Troubleshooting

This section provides you will tools to help you to troubleshoot the Cisco Intercompany Media Engine server. For more information on troubleshooting the Cisco Intercompany Media Engine feature, refer to the following URL:

http://docwiki.cisco.com/wiki/Cisco_Intercompany_Media_Engine

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 functions, on page 1

System history log fields, on page 2

Access the system history log using CLI, on page 4

System history log functions

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 Intercompany Media Engine

Product Version - 8.0.0.30671-1

Kernel Image - 2.6.9-78.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
    - 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, 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

Example

The following example shows a sample of the system history log.

System History Log

```
======================================Product Name -    Cisco Intercompany
 Media Engine
Product Version - 8.0.0.30671-1
Kernel Image -    2.6.9-78.EL
======================================
08/28/2009 10:40:34 | root: Install 8.0.0.30671-1 Start
08/28/2009 10:58:03 | root: Boot 8.0.0.30671-1 Start
08/28/2009 11:02:47 | root: Install 8.0.0.30671-1 Success
08/28/2009 11:02:47 | root: Boot 8.0.0.30671-1 Start
08/28/2009 13:33:48 | root: Cisco Option Install
ciscoime.proxy_commands.cop Start
08/28/2009 13:34:18 | root: Cisco Option Install
ciscoime.proxy_commands.cop Success
09/07/2009 23:44:43 | root: Upgrade 8.0.0.30600-103 Start
09/07/2009 23:56:48 | root: Upgrade 8.0.0.30600-103 Success
09/07/2009 23:57:06 | root: Switch Version 8.0.0.30671-1 to 8.0.0.30600-103
 Start
09/07/2009 23:57:52 | root: Switch Version 8.0.0.30671-1 to 8.0.0.30600-103
 Success
09/07/2009 23:57:52 | root: Restart 8.0.0.30600-103 Start
09/08/2009 00:00:36 | root: Boot 8.0.0.30600-103 Start
09/17/2009 12:40:38 | root: Upgrade 8.0.0.96000-2 Start
09/17/2009 12:52:54 | root: Upgrade 8.0.0.96000-2 Success
09/17/2009 12:53:11 | root: Switch Version 8.0.0.30600-103 to 8.0.0.96000-2
 Start
09/17/2009 12:53:55 | root: Switch Version 8.0.0.30600-103 to 8.0.0.96000-2
 Success
09/17/2009 12:53:55 | root: Restart 8.0.0.96000-2 Start
09/17/2009 12:56:27 | root: Boot 8.0.0.96000-2 Start
09/17/2009 13:29:47 | root: Switch Version 8.0.0.96000-2 to 8.0.0.30600-103
 Start
09/17/2009 13:30:34 | root: Switch Version 8.0.0.96000-2 to 8.0.0.30600-103
 Success
09/17/2009 13:30:34 | root: Restart 8.0.0.30600-103 Start
```

```
09/17/2009 13:33:06 | root: Boot 8.0.0.30600-103 Start
09/17/2009 14:22:20 | root: Upgrade 8.0.0.30600-9003 Start
09/17/2009 14:33:30 | root: Upgrade 8.0.0.30600-9003 Success
09/17/2009 14:33:48 | root: Switch Version 8.0.0.30600-103 to
8.0.0.30600-9003 Start
09/17/2009 14:34:33 | root: Switch Version 8.0.0.30600-103 to
8.0.0.30600-9003 Success
09/17/2009 14:34:33 | root: Restart 8.0.0.30600-9003 Start
09/17/2009 14:37:03 | root: Boot 8.0.0.30600-9003 Start
```

Access the system history log using CLI

You can access the system history log by using the CLI.

Procedure

You can access the system history log by using one of two **CLI file** commands.

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

For more information on the CLI file commands, see the *Cisco Intercompany Media Engine Command Line Interface Reference Guide*.

Related Topics

Access the system history log using RTMT, on page 4

Access the system history log using RTMT

You can access the system history log by using RTMT.

Procedure

From the Trace and Log Central tab, click **Collect Install Logs**.
For more information about using RTMT, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide.*

Related Topics

Access the system history log using CLI, on page 4

Audit logging

The following Cisco Intercompany Media Engine system components generate audit events:

- Real Time Monitoring Tool

- Cisco Unified Communications Operating System
- Command Line Interface
- Remote Support Account Enabled (CLI commands issued by technical supports teams)

The following example displays a sample audit event:

```
10:39:28.787| UserID:Administrator ClientAddress:10.194.109.32 Severity:6
EventType: CLICommand ResourceAccessed: GenericCLI EventStatus: Success
CompulsoryEvent: No AuditCategory: AdministrativeEvent ComponentID: CLI
AuditDetails: CLI Command-> utils ime license file install IME20091020095547801_node32.lic

App ID:Command Line Cluster ID: Node ID: node32
```

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 Cisco Intercompany Media Engine command line interface (CLI). 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 supports audit logging. If audit logs do not get written, then stop and start this service by using the CLI: utils service stop Cisco Audit Event Service and utils service start Cisco Audit Event Service.

All audit logs get collected, viewed and deleted from Trace and Log Central in the 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**.

Related Topics

Audit log types, on page 5
Set up audit logging, on page 7

Audit log types

The following types of audit logs display in RTMT:

Application Log

The application audit log, which displays in the AuditApp folder in RTMT, provides configuration changes for Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, the CLI, and Real Time Monitoring Tool (RTMT).

Although the Application Log stays enabled by default, you can disable audit logging by using the CLI **set auditlog status** command. If the audit logs get disabled, no new audit log files get created.

Cisco 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, Cisco 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 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.

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.

Note Audit log logs a CLI command successfully, even when the command is not allowed to run. For example, the following operation is permitted only on a bootstrap server:

admin:set ime dht global storagequota 1

When the above command is run on other servers, Audit log logs the CLI command with status=Success, even though the user would have received the message, `This command is only allowed to be run on a bootstrap server.`

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.

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.

Set up audit logging

The following procedure the commands that you need to work with SNMP users on the Cisco Intercompany Media Engine server:

Procedure

Step 1 Enter the following command to enable the operating system audit log: `utils auditd status`
Where status equals enable or disable. You can retrieve audit log files for the system through RTMT.

Step 2 Enter the following command to enable audit logging: `set auditlog status`
The system prompts you to enter the status parameter where status equals enable or disable.

You can retrieve audit log files for the system through RTMT.

Step 3 Enter the following command to set the purging status: `set auditlog purging`
The system prompts you to enter the status parameter where status equals enable or disable.

The Log Partition Monitor (LPM) looks at the Enable Purging option to determine whether it needs to purge audit logs. When you enable purging, LPM purges all the audit log files in RTMT whenever the common partition disk usage goes above the high water mark; however, you can disable purging by unchecking the check box. If purging is disabled, the number of audit logs continues to increase until the disk is full. This action could cause a disruption of the system. Be aware that this purging option is available for audit logs in an active partition. If the audit logs reside in an inactive partition, the audit logs get purged when the disk usage goes above the high water mark. You can access the audit logs by choosing Trace and **Log Central** > **Audit Logs** in RTMT.

Step 4 Enter the following command to set the log rotation status: `set auditlogrotation`
The system prompts you to enter the status parameter where status equals enable or disable.

Note When log rotation is disabled, audit log ignores the Maximum No. of Files setting.

The system reads this option to determine whether it needs to rotate the audit log files or it needs to continue to create new files. The maximum number of files cannot exceed 5000. When the Enable Rotation option is enabled, the system begins to overwrite the oldest audit log files after the maximum number of files gets reached.

Step 5 Enter the following command to set the maximum number of files: `set auditlog maxfilesize`
The system prompts you to enter the size parameter where size equals 1 to 10.

Enter the maximum number of files that you want to include in the log. Ensure that the value that you enter for the Maximum No. of Files setting is greater than the value that you enter for the No. of Files Deleted on Log Rotation setting.

Step 6 Enter the following command to set the maximum file size: `set auditlog maxnumfiles`
The system prompts you to enter the filecount parameter where filecount equals 1 to 10000.

Step 7 Enter the following command to set the auditlog remote syslog severity level: `set auditlog remotesyslogseverity`
The system prompts you to enter the severity parameter where severity equals one of the following: Emergency, Alert, Critical, Error, Warning, Notice, Informational, or Debug.

Step 8 Enter the following command to set the remote syslog server name: `set auditlog remotesyslogserver`
The system prompts you to enter the servername parameter where servername equals a valid hostname of a remote syslog server.

Netdump utility

In a Cisco Unified Communications Manager cluster, you must configure at least two nodes as netdump servers, so the first node and subsequent nodes can send crash dump logs to each other.

For example, if your cluster contains three servers (one primary/first node and two subsequent nodes), you can configure the first node and subsequent node #1 as the netdump servers. Then, you can configure the first node as a netdump client of the subsequent node #1 and configure all of the subsequent nodes as netdump clients of the first node. If the first node crashes, it sends the netdump to subsequent node #1. If any subsequent node crashes, it sends the netdump to the first node.

You can use an external netdump server rather than configuring a Cisco Unified Communications Manager server as a netdump server. For information on configuring an external netdump server, contact TAC.

Note Cisco recommends that you configure the netdump utility after you install Cisco Unified Communications Manager to assist in troubleshooting. If you have not already done so, configure the netdump utility before you upgrade Cisco Unified Communications Manager from supported appliance releases.

To configure the netdump servers and clients, use the command line interface (CLI) that is available for the Cisco Unified Communications Operating System.

Related Topics

Set up a netdump server, on page 8
Set up a netdump client, on page 9
Netdump server files, on page 9
Monitor netdump status, on page 10

Set up a netdump server

To configure a node as a netdump server, use the following procedure:

Procedure

Step 1 Start a CLI session on the node that you want to configure as the netdump server.
For more information refer to the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Step 2 Execute the `utils netdump server start` command.

Step 3 To view the status of the netdump server, execute the `utils netdump server status` command.

Step 4 Configure the netdump clients, as described in the Set up a netdump client, on page 9.

Set up a netdump client

To configure a node as a netdump client, use the following procedure:

Procedure

Step 1 Start a CLI session on the node that you want to configure as the netdump client.
For more information, refer to *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Step 2 Execute the `utils netdump client start ip-address-of-netdump-server` command.

Step 3 Execute the `utils netdump server add-client ip-address-of-netdump-client` command.
Repeat this command for each node that you want to configure as a netdump client.

Note Make sure that you enter the correct IP addresses. The CLI does not validate the IP addresses.

Step 4 To view the status of the netdump client, execute the `utils netdump client status` command.

Netdump server files

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

To use the CLI to collect the netdump logs, use the **file** CLI commands on the files in the crash directory. The log filenames begin with the IP address of the netdump client and end with the date that the file gets created. For information on the file commands, refer to the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Monitor netdump status

You can monitor the netdump status by configuring SyslogSearchStringFound alerts in Real Time Monitoring Tool. Use the following procedure to configure the appropriate alerts:

Procedure

Step 1 From the quick launch channel in Real Time Monitoring Tool, choose **Tools** > **Alert Central**.

Step 2 Right-click the **SyslogStringMatchFound** alert and choose **Set Alert/Properties**.

Step 3 Click **Next** three times.

Step 4 In the **SysLog Alert** window, click the **Add** button.

Step 5 When the Add Search String dialog box displays, enter netdump: failed and click **Add**.

Note Make sure that the case and syntax matches exactly.

Step 6 Click **Next**.

Step 7 In the **Email Notification** window, choose the appropriate trigger alert action, enter any user-defined email text, and click **Save**.