils diagnose list CLI, on page 34
admin:utils diagnose test CLI, on page 35
admin:utils diagnose moduleName CLI, on page 35
admin:utils diagnose fix CLI, on page 35
admin:utils create report hardware CLI, on page 35
admin:utils iostat CLI, on page 35

admin:utils diagnose list CLI

Displays all available diagnostic tests as follows:

```
Available diagnostics modules
disk_space           - Check available disk space as well as any unusual disk usage
service_manager      - Check if service manager is running
tomcat               - Check if Tomcat is deadlocked or not running
```

admin:utils diagnose test CLI

Executes each diagnostic test. It will not attempt to repair anything. This displays:

```
Starting diagnostic test(s)==========================
test - disk_space          —Passed
test - service_manager     —Passed
test - tomcat              —Passed
Diagnostics Completed
```

admin:utils diagnose moduleName CLI

Executes a single diagnostic test and attempt to fix the problem. You can also use admin:utils diagnose fix CLI to run all of the diagnostic tests at once. For example, admin:utils diagnose module tomcat displays:

```
Starting diagnostic test(s)==========================
test - tomcat              —Passed
Diagnostics Completed
```

admin:utils diagnose fix CLI

Execute all diagnostic tests, and if possible, attempt to repair the system. This displays:

```
Starting diagnostic test(s)==========================
test - disk_space          —Passed
test - service_manager     —Passed
test - tomcat              —Passed

Diagnostics Completed
```

admin:utils create report hardware CLI

Creates a system report containing disk array, remote console, diagnostic, and environmental data. No parameters are required. This displays:

```
***   W A R N I N G   ***
This process can take several minutes as the disk array, remote console,
system diagnostics and environmental systems are probed for their current
values.
Continue? Press y or Y to continue, any other key to cancel request.
Continuing with System Report request...
Collecting Disk Array Data...SmartArray Equipped server detected...Done
Collecting Remote Console Data...Done
Collecting Model Specific System Diagnostic Information...Done
Collecting Environmental Data...Done
Collecting Remote Console System Log Data...Done
Creating single compressed system report...Done
System report written to SystemReport-20070730020505.tgz
To retrieve diagnostics use CLI command:
file get activelog platform/log/SystemReport-20070730020505.tgz
```

admin:utils iostat CLI

Provides the iostat output for the given number of iterations and interval. Displays the interval in seconds between two iostat readings and the number of iostat iterations to be performed. This displays:

```
Executing command... Please be patient
Tue Oct  9 12:47:09 IST 2007
Linux 2.4.21-47.ELsmp (csevdir60)
10/09/2007 Time—12:47:09 PM
```

```
avg-cpu %user   %nice   %sys  %iowait %idle
        3.61    0.02    3.40  0.51    92.47
Device  rrqm/s  wrqm/s  r/s   w/s     rsec/s  wsec/s   rkB/s  wkB/s   avgrq-sz avgqu-sz
await  svctm
sda     3.10    19.78   0.34  7.49    27.52   218.37   13.76  109.19  31.39    0.05
5.78   0.73
sda1    0.38    4.91    0.14  0.64    4.21    44.40    2.10   22.20   62.10    0.02
26.63  1.62
sda2    0.00    0.00    0.00  0.00    0.00    0.00     0.00   0.00    10.88    0.00
2.20   2.20
sda3    0.00    0.00    0.00  0.00    0.00    0.000.00 0.00   0.00    10.88    0.00
2.20   2.20
sda4    0.00    0.00    0.00  0.00    0.00    0.00     0.00   0.00    10.88    0.00
2.20   2.20
sda5    0.00    0.08    0.01  0.01    0.04    0.73     0.02   0.37    64.43    0.00
283.91 69.81
sda6    2.71    14.79   0.20  6.84    23.26   173.24   11.63  86.62   27.92    0.02
2.98   0.61
```

CLI for Intracluster Connection Management and Monitoring

The following CLI can be used to monitor and manage intracluster connections:

- admin:utils dbreplication status
- admin:utils dbreplication repair all/nodename
- admin:utils dbreplication reset all/nodename
- admin:utils dbreplication stop
- admin:utils dbreplication dropadmindb
- admin:utils dbreplication setrepltimeout
- show tech dbstateinfo
- show tech dbinuse
- show tech notify
- run sql <query>

Hardware Migration

Customers may wish to migrate their Cisco Unified CM to more powerful hardware, either to prepare for upgrading to a later Cisco Unified CM release that does not support the older hardware, or just to leverage capabilities only available in the more powerful hardware, such as increases in capacity/performance or RAID. The procedure is to backup from the old hardware, install the same Cisco Unified CM release to the new hardware, then restore on the new hardware.

Migrating to more powerful hardware may require a migration SKU to cover royalties Cisco owes to third-parties. If you are considering this, have your account team check the Guide to Cisco Unified CM Upgrades and Server Migrations, which is a supplement to the Cisco Unified CM Ordering Guide.

Platform Security

Related Topics

Locked-Down System, on page 37
Cisco Security Agent Support, on page 37
Security Patching and Updating, on page 37
Role-Based Access Control, on page 37

Locked-Down System

For security, Cisco Security Agent is included along with a built-in firewall controlling connectivity among all cluster nodes, via IP tables and sensitive ports defined by the application. No AntiVirus application is installed on the appliance. The native OS used by the appliance is also hardened to minimize attack surface and vulnerabilities; fewer than 200 of the thousands of available packages are used to eliminate unused software and the corresponding vulnerabilities.

No “on-box” e-mail clients or Web browsers are supported, all unnecessary logins have been removed or disabled, and all software is provided by Cisco and digitally signed to ensure it is authorized by Cisco. The GUI, CLI, and API interfaces that Cisco provides are the only methods to administer the system, and authentication is required for users to interact with them. It also useful to note that appliances of this sort are less frequently targets of malware than Microsoft Windows or other systems with open-system access to the native OS, so significantly fewer patches need to be applied to the base OS.

Cisco Unified CM regulates its TCP/UDP port usage. See the *Cisco Unified Communications Manager TCP and UDP Port Usage* document for each Cisco Unified CM release for the specific list.

Cisco Security Agent Support

The Appliance supports the “headless” or unmanaged Cisco Security Agent. A future release will add support for the event monitoring features of Cisco Security Agent Management Center, but not for policy edits and distribution.

Security Patching and Updating

The Appliance's software image contains all security updates and patches made to firmware, drivers, native OS, database and Cisco Unified CM application components. Customers who keep current with Cisco maintenance releases are automatically covered for security updates. For more details, refer to the Application Note “Appliance Security Update Process for Cisco Unified Communications Manager” (C27-412838-00), available on request from your Cisco account team.

Role-Based Access Control

Cisco Unified CM uses Multi-Layer Admin (MLA) for RBAC control over authorization to Cisco Unified CM configuration.

Software Configuration Management

The Cisco Unified CM server uses a bundled image including all components needed for the system in a single set of DVDs or software downloads. Unlike Cisco Unified CM Release 4.x in which there were up to 6 different components to manage for a total of 18 updates per year on average to stay current, the server has 2 components with an average of 5 updates per year to stay current.

It is recommended that you keep your system current with the latest maintenance release for a major/minor feature release. Major and minor release install files are available on DVD media kits or on Product Upgrade Tool at http://www.cisco.com.

Rebuilds, upgrade files for minor and maintenance releases, and Cisco option files and tools are available as software downloads from Software Center at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Customers wishing to receive automatic e-mail notification of availability of new files on Software Center should subscribe to the e-mail notification tool on that site. Engineering “special” releases are only available to customers by using Cisco Technical Assistance Center.

General Install and Upgrade Procedures

Unattended first-time installs can be performed by using the Cisco Unified Communications Answer File Generator at http://www.cisco.com/web/cuc_afg/index.html. For other details, see the online help and the document Installing Cisco Unified Communications Manager.

For upgrades and from the list, find the appropriate release for your upgrade in the following index:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html

Detect Installed Release and Packages

You have several methods to display the installed release and packages that are:

- show version [active | inactive] and show packages active commands
- Cisco Unified Operations Manager
- Unified OS Administration
- Cisco Unified Communications Manager
- SNMP

A third-party NMS can query the Cisco Unified CM release by using the following SNMP OID:

- .iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoCcmMIB.ciscoCcmMIBObjects.ccmGeneralInfo.ccmTable.ccmEntry.ccmVersion

The Cisco Unified CM licensing web page displays the uploaded license file release, which may or may not be an exact match for what is installed on the system.

Available Reports

Three different reports are available:

- RTMT reports
- Serviceability reports
- Cisco Unified reporting

RTMT Reports

RTMT has a number of pre-can screens for information such as Summary, Call Activity, Device Status, Server Status, Service Status, and Alert Status. RTMT “Summary” pre-can screen shows a summary view of Cisco Unified C M system health. It shows CPU, Memory, Registered Phones, CallsInProgress, and ActiveGateway ports & channels. This should be one of the first thing you want to check each day to make sure CPU & memory usage are within normal range for your cluster and all phones are registered properly.

Phone Summary and Device Summary pre-can screens provide more detailed information about phone and gateway status. If there are a number of devices that fail to register, then you can use the Admin Find/List page or RTMT device search to get further information regarding the problem devices. Critical Services pre-can screen displays the current running/activation status of key services. You can access all the pre-can screens by simply clicking the corresponding icons on the left.

Serviceability Reports

The Cisco Serviceability Reporter service generates daily reports in Cisco Unified CallManager Serviceability Web Page. Each report provides a summary that comprises different charts that display the statistics for that particular report. Reporter generates reports once a day on the basis of logged information, such as—

- Device Statistics Report
- Server Statistics Report
- Service Statistics Report
- Call Activities Report
- Alert Summary Report
- Performance Protection Report

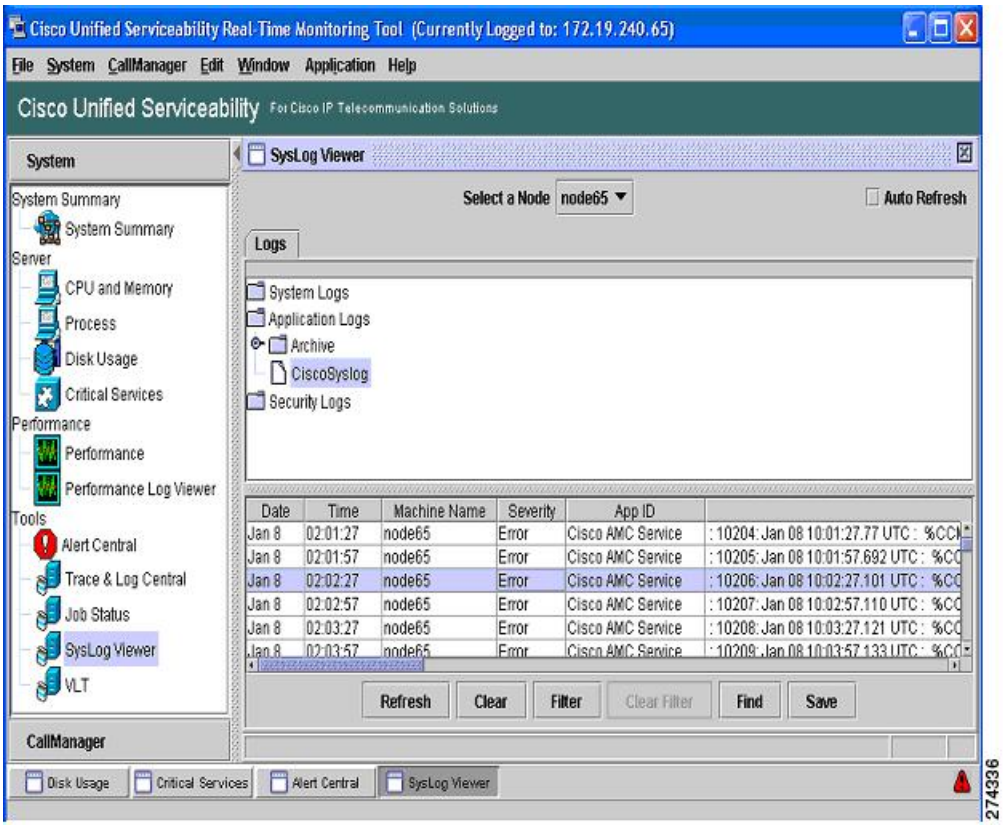
For detailed information about each report, go to http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/5_0_2/ccmsrvs/sssrvrep.html#wp1033420

Cisco Unified Reporting

Cisco Unified Reporting is accessed at the Cisco Unified CM Administration console and generates reports for troubleshooting or inspecting cluster data. It provides cluster data without requiring multiple steps to find the data. The tool design facilitates gathering data from existing sources, comparing the data, and reporting

irregularities. The following figure displays the available reports. Refer to the *Cisco Unified Reporting Administration Guide* for further detailed information.

Figure 13: System Reports



General Health and Troubleshooting Tips

For more information on troubleshooting, refer to the *Troubleshooting Guide for Cisco Unified Communications Manager* at the following index:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_troubleshooting_guides_list.html

Onboard Agents Support

Onboard agents are third-party software clients, agents or daemons installed on-box, including but not limited to:

- Anti-virus clients
- Uninterruptible Power Supply monitoring agents
- Management agents

Certain types of onboard agents are supported in Cisco Unified CM Release 4.x. The appliance used by Cisco Unified CM Release 5.0 and later releases does not support installation of onboard agents, rather it exposes APIs for third-party integration.

For more details, see the November 2007 bulletin on Third-Party Platform Agents at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_bulletins_list.html.

Call Detail Records and Call Maintenance Records

CDR and CMRs are used for a variety of uses including billing, chargeback, administrative oversight and diagnostics. In addition to a canned application for managing CDR/CMR, Cisco Unified CM Release 4.x supported various means of direct database access for external systems to access the CDR/CMR data. Cisco Unified CM Release 5.0 and later releases use SFTP to push formatted files off Cisco Unified CM to the requesting application.

When CDR is activated, a CPU utilization increase of 2% is typical, 4% if both CDR and CMR are activated.

Perfmon Counters

The following table lists some equivalent perfmon counters between Cisco Unified CM Release 4.x and Release 5.x and later.

Table 6: Equivalent Perfmon Counters

Cisco Unified CM Release 4.x Perfmon Counters		Cisco Unified CM Release 5.x Perfmon Counters	
Process	% Privileged Time	Process	STime
	% Processor Time		% CPU Time
Processor	% UserTime	Processor	User Percentage
	% Privileged Time		System Percentage
	% Idle Time		Nice Percentage
	% Processor Time		% CPU Time

Native Hardware Out of Band Management (OOB)

The supported features of HP iLO and IBM RSA II are enabled for the following areas:

- CPU status/utilization
- Memory status/utilization
- System components temperatures
- Fan status

- Power Supply status
- RAID & disk status
- Network status including NIC
- Operational status, including instrumentation of system/kernel status and data dumps following major system issues, indicating nature/type of the operational problem and degree of severity.

Support of these interfaces on the server includes the following capabilities (specific feature names vary by hardware vendor):

- Remote console (to access boot screens and the Cisco CLI)
- Remote power management

Phone Registration Status

Phone registration status needs to be monitored for sudden changes. If the registration status changes slightly and readjusts quickly over a short time frame, then it could be indicative of phone move, add, or change. A sudden smaller drop in phone registration counter can be indicative of a localized outage, for instance an access switch or a WAN circuit outage or malfunction. A significant drop in registered phone level needs immediate attention by the administrator. This counter especially needs to be monitored before and after the upgrades to ensure the system is restored completely.

Historical Information Download

You can also download some historical information using RTMT Trace Log Center or SOAP APIs, such as:

- Cisco AMC Service PerfMonLog is enabled by default but deprecated in Cisco Unified CM Release 6.0 because Cisco RIS Data Collector PerfMonLog is introduced.
- Cisco RIS Data Collector PerfMonLog is disabled by default in Cisco Unified CM Release 5.x and enabled by default in Cisco Unified CM Release 6.0.

Cisco CallManager Service Stops Responding

When the Cisco CallManager service stops responding, the following message displays in the System Event log:

```
The Cisco CallManager service terminated unexpectedly. It has done this
1 time. The following corrective action will be taken in 60000 ms.
Restart the service.
```

Other messages you may see in this situation:

```
Timeout 3000 milliseconds waiting for Cisco CallManager service to connect.
```

The Cisco Communications Manager failed to start due to the following error:

```
The service did not respond to the start or control request in a timely
fashion.
```

At this time when devices such as the Cisco Unified IP Phones and gateways, unregister from the Cisco Unified Communications Manager, users receive delayed dial tone, and/or the Cisco Unified Communications Manager server freezes due to high CPU usage. For event log messages that are not included here, view the Cisco Unified Communications Manager Event Logs.

Possible Cause The Cisco CallManager service can stop responding because the service does not have enough resources such as CPU or memory to function. Generally, the CPU utilization in the server is 100 percent at that time.

Solution Depending on what type of interruption you experience, you will need to gather different data that will help determine the root cause of the interruption.

Related Topics

Investigate Cisco CallManager Service Interruption, on page 43

Investigate Cisco CallManager Service Interruption

Depending on what type of service interruption you experience, you will need to gather different data that will help determine the root cause of the interruption.

You can do the following task if a lack of resources interruption occurs.

Procedure

Step 1 Collect Cisco CallManager traces 15 minutes before and after the interruption.

Step 2 Collect SDL traces 15 minutes before and after the interruption.

Step 3 Collect perfmon traces if available.

Step 4 If the traces are not available, start collecting the perfmon traces and track memory and CPU usage for each process that is running on the server. These will help in the event of another lack of resources interruption.

Database Replication Fails Between the Publisher and Subscriber

Replicating the database represents a core function of Cisco Unified Communications Manager clusters. The server with the master copy of the database acts as the publisher (first node), while the servers that replicate the database comprise subscribers (subsequent nodes).

Tip Before you install Cisco Unified Communications Manager on the subscriber server, you must add the subscriber to the Server Configuration window in Cisco Unified CM Administration to ensure that the subscriber replicates the database that exists on the publisher database server. After you add the subscriber server to the Server Configuration window and then install Cisco Unified Communications Manager on the subscriber, the subscriber receives a copy of the database that exists on the publisher server.

Changes that are made on the publisher server are not reflected on phones that are registered with the subscriber server.

Possible Cause Replication fails between the publisher and subscriber servers.

Solution Verify and, if necessary, repair database replication.

Related Topics

Verify and Repair Database Replication, on page 44

Verify and Repair Database Replication

Procedure

Step 1 Verify database replication. You can use the CLI, Cisco Unified Reporting, or RTMT to verify database replication.

a) To verify using the CLI, see Step 2, on page 44.
b) To verify using Cisco Unified Reporting, see Step 3, on page 44.
c) To verify using RTMT, see Step 4, on page 45.

Step 2 To verify database replication using the CLI, access the CLI and issue the following command to check replication on each node. You will need to run this CLI command on each node to check its replication status. Also, after a subscriber is installed, depending on the number of subscribers, it may take a considerable amount of time to achieve a status of 2.:

```
admin: show perf query class "Number of Replicates Created and State of Replication"
==>query class :

- Perf class (Number of Replicates Created and State of Replication)
has instances and values:
ReplicateCount  -> Number of Replicates Created   = 344
ReplicateCount  -> Replicate_State                = 2
```

Be aware that the Replicate_State object shows a value of 2 in this case. The following list shows the possible values for Replicate_State:

a) 0—This value indicates that replication did not start. Either no subsequent nodes (subscribers) exist, or the Cisco Database Layer Monitor service is not running and has not been running since the subscriber was installed.
b) 1—This value indicates that replicates have been created, but their count is incorrect.
c) 2—This value indicates that replication is good.
d) 3—This value indicates that replication is bad in the cluster.
e) 4—This value indicates that replication setup did not succeed.

Step 3 To verify database replication using Cisco Unified Reporting, perform the following tasks.

a) From the Navigation drop-down list box in the upper, right corner in Cisco Unified CM Administration, choose Cisco Unified Reporting.
b) After Cisco Unified Reporting displays, click **System Reports**.
c) Generate and view the **Cisco Unified CM Database Status** report, which provides debugging information for database replication.
Once you have generated the report, open it and look at the **Cisco Unified CM Database Status**. It gives the RTMT replication counters for all servers in the cluster. All servers should have a replicate state of 2, and all servers should have the same number of replicates created.

If you see any servers whose replicate states are not equal to 2 in the above status check, inspect the "Replication Server List" on this report. It shows which servers are connected and communicating with

each node. Each server should show itself as local (in its list) and the other servers as active connected. If you see any servers as dropped, it usually means there is a communication problem between the nodes.

d) If you want to do so, generate and view the **Cisco Unified CM Database Status** report, which provides a snapshot of the health of the Cisco Unified Communications Manager database.

Step 4 To verify database replication using RTMT, perform the following tasks:

a) Open the Cisco Unified Real-Time Monitoring Tool (RTMT).
b) Click the **CallManager** tab.
c) Click **Database Summary**. The Replication Status pane displays.
The following list shows the possible values for the Replication Status pane:

d) 0—This value indicates that replication has not started. Either no subsequent nodes (subscribers) exist, or the Cisco Database Layer Monitor service is not running and has not been running since the subscriber was installed.
e) 1—This value indicates that replicates have been created, but their count is incorrect.
f) 2—This value indicates that replication is good.
g) 3—This value indicates that replication is bad in the cluster.
h) 4—This value indicates that replication setup did not succeed.
i) To view the Replicate_State performance monitoring counter, choose **System** > **Performance** > **Open Performance Monitoring**. Double-click the publisher database server (first node) to expand the performance monitors. Click **Number of Replicates Created and State of Replication**. Double-click **Replicate_State**. Click **ReplicateCount** from the **Object Instances** window and click **Add**.

Tip To view the definition of the counter, right click the counter name and choose Counter Description.

Step 5 If all the servers have a good RTMT status, but you suspect the databases are not in sync, you can run the CLI command **utils dbreplication status** (If any of the servers showed an RTMT status of 4, proceed to Step 6, on page 45).
This status command can be run on all servers by using **utils dbreplication status all** or on one subscriber by using **utils dbreplication status <hostname>**.

The status report will tell you if any tables are suspect. If there are suspect tables, you will want to do a replication repair CLI command to sync the data from the publisher server to the subscriber servers.

The replication repair can be done on all subscriber servers (using the all parameter) or on just one subscriber server by using the following: `utils dbreplication repair usage:utils dbreplication repair [nodename]|all`.

After running the replication repair, which can take several minutes, you can run another status command to verify that all tables are now in sync. If tables are in sync after running the repair, you are successful in fixing replication.

Note Only do Step 6, on page 45 if one of the servers showed an RTMT status of 4, or had a status of 0 for more than four hours.

Step 6 Generate and view the **Cisco Unified CM Database Status** report, which provides debugging information for database replication. For each subscriber server that has a bad RTMT status, check that the hosts, rhosts, sqlhosts, and services files have the appropriate information.
Generate and view the **Cisco Unified CM Cluster Overview** report. Verify that the subscriber servers have the same version, verify that connectivity is good, and verify that time delay is within tolerances.

If the preceding conditions are acceptable, do the following to reset replication on that subscriber server:

a) At the subscriber server, perform the CLI command **utils dbreplication stop**
b) Do this for all subscriber servers that have an RTMT value of 4

c) At the publisher server, perform the CLI command utils dbreplication stop
d) At the publisher server, perform the CLI command **utils dbreplication reset** <*hostname*> where <*hostname*> is the hostname of the subscriber server that needs to be reset. If all subscriber servers need to be reset, use command **utils dbreplication reset all**

Database Replication Does Not Occur on Lost Node

Database replication does not occur when connectivity is restored on lost node recovery. You can verify the state of replication. Only use the following procedure if you have already tried to reset replication on the node, and have been unsuccessful.

Possible Cause

The CDR check remains stuck in a loop, due to a delete on device table.

1 **Solution** Run **utils dbreplication stop** on the affected subscribers. You can run them all at once.

2 **Solution** Wait until step 1 completes, then run **utils dbreplication stop** on the affected publisher server.

3 **Solution** Run **utils dbreplication clusterreset** from the affected publisher server. When you run the command, the log name gets listed in the log file. Watch this file to monitor the process status. The path is: `/var/log/active/cm/trace/dbl/sdi`

4 **Solution** From the affected publisher, run **utils dbreplication reset all**.

5 **Solution** Stop and restart all the services on all the subscriber servers [or restart/reboot all the systems (subscriber servers)] in the cluster to get the service changes. Do this only after **utils dbreplication status** shows Status 2.

Related Topics

Database Replication Fails Between the Publisher and Subscriber, on page 43

Database Tables Out of Synchronization Do Not Trigger Alert

Out of sync means that two servers in the cluster do not contain the same information in a specific database table.

On Cisco Unified Communications Manager Version 6.x or later, the symptoms include unexpected call processing behaviors. Calls do get not routed or handled as expected. The symptoms may occur on either the publisher or on the subscriber servers.

On Cisco Unified Communications Manager Version 5.x, the symptoms include unexpected call processing behaviors. Calls do not get routed or handled as expected but only when the publisher server is offline. If you

see these symptoms, you can run the **utils dbreplication status** command "Out of sync" displays. If "Out of sync" does not display, this is not the problem.

Possible Cause Database tables remain out of sync between nodes. Replication alerts only indicate failure in the replication process and do not indicate when database tables are out of sync. Normally, if replication is working, tables should remain in sync. Instances can occur in which replication appears to be working, but database tables are "Out of sync".

1 **Solution** Reset cluster replication by using CLI commands. Ensure servers in the cluster are online with full IP connectivity for this to work. Confirm that all servers in the cluster are online by using platform CLI and Cisco Unified Reporting.

2 **Solution** If the servers are in Replication State 2, use the **utils dbreplication repair** *server name* command on the publisher server.

Solution If the servers are not in Replication State 2, use the **utils dbreplication stop** command on all subscriber servers.

Solution Then, use the **utils dbreplication stop** and then **utils dbreplication reset all** commands on the publisher server.

Reset Database Replication When Reverting to Prior Release

If you revert the servers in a cluster to run an older product release, you must manually reset database replication within the cluster. To reset database replication after you revert all the cluster servers to the older product release, use the utils dbreplication reset command all on the publisher server.

When you switch versions by using Cisco Unified Communications Operating System Administration or the CLI, you get a message reminding you about the requirement to reset database replication if you are reverting to an older product release.

Useful Commands and Utilities

This section provides a quick reference for commands and utilities to help you troubleshoot a Cisco Unified Communications Manager server with root access disabled.

The following table provides a summary of the CLI commands and GUI selections that you can use to gather information troubleshoot various system problems.

Table 7: Summary of CLI Commands and GUI Selections

Information	Linux Command	Serviceability GUI Tool	CLI commands
CPU usage	top	RTMT Go to View tab and select **Server** > **CPU and Memory**	Processor CPU usage: show perf query class Processor Process CPU Usage for all processes: show perf query counter Process “% CPU Time” Individual process counter details (including CPU usage) show perf query instance <Process task_name>
Process state	ps	RTMT Go to **View** tab and select **Server** > **Process**	show perf query counter Process “Process Status”
Disk usage	df/du	RTMT Go to **View** tab and select **Server** > **Disk Usage**	show perf query counter Partition“% Used” or show perf query class Partition
Memory	free	RTMT Go to **View** tab and select **Server** > **CPU and Memory**	show perf query class Memory
Network status	netstats		show network status
Reboot server	reboot	Log in to Platform Web page on the server Go to **Restart** > **Current Version**	utils system restart
Collect Traces/logs	Sftp, ftp	RTMT Go to **Tools** tab and select **Trace** > **Trace & Log Central**	List file: file list Download files: file get View a file: file view

Related Documentation

It supplements but does not replace the existing documentation including the following:

- Maintain and operate guides index at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
  - *Cisco Unified Communications Manager Serviceability Administration Guide*
  - *Changing the IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service*

- *Cisco Unified Communications Real-Time Monitoring Tool Administration Guide*
- *Cisco Unified Communications Operating System Administration Guide*
- *Disaster Recovery System Administration Guide*

- Install and upgrade guides index at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html
  - *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*
  - *Upgrading to Cisco Unified Communications Manager*
  - *Installing Cisco Security Agent for Cisco Unified Communications Manager*

For documentation for CDR/CMR, see the following documents:

- For Cisco Unified CM Release 8.0(1)
  http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/8_0_1/cdrdef/cdradmin.html
- For Cisco Unified CM Release 6.1(1)
  http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/6_1_1/car/carexprt.html
- For Cisco Unified CM Release 6.0(1)
  http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/6_0_1/car/carexprt.html
- Cisco Unified CM Release 5.1(3)
  http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/5_1_3/car/carexprt.html
- Cisco Unified CM Release 5.0(4)
  http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/cdr_defs/5_x/cdr504.html

Cisco Unified Communications Manager and IM and Presence Service Managed Services Guide, Release 10.0(1)