CHAPTER 6

Managing Services on the Cisco Intercompany Media Engine Server

TheCisco IME server contains network services and servlets that the system requires to function. Since these services are required for basic functionality, they do not require activation. However, you may need to stop and start (or restart) these services for troubleshooting purposes.

If something is wrong with a service or servlet, CriticalServiceDown alert is raised in RTMT. Alarms provide information on runtime status and the state of the system, so you can troubleshoot problems that are associated with your system. After viewing the alarm information, you can run a trace on the service. The trace files can help you further troubleshoot issues with your system.

This section contains information on services and describes how to troubleshoot issues using alarms and traces:

Services

After the installation of the Cisco IME application, network services start on the server automatically. The network services include services that the system requires to function; for example, database and platform services. You can configure these services by setting service parameters for each service. If necessary, for example, for troubleshooting purposes, you may need to stop and start (or restart) a network service. You perform these task by using the command line interface (CLI) on the Cisco IME server.

This section provides descriptions of services/servlets and describes how to start and stop services and configure service parameters from the CLI:

Service Descriptions

This section describes the network services that exist of the Cisco IME server and are grouped by the following functional areas:

For information on working with services, see the "Service Configuration Checklist" section on page 6-4.

Performance and Monitoring Services

This section describes the Performance and Monitoring Services.

Cisco CallManager Serviceability RTMT

The Cisco CallManager Serviceability RTMT servlet supports the Real Time Monitoring Tool (RTMT), which allows you to collect and view traces, view performance monitoring objects, work with alerts, and monitor devices, system performance, and so on.

Cisco Log Partition Monitoring Tool

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 by using configured thresholds and a polling interval.

Cisco RIS Data Collector

The Real-time Information Server (RIS) maintains real-time 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 the Real Time Monitoring Tool (RTMT), to retrieve the information that is stored in the RIS server.

Cisco AMC Service

Used for the Real Time Monitoring Tool (RTMT), this service, Alert Manager and Collector service, allows RTMT to retrieve real-time information that exists on the server.

Cisco Audit Event Service

The Cisco Audit Event Service monitors and logs any configuration change to the Cisco IME system by a user or as a result of the user action.

Backup and Restore Services

This section describes the Backup and Restore Services.

Cisco DRF Master

The CiscoDRF Master Agent service supports the DRF Master Agent, which works with the Disaster Recovery System 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.

Cisco DRF Local

The Cisco DRF Local service supports the Cisco DRF Local Agent, which acts as the workhorse for the DRF Master Agent. Components 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 Services

This section describes the System Services.

Cisco CDP

Cisco CDP advertises the voice application to other network management applications, so the network management application, for example, SNMP or CiscoWorks Lan Management Solution, can perform network management tasks for the voice application.

Cisco Trace Collection Servlet

The Cisco Trace Collection Servlet, along with the Cisco Trace Collection Service, supports trace collection and allows users to view traces by using RTMT. If you stop this service on a server, you cannot collect or view traces on that server.

For SysLog Viewer and Trace and Log Central to work in RTMT, the Cisco Trace Collection Servlet and the Cisco Trace Collection Service must run on the server.

Cisco Trace Collection Service

The Cisco Trace Collection Service, along with the Cisco Trace Collection Servlet, supports trace collection and allows users to view traces by using the RTMT client. If you stop this service on a server, you cannot collect or view traces on that server.

For SysLog Viewer and Trace and Log Central to work in RTMT, the Cisco Trace Collection Servlet and the Cisco Trace Collection Service must run on the server.

Tip If necessary, Cisco recommends that, to reduce the initialization time, you restart the Cisco Trace Collection Service before restarting Cisco Trace Collection Servlet.

Platform Services

This section describes the Platform Services.

Cisco Tomcat

The Cisco Tomcat service supports the web server.

SNMP Master Agent

This service, which acts as the agent protocol engine, provides authentication, authorization, access control, and privacy functions that relate to SNMP requests.

Tip After you complete SNMP configuration in the CLI, you must restart the SNMP Master Agent service in the Control Center—Network Features window.

MIB2 Agent

This service provides SNMP access to variables, which are defined in RFC 1213, that read and write variables; for example, system, interfaces, IP, and so on.

Host Resources Agent

This service provides SNMP access to host information, such as storage resources, process tables, and installed software base. This service implements the HOST-RESOURCES-MIB.

Native Agent Adaptor

This service, which supports vendor MIBs, allows you to forward SNMP requests to another SNMP agent that runs on the system.

System Application Agent

This service provides SNMP access to the applications that are installed and executing on the system. This implements the SYSAPPL-MIB.

Cisco CDP Agent

This service uses the Cisco Discovery Protocol to provide SNMP access to network connectivity information on the Cisco IME server. This service implements the CISCO-CDP-MIB.

Cisco Syslog Agent

This service supports gathering of syslog messages that various components generate. This service implements the CISCO-SYSLOG-MIB.

Cisco Certificate Expiry Monitor

This service periodically checks the expiration status of certificates that the system generates and sends notification when a certificate gets close to its expiration date.

Cisco IME Service

This service provides the primary functionality of the IME server. It manages data of the peer-to-peer network, communication to other nodes in the peer-to-peer network, and the communication to Cisco Unified Communication Manager.

Cisco IME Configuration Manager

This service manages administration and configuration settings used by the other services.

Service Configuration Checklist

Table 6-1 provides an overview of the steps for configuring services.

Table 6-1 Alarm Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Configure the appropriate service parameters.	Working with Services, page 6-5
Step 2	In the CLI, configure the server(s), service(s), destination(s), and event level(s) for the applications (services) alarm information that you want to collect. • All services can go to the SDI log (but must be configured using **`set alarm`** CLI command). • All alarms can go to the SysLog Viewer. • Ensure that Event Log alarm monitor is enabled with the desired severity. Use **`set alarm`** CLI command for this. • To send syslog messages to the Remote Syslog Server, enable the Remote Syslog destination and specify a host name. Use **`set alarm`** CLI command for configuration. If you do not configure the remote server name, the system does not send Syslog messages to the remote syslog server. **Tip** Do not configure a Cisco Unified Communications Manager server as a remote Syslog server.	• Alarms, page 6-6
Step 3	If you chose an SDI trace file as the alarm destination, collect traces and view the information with the Trace and Log Central option in RTMT.	• Traces, page 6-8 • *Cisco Unified Real Time Monitoring Tool Administration Guide*
Step 4	If you chose local syslog as the alarm destination, view the alarm information in the SysLog Viewer in RTMT.	• Traces, page 6-8 • *Cisco Unified Real Time Monitoring Tool Administration Guide*
Step 5	See the corresponding alarm definition for the description and recommended action, in the SysLog Viewer in RTMT.	• *Cisco Unified Real Time Monitoring Tool Administration Guide*

Working with Services

To start, stop, or restart services or to configure service parameters for services on the Cisco IME server, you must use the command line interface (CLI). You can start, stop, or refresh only one service at a time. Be aware that when a service is stopping, you cannot start it until after the service is stopped. Likewise, when a service is starting, you cannot stop it until after the service is started.

Caution Some changes to service parameters may cause system failure. Cisco recommends that you do not make any changes to service parameters unless you fully understand the feature that you are changing or unless the Cisco Technical Assistance Center (TAC) specifies the changes.

Table 6-2 shows the commands that you need to work with services on the Cisco IME server:

Table 6-2 Service CLI Commands

Task	Command
Display a list of services and service status	utils service list
Stop a service	utils service stop *servicename*
Start a service	utils service start *servicename*
Restart a service	utils service restart *servicename*
Show service parameters	show *servicename* serviceparam *serviceparametername* where, *servicename* can be ime, amc, risdc or enterprise. *serviceparametername* is one of the service parameters defined for that service. To see a list of serviceparameters that are defined for a service, use the following command: show *servicename* serviceparam ?
Set service parameters	set *servicename* serviceparam *service parameter name* where *servicename* equals <ime | amc | risdc | enterprise> and *service parameter name* is one of the service parameters defined for that service.

Additional Information

Related Topics, page 6-11

Alarms

Alarms provide information on runtime status and the state of the system, so you can troubleshoot problems that are associated with your system; for example, to identify issues with the Disaster Recovery System. Alarm information, which includes an explanation and recommended action, also includes the application name, machine name, and so on, to help you perform troubleshooting.

You configure the alarm interface to send alarm information to multiple locations, and each location can have its own alarm event level (from debug to emergency). You can direct alarms to the Syslog Viewer (local syslog), Syslog file (remote syslog), an SDI trace log file, or to all destinations.

When a service issues an alarm, the alarm interface sends the alarm information to the locations that you configure (and that are specified in the routing list in the alarm definition) (for example, SDI trace). The system can either forward the alarm information, as is the case with SNMP traps, or the system can write the alarm information to its final destination (such as a log file).

You use the Trace and Log Central option in the Real Time Monitoring Tool (RTMT) to collect alarms that get sent to an SDI trace log file. You use the SysLog Viewer in RTMT to view alarm information that gets sent to the local syslog.

As soon as you enter the CLI command, the system will prompt you for the required parameters. Enter the values to see the output.

Table 6-2 shows the commands that you need to work with alarms on the Cisco IME server:

Table 6-3 Alarm CLI Commands

Task	Command
Display the alarm configuration for a specific service/list of all services	show alarm Required Parameter(s): *servicename*—Name of the service. It could contain multiple words. Example: Enter the servicename as *all* to show the alarm configurations of all the services. Enter the servicename as *Cisco Tomcat* to show the alarm configuration of Cisco Tomcat service.
Enable/Disable alarms for a particular destination	set alarm *status* Required Parameter(s): *status*—enable or disable. *servicename*—Name of the service. It could contain multiple words. *monitorname*—SDI, SDL, Event_Log, or Sys_Log.
Enable alarms for a remote Syslog server	set alarm remotesyslogserver Required Parameter(s): *servicename*—Name of the service. It could contain multiple words. *servername*—Name of the remote syslog server.

Table 6-3 Alarm CLI Commands (continued)

Task	Command
Set the event level for an alarm	set alarm *severity* Required Parameter(s): *servicename*—Name of the service. It could contain multiple words. *monitorname*—SDI, SDL, Event_Log, or Sys_Log. *severity* equals one of the following: – Emergency—This level designates the system as unusable. – Alert—This level indicates that immediate action is needed. – Critical—The system detects a critical condition. – Error—This level signifies that an error condition exists. – Warning—This level indicates that a warning condition is detected. – Notice—This level designates a normal but significant condition. – Informational—This level designates information messages only. – Debug—This level designates detailed event information that Cisco TAC engineers use for debugging.
Set alarm configuration to default values **Tip** This option is available only for service names beginning with Cisco.	set alarm default Required Parameter(s): *servicename*—Name of the service. It could contain multiple words.

Additional Information

Related Topics, page 6-11

Traces

Traces assist you in troubleshooting issues with your application. You use the CLI to specify the level of information that you want traced as well the type of information that you want to be included in each trace file. You can configure trace parameters for any service on the Cisco IME server.

You can direct alarms to various locations, including SDI trace log files. If you want to do so, you can configure trace for alerts in the Real Time Monitoring Tool (RTMT).

After you have configured information that you want to include in the trace files for the various services, you can collect and view trace files by using the trace and log central option in the Real Time Monitoring Tool. To do this, configure alarms using **set alarm** CLI command.

You can configure the level of information that you want traced (debug level), what information you want to trace (trace fields), and information about the trace files (such as number of files per service, size of file, and time that the data is stored in the trace files)

After you have configured information that you want to include in the trace files for the various services, you can collect trace files by using the trace and log central option in RTMT. For more information regarding trace collection, see the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

Configuring Trace

You use the command line interface (CLI) to enable and disable tracing as well as to configure trace settings for specific services on the Cisco IME server. As soon as you enter the CLI command, the system prompts you for the required parameters. After the system generates trace files, you use RTMT to collect them. For more information regarding trace collection, see the "Collecting Traces" section on page 6-10 and refer to the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

Table 6-4 shows the commands that you need to work with traces on the Cisco IME server:

Table 6-4 Trace CLI Commands

Task	Command
Display the trace configuration for a specified service	show trace Required Parameter(s): *servicename*—Name of the service. It could contain multiple words. Example: Enter the servicename as *all* to show the trace configurations of all the services. Enter the servicename as *Cisco AMC Service* to show the trace configuration of Cisco AMC service.
Display the trace levels available for a specified service	show tracelevels Required Parameter(s): *servicename*—Name of the service. It could contain multiple words.
Enable/Disable trace for a specified service	set trace *status* Required Parameter(s): *status*— enable or disable *servicename*—Name of the service. It could contain multiple words.

Table 6-4 Trace CLI Commands (continued)

Task	Command
Specify the debug trace level settings for a specified service	set trace *tracelevel* Required Parameter(s): *tracelevel*—Use show tracelevels CLI command, to find the tracelevels for a given servicename. *servicename*—Name of the service. It could contain multiple words.
Specify the maximum size of a trace files for a specific service from 1 to 10 megabytes.	set trace maxfilesize Required Parameter(s): *servicename*—Name of the service. It could contain multiple words. *size*—Maximum size of the trace files from 1 to 10 megabytes.
Specify the maximum number of trace files per service. The system automatically appends a sequence number to the file name to indicate which file it is; for example, cus299.txt. When the last file in the sequence is full, the trace data begins writing over the first file.	set trace maxnumfiles Required Parameter(s): *servicename*—Name of the service. It could contain multiple words. *filecount*—Number of trace files from 1 to 10000.
Set the usercategories flag to the value provided, for a specified service. **Tip** This option is available only for service names beginning with Cisco.	set trace usercategories Required Parameter(s): *flagnumber*—Hexadecimal value from 0 to 7FFF. 7FFF means all the flags are enabled. *servicename*—Name of the service. It could contain multiple words.
Set trace configuration to default values for a specified service. **Tip** This option is available only for service names beginning with Cisco.	set trace default Required Parameter(s): *servicename*—Name of the service. It could contain multiple words.

Additional Information

Related Topics, page 6-11

Collecting Traces

The trace and log central feature in the Cisco Unified Real-Time Monitoring Tool (RTMT) allows you to configure on-demand trace collection for a specific date range or an absolute time. You can collect trace files that contain search criteria that you specify and save the trace collection criteria for later use, schedule one recurring trace collection and download the trace files to a SFTP or FTP server on your network, or to the localhost, or collect a crash dump file.

After you collect the files, you can view them in the appropriate viewer within the real-time monitoring tool. You can also view traces on the server without downloading the trace files by using the remote browse feature. You can open the trace files by either selecting the internal viewer that is provided with RTMT or choosing an appropriate program as an external viewer.

Note From RTMT, you can also edit the trace setting for the traces on the server that you have specified. Enabling trace settings decreases system performance; therefore, enable Trace only for troubleshooting purposes.

Note To use the trace and log central feature in the RTMT, make sure that RTMT can directly access the server without Network Access Translation (NAT). If you have set up a NAT to access devices, configure the server(s) with a hostname instead of an IP address and make sure that the host names and their routable IP address are in the DNS server or host file.

Additional Information

Related Topics, page 6-11

Related Topics

- Services, page 6-1
- Service Descriptions, page 6-1
- Service Configuration Checklist, page 6-4
- Working with Services, page 6-5
- Alarms, page 6-6
- Traces, page 6-8
- Configuring Trace, page 6-9
- Collecting Traces, page 6-10