CHAPTER 1

Troubleshooting Overview

This section provides the necessary background information and available resources to troubleshoot the *Cisco Unified Communications Manager*.

Cisco Unified Serviceability

Cisco Unified Serviceability, a web-based troubleshooting tool for Unified Communications Manager, provides the following functionality to assist administrators troubleshoot system problems:

- Saves Unified Communications Manager services alarms and events for troubleshooting and provides alarm message definitions.
- Saves Unified Communications Manager services trace information to various log files for troubleshooting. Administrators can configure, collect, and view trace information.
- Monitors real-time behavior of the components in a Unified Communications Manager cluster through the real-time monitoring tool (RTMT).
- Generates reports for Quality of Service, traffic, and billing information through Unified Communications Manager CDR Analysis and Reporting (CAR).
- Provides feature services that you can activate, deactivate, and view through the Service Activation window.
- Provides an interface for starting and stopping feature and network services.
- Archives reports that are associated with Cisco Unified Serviceability tools.
- Allows Unified Communications Manager to work as a managed device for SNMP remote management and troubleshooting.
- Monitors the disk usage of the log partition on a server (or all servers in the cluster).

Access Cisco Unified Serviceability from the Unified Communications Manager Administration window by choosing Cisco Unified Serviceability from the Navigation drop-down list box. Installing the Unified Communications Manager software automatically installs Cisco Unified Serviceability and makes it available.

Refer to the *Cisco Unified Serviceability Administration Guide* for detailed information and configuration procedures on the serviceability tools.

CiscoUnifiedCommunicationsOperatingSystemAdministration

Cisco Unified Communications Operating System Administration allows you to perform the following tasks to configure and manage the Cisco Unified Communications Operating System:

- Check software and hardware status.
- Check and update IP addresses.
- Ping other network devices.
- Manage Network Time Protocol servers.
- Upgrade system software and options.
- Restart the system.

Refer to the *Administration Guide for Cisco Unified Communications Manager* for detailed information and configuration procedures on the serviceability tools.

General Model of Problem Solving

When troubleshooting a telephony or IP network environment, define the specific symptoms, identify all potential problems that could be causing the symptoms, and then systematically eliminate each potential problem (from most likely to least likely) until the symptoms disappear.

The following steps provide guidelines to use in the problem-solving process.

Procedure

1. Analyze the network problem and create a clear problem statement. Define symptoms and potential causes.
2. Gather the facts that you need to help isolate possible causes.
3. Consider possible causes based on the facts that you gathered.
4. Create an action plan based on those causes. Begin with the most likely problem and devise a plan in which you manipulate only one variable.
5. Implement the action plan; perform each step carefully while testing to see whether the symptom disappears.
6. Analyze the results to determine whether the problem has been resolved. If the problem was resolved, consider the process complete.
7. If the problem has not been resolved, create an action plan based on the next most probable cause on your list. Return to 4, on page 2 and repeat the process until the problem is solved.

Make sure that you undo anything that you changed while implementing your action plan. Remember that you want to change only one variable at a time.

Note If you exhaust all the common causes and actions (either those outlined in this document or others that you have identified in your environment), contact Cisco TAC.

Network Failure Preparation

You can always recover more easily from a network failure if you are prepared ahead of time. To determine if you are prepared for a network failure, answer the following questions:

- Do you have an accurate physical and logical map of your internetwork that outlines the physical location of all of the devices on the network and how they are connected as well as a logical map of network addresses, network numbers, and subnetworks?
- Do you have a list of all network protocols that are implemented in your network for each of the protocols implemented and a list of the network numbers, subnetworks, zones, and areas that are associated with them?
- Do you know which protocols are being routed and the correct, up-to-date configuration information for each protocol?
- Do you know which protocols are being bridged? Are any filters configured in any of these bridges, and do you have a copy of these configurations? Is this applicable to Unified Communications Manager?
- Do you know all the points of contact to external networks, including any connections to the Internet? For each external network connection, do you know what routing protocol is being used?
- Has your organization documented normal network behavior and performance, so you can compare current problems with a baseline?

If you can answer yes to these questions, faster recovery from a failure results.

Where to Find More Information

Use the following links for information on various IP telephony topics:

- For further information about related Cisco IP telephony applications and products, refer to the *Cisco Unified Communications Manager Documentation Guide*. The following URL shows an example of the path to the documentation guide:

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html
- For documentation related to Cisco Unity, refer to the following URL:
  http://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html
- For documentation related to Cisco Emergency Responder, refer to the following URL:
- http://www.cisco.com/en/US/products/sw/voicesw/ps842/tsd_products_support_series_home.html
- For documentation related to Cisco Unified IP Phones, refer to the following URL:

- http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html
- For information on designing and troubleshooting IP telephony networks, refer to the Cisco IP Telephony Solution Reference Network Design Guides that are available at www.cisco.com/go/srnd.

CHAPTER 2

Troubleshooting Tools

This section addresses the tools and utilities that you use to configure, monitor, and troubleshootUnified Communications Manager and provides general guidelines for collecting information to avoid repetitive testing and recollection of identical data.

Note To access some of the URL sites that are listed in this document, you must be a registered user, and you must be logged in.

Cisco Unified Serviceability Troubleshooting Tools

Refer to the *Cisco Unified Serviceability Administration Guide* for detailed information of the following different types of tools that Cisco Unified Serviceability provides to monitor and analyze the various Unified Communications Manager systems.

Table 2: Serviceability Tools

Term	Definition
Cisco Unified Real-Time Monitoring Tool (RTMT)	This tool provides real-time information about Unified Communications Manager devices and performance counters and enables you to collect traces. Performance counters can be system-specific or Unified Communications Manager specific. Objects comprise the logical groupings of like counters for a specific device or feature, such as Cisco Unified IP Phones or Unified Communications Manager System Performance. Counters measure various aspects of system performance. Counters measure statistics such as the number of registered phones, calls that are attempted and calls in progress.
Alarms	Administrators use alarms to obtain run-time status and state of the Unified Communications Manager system. Alarms contain information about system problems such as explanation and recommended action. Administrators search the alarm definitions database for alarm information. The alarm definition contains a description of the alarm and recommended actions.
Trace	Administrators and Cisco engineers use trace files to obtain specific information about Unified Communications Manager service problems. Cisco Unified Serviceability sends configured trace information to the trace log file. Two types of trace log files exist: SDI and SDL. Every service includes a default trace log file. The system traces system diagnostic interface (SDI) information from the services and logs run-time events and traces to a log file. The SDL trace log file contains call-processing information from services such as Cisco CallManager and Cisco CTIManager. The system traces the signal distribution layer (SDL) of the call and logs state transitions into a log file. **Note** In most cases, you will only gather SDL traces when Cisco Technical Assistance Center (TAC) requests you to do so.
Quality Report Tool	This term designates voice quality and general problem-reporting utility in Cisco Unified Serviceability.

Term	Definition
Serviceability Connector	This offering increases the speed with which Cisco technical assistance staff can diagnose issues with your infrastructure. It automates the tasks of finding, retrieving and storing diagnostic logs and information into an SR case, and triggering analysis against diagnostic signatures so that TAC can more efficiently identify and resolve issues with your on-premises equipment.

Command Line Interface

Use the command line interface (CLI) to access the Unified Communications Manager system for basic maintenance and failure recovery. Obtain access to the system by either a hard-wired terminal (a system monitor and keyboard) or by performing a SSH session.

The account name and password get created at install time. You can change the password after install, but you never can change the account name.

A command represents a text instruction that caused the system to perform some function. Commands may be stand alone, or they can have mandatory or optional arguments or options.

A level comprises a collection of commands; for example, show designates a level, whereas show status specifies a command. Each level and command also includes an associated privilege level. You can execute a command only if you have sufficient privilege level.

For complete information on the Unified Communications Manager CLI command set, see the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

kerneldump Utility

The kerneldump utility allows you to collect crash dump logs locally on the affected machine without requiring a secondary server.

In a Unified Communications Manager cluster, you only need to ensure the kerneldump utility is enabled on the server before you can collect the crash dump information.

Note Cisco recommends that you verify the kerneldump utility is enabled after you install Unified Communications Manager to allow for more efficient troubleshooting. If you have not already done so, enable the kerneldump utility before you upgrade the Unified Communications Manager from supported appliance releases.

Important Enabling or disabling the kerneldump utility will require a reboot of the node. Do not execute the enable command unless you are within a window where a reboot would be acceptable.

The command line interface (CLI) for the Cisco Unified Communications Operating System can be used to enable, disable, or check the status of the kerneldump utility.

Use the following procedure to enable the kernel dump utility:

Working with Files That Are Collected by the Utility

To view the crash information from the kerneldump utility, use the Cisco Unified Real-Time Monitoring Tool or the command line interface (CLI). To collect the kerneldump logs by using the Cisco Unified Real-Time Monitoring Tool, choose the Collect Files option from Trace & Log Central. From the Select System Services/Applications tab, choose the Kerneldump logs check box. For more information on collecting files using Cisco Unified Real-Time Monitoring Tool, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

To use the CLI to collect the kerneldump logs, use the "file" CLI commands on the files in the crash directory. These are found under the "activelog" partition. The log filenames begin with the IP address of the kerneldump client and end with the date that the file is created. For more information on the file commands, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Enable the Kerneldump Utility

Use this procedure to enable the kerneldump utility. In the event of a kernel crash, the utility provides a mechanism for collecting and dumping the crash. You can configure the utility to dump logs to the local server or to an external server.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Complete either of the following:

- To dump kernel crashes on the local server, run the `utils os kernelcrash enable` CLI command.
- To dump kernel crashes to an external server, run the `utils os kerneldump ssh enable <ip_address>` CLI command with the IP address of the external server.

Step 3 Reboot the server.

Example

Note If you need to disable the kerneldump utility, you can run the `utils os kernelcrash disable` CLI command to disable the local server for core dumps and the `utils os kerneldump ssh disable <ip_address>` CLI command to disable the utility on the external server.

What to do next

Configure an email alert in the Real-Time Monitoring Tool to be advised of core dumps. For details, see Enable Email Alert for Core Dump, on page 9

Refer to the *Troubleshooting Guide for Cisco Unified Communications Manager* for more information on the kerneldump utility and troubleshooting.

Enable Email Alert for Core Dump

Use this procedure to configure the Real-Time Monitoring Tool to email the administrator whenever a core dump occurs.

Procedure

Step 1 Select **System** > **Tools** > **Alert** > **Alert Central**.

Step 2 Right-click **CoreDumpFileFound** alert and select **Set Alert Properties**.

Step 3 Follow the wizard prompts to set your preferred criteria:

a) In the **Alert Properties: Email Notification** popup, make sure that **Enable Email** is checked and click **Configure** to set the default alert action, which will be to email an administrator.

b) Follow the prompts and **Add** a Receipient email address. When this alert is triggered, the default action will be to email this address.

c) Click **Save**.

Step 4 Set the default Email server:

a) Select **System** > **Tools** > **Alert** > **Config Email Server**.

b) Enter the e-mail server settings.

c) Click **OK**.

Network Management

Use the network management tools for Unified Communications Manager remote serviceability.

- System Log Management
- Cisco Discovery Protocol Support
- Simple Network Management Protocol support

Refer to the documentation at the URLs provided in the sections for these network management tools for more information.

System Log Management

Although it can be adapted to other network management systems, Cisco Syslog Analysis, which is packaged with Resource Manager Essentials (RME), provides the best method to manage Syslog messages from Cisco devices.

Cisco Syslog Analyzer serves as the component of Cisco Syslog Analysis that provides common storage and analysis of the system log for multiple applications. The other major component, Syslog Analyzer Collector, gathers log messages from Unified Communications Manager servers.

These two Cisco applications work together to provide a centralized system logging service for Cisco Unified Communications Solutions.

Refer to the following URL for RME documentation:

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml

Cisco Discovery Protocol Support

The Cisco Discovery Protocol Support enables discovery of Unified Communications Manager servers and management of those servers.

Refer to the following URL for RME documentation:

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml

Simple Network Management Protocol Support

Network management systems (NMS) use SNMP, an industry-standard interface, to exchange management information between network devices. A part of the TCP/IP protocol suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth.

An SNMP-managed network comprises three key components: managed devices, agents, and network management systems.

- A managed device designates a network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make it available by using SNMP.
- An agent, as network management software, resides on a managed device. An agent contains local knowledge of management information and translates it into a form that is compatible with SNMP.
- A network management system comprises an SNMP management application together with the computer on which it runs. An NMS executes applications that monitor and control managed devices. An NMS provides the bulk of the processing and memory resources that are required for network management. The following NMSs share compatibility with Unified Communications Manager:
  - CiscoWorks Common Services Software
  - HP OpenView
  - Third-party applications that support SNMP and Unified Communications Manager SNMP interfaces

Sniffer Traces

Typically, you collect sniffer traces by connecting a laptop or other sniffer-equipped device on a Catalyst port that is configured to span the VLAN or port(s) (CatOS, Cat6K-IOS, XL-IOS) that contains the trouble information. If no free port is available, connect the sniffer-equipped device on a hub that is inserted between the switch and the device.

Tip To help facilitate reading and interpreting of the traces by the TAC engineer, Cisco recommends using Sniffer Pro software because it is widely used within the TAC.

Have available the IP/MAC addresses of all equipment that is involved, such as IP phones, gateways, Unified Communications Managers, and so on.

Debugs

The output from **debug** privileged EXEC commands provides diagnostic information about a variety of internetworking event that relate to protocol status and network activity in general.

Set up your terminal emulator software (such as HyperTerminal), so it can capture the debug output to a file. In HyperTerminal, click **Transfer**; then, click **Capture Text** and choose the appropriate options.

Before running any IOS voice gateway debugs, make sure that **`service timestamps debug datetime msec`** is globally configured on the gateway.

Note Avoid collecting debugs in a live environment during operation hours.

Preferably, collect debugs during non-working hours. If you must collect debugs in a live environment, configure **`no logging console`** and **`logging buffered`**. To collect the debugs, use **`show log`**.

Because some debugs can be lengthy, collect them directly on the console port (default **`logging console`**) or on the buffer (**`logging buffer`**). Collecting debugs over a Telnet session may impact the device performance, and the result could be incomplete debugs, which requires that you re-collect them.

To stop a debug, use the **`no debug all`** or **`undebug all`** commands. Verify that the debugs have been turned off by using the command **`show debug`**.

Cisco Secure Telnet

Cisco Secure Telnet allows Cisco Service Engineers (CSE) transparent firewall access to theUnified Communications Manager node on your site. Using strong encryption, Cisco Secure Telnet enables a special Telnet client from Cisco Systems to connect to a Telnet daemon behind your firewall. This secure connection allows remote monitoring and troubleshooting of your Unified Communications Manager nodes, without requiring firewall modifications.

Note Cisco provides this service only with your permission. You must ensure that a network administrator is available at your site to help initiate the process.

Packet Capture

This section contains information about packet capture.

Related Topics

Packet Capturing Overview, on page 12
Configuration Checklist for Packet Capturing, on page 12
Adding an End User to the Standard Packet Sniffer Access Control Group , on page 13
Configuring Packet-Capturing Service Parameters, on page 13
Configuring Packet Capturing in the Phone Configuration Window, on page 14
Configuring Packet Capturing in Gateway and Trunk Configuration Windows, on page 15
Packet-Capturing Configuration Settings, on page 16
Analyzing Captured Packets, on page 18

Packet Capturing Overview

Because third-party troubleshooting tools that sniff media and TCP packets do not work after you enable encryption, you must use Unified Communications Manager to perform the following tasks if a problem occurs:

- Analyze packets for messages that are exchanged between Unified Communications Manager and the device [Cisco Unified IP Phone (SIP and SCCP), Cisco IOS MGCP gateway, H.323 gateway, H.323/H.245/H.225 trunk, or SIP trunk].
- Capture the Secure Real Time Protocol (SRTP) packets between the devices.
- Extract the media encryption key material from messages and decrypt the media between the devices.

Tip Performing this task for several devices at the same time may cause high CPU usage and call-processing interruptions. Cisco strongly recommends that you perform this task when you can minimize call-processing interruptions.

For more information, see the *Cisco Unified Communications Manager Security Guide*.

Configuration Checklist for Packet Capturing

Extracting and analyzing pertinent data includes performing the following tasks.

Procedure

1. Add end users to the Standard Packet Sniffer Users group.
2. Configure packet capturing service parameters in the Service Parameter Configuration window in Unified Communications Manager Administration; for example, configure the Packet Capture Enable service parameter.
3. Configure packet capturing settings on a per-device basis in the Phone or Gateway or Trunk Configuration window.

Note Cisco strongly recommends that you do not enable packet capturing for many devices at the same time because this task may cause high CPU usage in your network.

4. Capture SRTP packets by using a sniffer trace between the affected devices. Refer to the documentation that supports your sniffer trace tool.
5. After you capture the packets, set the Packet Capture Enable service parameter to False.
6. Gather the files that you need to analyze the packets.
7. Cisco Technical Assistance Center (TAC) analyzes the packets. Contact TAC directly to perform this task.

Related Topics

Adding an End User to the Standard Packet Sniffer Access Control Group , on page 13
Analyzing Captured Packets, on page 18
Configuring Packet Capturing in Gateway and Trunk Configuration Windows, on page 15
Configuring Packet Capturing in the Phone Configuration Window, on page 14
Configuring Packet-Capturing Service Parameters, on page 13
Packet-Capturing Configuration Settings, on page 16

Adding an End User to the Standard Packet Sniffer Access Control Group

End users that belong to the Standard Packet Sniffer Users group can configure the Packet Capture Mode and Packet Capture Duration settings for devices that support packet capturing. If the user does not exist in the Standard Packet Sniffer Access Control Group, the user cannot initiate packet capturing.

The following procedure, which describes how to add an end user to the Standard Packet Sniffer Access Control Group, assumes that you configured the end user in Unified Communications Manager Administration, as described in the *Administration Guide for Cisco Unified Communications Manager* .

Procedure

1. Find the access control group, as described in the *Administration Guide for Cisco Unified Communications Manager*.
2. After the Find/List window displays, click the **Standard Packet Sniffer Users** link.
3. Click the **Add Users to Group** button.
4. Add the end user, as described in the *Administration Guide for Cisco Unified Communications Manager*.
5. After you add the user, click **Save**.

Configuring Packet-Capturing Service Parameters

To configure parameters for packet capturing, perform the following procedure:

Procedure

1. In Unified Communications Manager Administration, choose **System** > **Service Parameters**.
2. From the Server drop-down list box, choose an Active server where you activated the Cisco CallManager service.
3. From the Service drop-down list box, choose the **Cisco CallManager (Active)** service.

4. Scroll to the TLS Packet Capturing Configuration pane and configure the packet capturing settings.

Tip For information on the service parameters, click the name of the parameter or the question mark that displays in the window.

Note For packet capturing to occur, you must set the Packet Capture Enable service parameter to True.

5. For the changes to take effect, click **Save**.
6. You can continue to configure packet-capturing.

Related Topics

Configuring Packet Capturing in Gateway and Trunk Configuration Windows, on page 15
Configuring Packet Capturing in the Phone Configuration Window, on page 14

Configuring Packet Capturing in the Phone Configuration Window

After you enable packet capturing in the Service Parameter window, you can configure packet capturing on a per-device basis in the Phone Configuration window of Unified Communications Manager Administration.

You enable or disable packet capturing on a per-phone basis. The default setting for packet capturing equals None.

Caution Cisco strongly recommends that you do not enable packet capturing for many phones at the same time because this task may cause high CPU usage in your network.

If you do not want to capture packets or if you completed the task, set the Packet Capture Enable service parameter to False.

To configure packet capturing for phones, perform the following procedure:

Procedure

1. Before you configure the packet-capturing settings, see the topics related to packet capturing configuration.
2. Find the SIP or SCCP phone, as described in the *System Configuration Guide for Cisco Unified Communications Manager* .
3. After the Phone Configuration window displays, configure the troubleshooting settings, as described in Packet-Capturing Configuration Settings.
4. After you complete the configuration, click **Save**.
5. In the Reset dialog box, click **OK**.

Tip Although Unified Communications Manager Administration prompts you to reset the device, you do not need to reset the device to capture packets.

Additional Steps

Capture SRTP packets by using a sniffer trace between the affected devices.

After you capture the packets, set the Packet Capture Enable service parameter to False.

Related Topics

Analyzing Captured Packets, on page 18
Configuration Checklist for Packet Capturing, on page 12

Configuring Packet Capturing in Gateway and Trunk Configuration Windows

The following gateways and trunks support packet capturing in Unified Communications Manager Administration.

- Cisco IOS MGCP gateways
- H.323 gateways
- H.323/H.245/H.225 trunks
- SIP trunks

Tip Cisco strongly recommends that you do not enable packet capturing for many devices at the same time because this task may cause high CPU usage in your network.

If you do not want to capture packets or if you completed the task, set the Packet Capture Enable service parameter to False.

To configure packet-capturing settings in the Gateway or Trunk Configuration window, perform the following procedure:

Procedure

1. Before you configure the packet-capturing settings, see the topics related to packet capturing configuration.
2. Perform one of the following tasks:
   - Find the Cisco IOS MGCP gateway, as described in the *System Configuration Guide for Cisco Unified Communications Manager* .
   - Find the H.323 gateway, as described in the *System Configuration Guide for Cisco Unified Communications Manager* .
   - Find the H.323/H.245/H.225 trunk, as described in the *System Configuration Guide for Cisco Unified Communications Manager* .
   - Find the SIP trunk, as described in the *System Configuration Guide for Cisco Unified Communications Manager* .

3. After the configuration window displays, locate the Packet Capture Mode and Packet Capture Duration settings.

Tip If you located a Cisco IOS MGCP gateway, ensure that you configured the ports for the Cisco IOS MGCP gateway, as described in the *Administration Guide for Cisco Unified Communications Manager* . The packet-capturing settings for the Cisco IOS MGCP gateway display in the Gateway Configuration window for endpoint identifiers. To access this window, click the endpoint identifier for the voice interface card.

4. Configure the troubleshooting settings, as described in Packet-Capturing Configuration Settings.
5. After you configure the packet-capturing settings, click **Save**.
6. In the Reset dialog box, click **OK**.

Tip Although Unified Communications Manager Administration prompts you to reset the device, you do not need to reset the device to capture packets.

Additional Steps

Capture SRTP packets by using a sniffer trace between the affected devices.

After you capture the packets, set the Packet Capture Enable service parameter to False.

Related Topics

Analyzing Captured Packets, on page 18
Configuration Checklist for Packet Capturing, on page 12

Packet-Capturing Configuration Settings

The following table describes the Packet Capture Mode and Packet Capture Duration settings when configuring packet capturing for gateways, trunks, and phones.

Setting	Description
Packet Capture Mode	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. Choose one of the following options from the drop-down list box: • **None**—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, Unified Communications Manager sets the Packet Capture Mode to None. • **Batch Processing Mode**— Unified Communications Manager writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Unified Communications Manager, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Unified Communications Manager stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file. **Tip** Before you contact TAC, you must capture the SRTP packets by using a sniffer trace between the affected devices.
Packet Capture Duration	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays.

Related Topics

Configuring Packet Capturing in Gateway and Trunk Configuration Windows, on page 15
Configuring Packet Capturing in the Phone Configuration Window, on page 14

Analyzing Captured Packets

Cisco Technical Assistance Center (TAC) analyzes the packets by using a debugging tool. Before you contact TAC, capture SRTP packets by using a sniffer trace between the affected devices. Contact TAC directly after you gather the following information:

- Packet Capture File—**https://<IP address or server name>/pktCap/pktCap.jsp?file=mm-dd-yyyy.pkt**, where you browse into the server and locate the packet-capture file by month, date, and year (mm-dd-yyyy)
- Key for the file—**https://<IP address or server name>/pktCap/pktCap.jsp?key=mm-dd-yyyy.pkt**, where you browse into the server and locate the key by month, date, and year (mm-dd-yyyy)
- User name and password of end user that belongs to the Standard Packet Sniffer Users group

For more information, see the *Cisco Unified Communications Manager Security Guide*.

Common Troubleshooting Tasks, Tools, and Commands

This section provides a quick reference for commands and utilities to help you troubleshoot a 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 3: 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

Information	Linux Command	Serviceability GUI Tool	CLI commands
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 **Server** > **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

The following table provides a list of common problems and tools to use to troubleshoot them.

Table 4: Troubleshooting Common Problems with CLI Commands and GUI Selections

Task	GUI Tool	CLI commands
Accessing the database	none	Log in as admin and use any of the following **show** commands: • show tech database • show tech dbinuse • show tech dbschema • show tech devdefaults • show tech gateway • show tech locales • show tech notify • show tech procedures • show tech routepatterns • show tech routeplan • show tech systables • show tech table • show tech triggers • show tech version • show tech params* To run a SQL command, use the **run** command: • run sql <sql command>

Task	GUI Tool	CLI commands
Freeing up disk space **Note** You can only delete files from the Log partition.	Using the RTMT client application, go to the **Tools** tab and select **Trace & Log Central** > **Collect Files**. Choose the criteria to select the files you want to collect, then check the option **Delete Files**. This will delete the files on the Unified Communications Manager server after downloading the files to your PC.	file delete
Viewing core files	You cannot view the core files; however, you can download the Core files by using the RTMT application and selecting **Trace & Log Central** > **Collect Crash Dump**.	utils core [options.]
Rebooting the Unified Communications Manager server	Log in to Platform on the server and go to **Restart** > **Current Version**.	utils system restart
Changing debug levels for traces	Log in to Cisco Unity Connection Serviceability Administration at `https://<server_ipaddress>:8443/ccmservice/` and choose **Trace > Configuration**.	set trace enable [Detailed, Significant, Error, Arbitrary, Entry_exit, State_Transition, Special] [syslogmib, cdpmib, dbl, dbnotify]
Looking at netstats	none	show network status

Troubleshooting Tips

The following tips may help you when you are troubleshooting the Unified Communications Manager.

Tip Check the release notes for Unified Communications Manager for known problems. The release notes provide descriptions and workaround solutions for known problems.

Tip Know where your devices are registered.

Each Unified Communications Manager log traces files locally. If a phone or gateway is registered to a particular Unified Communications Manager, the call processing gets done on thatUnified Communications Manager if the call is initiated there. You will need to capture traces on that Unified Communications Manager to debug a problem.

A common mistake involves having devices that are registered on a subscriber server but are capturing traces on the publisher server. These trace files will be nearly empty (and definitely will not have the call in them).

Another common problem involves having Device 1 registered to CM1 and Device 2 registered to CM2. If Device 1 calls Device 2, the call trace occurs in CM1, and, if Device 2 calls Device 1, the trace occurs in CM2. If you are troubleshooting a two-way calling issue, you need both traces from both Unified Communications Managers to obtain all the information that is needed to troubleshoot.

Tip Know the approximate time of the problem.

Multiple calls may have occurred, so knowing the approximate time of the call helps TAC quickly locate the trouble.

You can obtain phone statistics on a Cisco Unified IP Phone 79xx by pressing the **i** or **?** button twice during an active call.

When you are running a test to reproduce the issue and produce information, know the following data that is crucial to understanding the issue:

- Calling number/called number
- Any other number that is involved in the specific scenario
- Time of the call

Note Remember that time synchronization of all equipment is important for troubleshooting.

If you are reproducing a problem, make sure to choose the file for the timeframe by looking at the modification date and the time stamps in the file. The best way to collect the right trace means that you reproduce a problem and then quickly locate the most recent file and copy it from the Unified Communications Manager server.

Tip Save the log files to prevent them from being overwritten.

Files will get overwritten after some time. The only way to know which file is being logged to is to choose **View** > **Refresh** on the menu bar and look at the dates and times on the files.

System History Log

This system history log provides a central location for getting a quick overview of the initial system install, system upgrades, Cisco option installations, and DRS backups and DRS restores, as well as switch version and reboot history.

Related Topics

System History Log Overview, on page 22
System History Log Fields, on page 22
Accessing the System History Log, on page 23

System History Log Overview

The system history log exists as a simple ASCII file, **system-history.log**, and the data does not get maintained in the database. Because it does not get excessively large, the system history file does not get rotated.

The system history log provides the following functions:

- Logs the initial software installation on a server.
- Logs the success, failure, or cancellation of every software upgrade (Cisco option files and patches).
- Logs every DRS backup and restore that is performed.
- Logs every invocation of Switch Version that is issued through either the CLI or the GUI.
- Logs every invocation of Restart and Shutdown that is issued through either the CLI or the GUI.
- Logs every boot of the system. If not correlated with a restart or shutdown entry, the boot is the result of a manual reboot, power cycle, or kernel panic.
- Maintains a single file that contains the system history, since initial installation or since feature availability.
- Exists in the install folder. You can access the log from the CLI by using the **file** commands or from the Real Time Monitoring Tool (RTMT).

System History Log Fields

The log displays a common header that contains information about the product name, product version, and kernel image; for example:

```
======================================

Product Name - Cisco Unified Communications Manager

Product Version - 7.1.0.39000-9023

Kernel Image - 2.6.9-67.EL

======================================
```

Each system history log entry contains the following fields:

timestamp userid action description start/result

The system history log fields can contain the following values:

- *timestamp*—Displays the local time and date on the server with the format *mm/dd/yyyy hh:mm:ss*.
- *userid*—Displays the user name of the user who invokes the action.
- *action*—Displays one of the following actions:
  - Install
  - Windows Upgrade
  - Upgrade During Install
  - Upgrade
  - Cisco Option Install

- Switch Version
- System Restart
- Shutdown
- Boot
- DRS Backup
- DRS Restore

- *description*—Displays one of the following messages:
  - *Version*: Displays for the Basic Install, Windows Upgrade, Upgrade During Install, and Upgrade actions.
  - *Cisco Option file name*: Displays for the Cisco Option Install action.
  - *Timestamp*: Displays for the DRS Backup and DRS Restore actions.
  - *Active version to inactive version*: Displays for the Switch Version action.
  - *Active version*: Displays for the System Restart, Shutdown, and Boot actions.
- *result*—Displays the following results:
  - Start
  - Success or Failure
  - Cancel

The following shows a sample of the system history log.

```
admin:file dump install system-history.log=======================================
Product Name -    Cisco Unified Communications Manager
Product Version - 6.1.2.9901-117
Kernel Image -    2.4.21-47.EL.cs.3BOOT
=======================================
07/25/2008 14:20:06 | root: Install 6.1.2.9901-117 Start
07/25/2008 15:05:37 | root: Install 6.1.2.9901-117 Success
07/25/2008 15:05:38 | root: Boot 6.1.2.9901-117 Start
07/30/2008 10:08:56 | root: Upgrade 6.1.2.9901-126 Start
07/30/2008 10:46:31 | root: Upgrade 6.1.2.9901-126 Success
07/30/2008 10:46:43 | root: Switch Version 6.1.2.9901-117 to 6.1.2.9901-126 Start

07/30/2008 10:48:39 | root: Switch Version 6.1.2.9901-117 to 6.1.2.9901-126 Success

07/30/2008 10:48:39 | root: Restart 6.1.2.9901-126 Start
07/30/2008 10:51:27 | root: Boot 6.1.2.9901-126 Start
08/01/2008 16:29:31 | root: Restart 6.1.2.9901-126 Start
08/01/2008 16:32:31 | root: Boot 6.1.2.9901-126 Start
```

Accessing the System History Log

You can use either the CLI or RTMT to access the system history log.

Using the CLI

You can access the system history log by using the CLI **file** command; for example:

- **file view install system-history.log**
- **file get install system-history.log**

For more information on the CLI **file** commands, see the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Using RTMT

You can also access the system history log by using RTMT. From the Trace and Log Central tab, choose **Collect Install Logs**.

For more information about using RTMT, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Audit Logging

Centralized audit logging ensures that configuration changes to the Unified Communications Manager system gets logged in separate log files for auditing. An audit event represents any event that is required to be logged. The following Unified Communications Manager components generate audit events:

- Unified Communications Manager Administration
- Cisco Unified Serviceability
- Unified Communications Manager CDR Analysis and Reporting
- Cisco Unified Real-Time Monitoring Tool
- Cisco Unified Communications Operating System
- Disaster Recovery System
- Database
- Command Line Interface
- Remote Support Account Enabled (CLI commands issued by technical supports teams)

In Cisco Business Edition 5000, the following Cisco Unity Connection components also generate audit events:

- Cisco Unity Connection Administration
- Cisco Personal Communications Assistant (Cisco PCA)
- Cisco Unity Connection Serviceability
- Cisco Unity Connection clients that use the Representational State Transfer (REST) APIs

The following example displays a sample audit event:

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
```

```
EventType:ServiceStatusUpdated ResourceAccessed: CCMService EventStatus:Successful
 Description: Call Manager Service status is stopped App ID:Cisco Tomcat Cluster
 ID:StandAloneCluster Node ID:sa-cm1-3
```

Audit logs, which contain information about audit events, get written in the common partition. The Log Partition Monitor (LPM) manages the purging of these audit logs as needed, similar to trace files. By default, the LPM purges the audit logs, but the audit user can change this setting from the Audit User Configuration window in Cisco Unified Serviceability. The LPM sends an alert whenever the common partition disk usage exceeds the threshold; however, the alert does not have the information about whether the disk is full because of audit logs or trace files.

Tip The Cisco Audit Event Service, which is a network service that supports audit logging, displays in Control Center—Network Services in Cisco Unified Serviceability. If audit logs do not get written, then stop and start this service by choosing **Tools** > **Control Center—Network Services** in Cisco Unified Serviceability.

All audit logs get collected, viewed and deleted from Trace and Log Central in the Cisco Unified Real-Time Monitoring Tool. Access the audit logs in RTMT in Trace and Log Central. Go to **System** > **Real-Time Trace** > **Audit Logs** > **Nodes**. After you select the node, another window displays **System** > **Cisco Audit Logs**.

The following types of audit logs display in RTMT:

- Application log
- Database log
- Operating system log
- Remote SupportAccEnabled log

Application Log

The application audit log, which displays in the AuditApp folder in RTMT, provides configuration changes for Unified Communications Manager Administration, Cisco Unified Serviceability, the CLI, Cisco Unified Real-Time Monitoring Tool (RTMT), Disaster Recovery System, and Cisco Unified CDR Analysis and Reporting (CAR). For Cisco Business Edition 5000, the application audit log also logs changes for Cisco Unity Connection Administration, Cisco Personal Communications Assistant (Cisco PCA), Cisco Unity Connection Serviceability, and clients that use the Representational State Transfer (REST) APIs.

Although the Application Log stays enabled by default, you can configure it in Cisco Unified Serviceability by choosing **Tools** > **Audit Log Configuration**. For a description of the settings that you can configure for audit log configuration, refer to the *Cisco Unified Serviceability Administration Guide*.

If the audit logs get disabled in Cisco Unified Serviceability, no new audit log files get created.

Tip Only a user with an audit role has permission to change the Audit Log settings. By default, the CCMAdministrator has the audit role after fresh installs and upgrades. The CCMAdministrator can assign the "standard audit users" group to a new user that the CCMAdministrator specifically creates for audit purposes. The CCMAdministrator can then be removed from the audit user group. The "standard audit log configuration" role provides the ability to delete audit logs, read/update access to Cisco Unified Real-Time Monitoring Tool, Trace Collection Tool, RTMT Alert Configuration, the Control Center - Network Services window, RTMT Profile Saving, the Audit Configuration window, and a new resource called Audit Traces. For Cisco Unity Connection in Cisco Business Edition 5000, the application administration account that was created during installation has the Audit Administrator role and can assign other administrative users to the role.

Unified Communications Manager creates one application audit log file until the configured maximum file size is reached; then, it closes and creates a new application audit log file. If the system specifies rotating the log files, Unified Communications Manager saves the configured number of files. Some of the logging events can be viewed by using RTMT SyslogViewer.

The following events get logged for Unified Communications Manager Administration:

- User logging (user logins and user logouts).
- User role membership updates (user added, user deleted, user role updated).
- Role updates (new roles added, deleted, or updated).
- Device updates (phones and gateways).
- Server configuration updates (changes to alarm or trace configurations, service parameters, enterprise parameters, IP addresses, host names, Ethernet settings, and Unified Communications Manager server additions or deletions).

The following events get logged for Cisco Unified Serviceability:

- Activation, deactivation, start, or stop of a service from any Serviceability window.
- Changes in trace configurations and alarm configurations.
- Changes in SNMP configurations.
- Changes in CDR Management.
- Review of any report in the Serviceability Reports Archive. View this log on the reporter node.

RTMT logs the following events with an audit event alarm:

- Alert configuration.
- Alert suspension.
- E-mail configuration.
- Set node alert status.
- Alert addition.
- Add alert action.

- Clear alert.
- Enable alert.
- Remove alert action.
- Remove alert.

The following events get logged for Unified Communications Manager CDR Analysis and Reporting:

- Scheduling the CDR Loader.
- Scheduling the daily, weekly, and monthly user reports, system reports, and device reports.
- Mail parameters configurations.
- Dial plan configurations.
- Gateway configurations.
- System preferences configurations.
- Autopurge configurations.
- Rating engine configurations for duration, time of day, and voice quality.
- QoS configurations.
- Automatic generation/alert of pregenerated reports configurations.
- Notification limits configurations.

The following events gets logged for Disaster Recovery System:

- Backup initiated successfully/failed
- Restore initiated successfully/failed
- Backup cancelled successfully
- Backup completed successfully/failed
- Restore completed successfully/failed
- Save/update/delete/enable/disable of backup schedule
- Save/update/delete of destination device for backup

For Cisco Business Edition 5000, Cisco Unity Connection Administration logs the following events:

- User logging (user logins and user logouts).
- All configuration changes, including but not limited to users, contacts, call management objects, networking, system settings, and telephony.
- Task management (enabling or disabling a task).
- Bulk Administration Tool (bulk creates, bulk deletes).
- Custom Keypad Map (map updates)

For Cisco Business Edition 5000, Cisco PCA logs the following events:

- User logging (user logins and user logouts).
- All configuration changes made via the Messaging Assistant.

For Cisco Business Edition 5000, Cisco Unity Connection Serviceability logs the following events:

- User logging (user logins and user logouts).
- All configuration changes.
- Activating, deactivating, starting or stopping services.

For Cisco Business Edition 5000, clients that use the REST APIs log the following events:

- User logging (user API authentication).
- API calls that utilize Cisco Unity Connection Provisioning Interface (CUPI).

Database Log

The database audit log, which displays in the informix folder in RTMT, reports database changes. This log, which is not enabled by default, gets configured in Cisco Unified Serviceability by choosing **Tools** > **Audit Log Configuration**. For a description of the settings that you can configure for audit log configuration, refer to the *Cisco Unified Serviceability Administration Guide*.

This audit differs from the Application audit because it logs database changes, and the Application audit logs application configuration changes. The informix folder does not display in RTMT unless database auditing is enabled in Cisco Unified Serviceability.

Operating System Log

The operating system audit log, which displays in the vos folder in RTMT, reports events that are triggered by the operating system. It does not get enabled by default. The **utils auditd** CLI command enables, disables, or gives status about the events.

The vos folder does not display in RTMT unless the audit is enabled in the CLI.

For information on the CLI, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Remote Support Acct Enabled Log

The Remote Support Acct Enabled audit log, which displays in the vos folder in RTMT, reports CLI commands that get issued by technical support teams. You cannot configure it, and the log gets created only if the Remote Support Acct gets enabled by the technical support team.

Verify Cisco Unified Communications Manager Services Are Running

Use the following procedure to verify which Cisco CallManager services are active on a server.

Procedure

1. From Unified Communications Manager Administration, choose **Navigation** > **Cisco Unified Serviceability**.
2. Choose **Tools** > **Service Activation**.
3. From the Servers column, choose the desired server.

   The server that you choose displays next to the Current Server title, and a series of boxes with configured services displays.

   Activation Status column displays either Activated or Deactivated in the Cisco CallManager line.

   If the **Activated** status displays, the specified Cisco CallManager service remains active on the chosen server.

   If the **Deactivated** status displays, continue with the following steps.
4. Check the check box for the desired Cisco CallManager service.
5. Click the **Update** button.

   The Activation Status column displays **Activated** in the specified Cisco CallManager service line.

   The specified service now shows active for the chosen server.

Perform the following procedure if the Cisco CallManager service has been in activated and you want to verify if the service is currently running.

Procedure

1. From Unified Communications Manager Administration, choose **Navigation** > **Cisco Unified Serviceability**.

   The Cisco Unified Serviceability window displays.
2. Choose **Tools** > **Control Center – Feature Services**.
3. From the Servers column, choose the server.

   The server that you chose displays next to the Current Server title, and a box with configured services displays.

   The Status column displays which services are running for the chosen server.