Troubleshooting

Last updated: December 2, 2010

About Troubleshooting

Cisco technical support personnel may request that you run one or more of these commands when troubleshooting a problem. Cisco technical support personnel will provide additional information about the commands at that time.

Caution Some of these commands may impact the performance of your system. We strongly recommend that you do not use these commands unless directed to do so by Cisco Technical Support.

Running a Network Connectivity Test

You can run a network connectivity test to initiate a connection between the Cisco UMG device and all the systems that are configured on the system, including the Cisco Unified Communications Manager, Cisco Unity Connection servers, SRST sites, and SRSV-CUE devices.

The test may take several minutes to complete, during which time the status page will refresh automatically. You can either wait for the test to complete or go to other pages and later return to this page to see the test results.

Procedure

Step 1 Log in to the Cisco UMG GUI.

Step 2 Choose **Troubleshoot > Network Connectivity**.

The system displays the Network Connectivity Test page.

Step 3 To start a network connectivity test, click **Start Network Connectivity Test**.

When the test is complete, the system displays a message stating that the test is complete and shows the results. After you run a network connectivity test, the system displays the results for the following:

- Central call agents
- Central voicemail servers
- Branch voicemail servers
- Branch call agents

For each category, the system shows the hostname of the system to which it tried to connect; the result, either success or failure; the amount of time in milliseconds that it took to connect; and any details.

If the connectivity test fails, the system displays a brief indication of the cause of the failure. You can find additional failure diagnostic information in the trace buffer or message log.

Step 4 To cancel the network connectivity test that is currently running, click **Cancel Network Connectivity Test**.

Step 5 To see the results of the previous test click **Click here for results of previous test**.

Note Results of the previous test are only available for the current login session. For example, if the administrator logs out and then logs back in later, the previous results will not be available.

Step 6 To restart a previous network connectivity test, click **Restart Network Connectivity Test**.

Log and Trace Files

About Logging

Logging and tracing to the hard disk is turned off by default. Executing the **log trace** command starts the log and trace functions immediately.

To check the log and trace files on the hard disk, use the **show logs** command in Cisco UMG EXEC mode. It displays the list of logs available, their size, and their dates of most recent modification.

Each file has a fixed length of 10 MB, and tracing or logging stops automatically when the file reaches this length. New files overwrite the old files.

Note Logs for E-SRST are turned on by default. Logs for SRSV and VPIM are turned off by default.

Example of Log Output

The following is an example of the log output:

```
umg-1# show logs
SIZE             LAST_MODIFIED_TIME                              NAME
  1225782   Mon Aug 20 16:55:39 PDT 2007                linux_session.log
     4585   Wed Aug 08 14:52:25 PDT 2007                       install.log
     7883   Mon Aug 20 17:10:00 PDT 2007                            dmesg
  5000139   Mon Aug 20 13:40:37 PDT 2007                messages.log.prev
     9724   Mon Aug 20 17:10:05 PDT 2007                        syslog.log
    10418   Tue Aug 07 13:39:18 PDT 2007                    sshd.log.prev
      968   Wed May 09 20:51:34 PDT 2007                  dirsnapshot.log
   131357   Thu Aug 09 01:28:31 PDT 2007                     shutdown.log
 51325740   Tue Aug 21 17:56:10 PDT 2007                       atrace.log
     1534   Mon Aug 20 17:10:04 PDT 2007                debug_server.log
    10274   Tue Jul 31 13:32:51 PDT 2007                postgres.log.prev
     2398   Mon Aug 20 17:10:04 PDT 2007                         sshd.log
104857899   Mon Aug 20 15:13:44 PDT 2007                  atrace.log.prev
     4119   Mon Aug 20 17:10:22 PDT 2007                     postgres.log
     4264   Mon Aug 20 17:10:07 PDT 2007                         klog.log
   984742   Tue Aug 21 18:04:36 PDT 2007                     messages.log
    55435   Wed Aug 08 14:52:06 PDT 2007          shutdown_installer.log
umg-1#
```

Log Commands in Cisco UMG Configuration Mode

- **log console errors**—Displays error messages (severity=3)
- **log console info**—Displays information messages (severity=6)
- **log console notice**—Displays notices (severity=5)
- **log console warning**—Displays warning messages (severity=4)
- **log server address** *a.b.c.d*

Log Commands in Cisco UMG EXEC Mode

- **log console monitor**
- **log trace boot**
- **log trace buffer save**

Saving and Viewing Log Files

Problem You must be able to save log files to a remote location.

Recommended Action Log files are saved to a disk by default. You can configure Cisco UMG to store the log files on a separate server by using the **log server address** command. Also, you can copy log files on the disk to a separate server if they need to be kept for history purposes, for example:

copy log *filename*.**log url ftp://***ftp-user-id*:*ftp-user-passwd*@*ftp-ip-address*/*directory*

```
umg# copy log messages.log url ftp://admin:messaging@172.168.0.5/log_history
```

Problem You cannot display the contents of the log files.

Recommended Action Copy the log files from Cisco UMG to an external server and use a text editor, such as **vi**, to display the content.

Saving Configuration Changes

Problem You lost some configuration data.

Recommended Action Copy your changes to the running configuration at frequent intervals. See the "Copying Configurations" section on page 131.

Problem You lost configuration data when you rebooted the system.

Explanation You did not save the data before the reboot.

Recommended Action Issue a **copy running-config startup-config** command to copy your changes from the running configuration to the startup configuration. When Cisco UMG reboots, it reloads the startup configuration.

Note Messages are considered application data and are saved directly to the disk in the startup configuration. (They should be backed up on another server in case of a power outage or a new installation.) All other configuration changes require an explicit "save configuration" operation to preserve them in the startup configuration.

Using Trace Commands

To troubleshoot network configuration in Cisco UMG, use the **trace** command in EXEC mode. For a detailed list of all the arguments associated with the trace command, see the *Command Reference for Cisco Unified Messaging Gateway Release 8.0*.

Examples

	Command or Action	Purpose
Step 1	**trace dns resolver** { **all** | **receive** | **send** } **Example:** `umg-1# trace dns resolver all`	Enables tracing for DNS network functions. • **all**—Traces every DNS activity. • **receive**—Traces DNS receiving. • **send**—Traces DNS sending.
Step 2	**trace sysdb all** **Example:** `umg-1# trace sysdb all`	Enables tracing for every sysdb entity and activity.

	Command or Action	Purpose
Step 3	**trace dns all** **Example:** `umg-1# trace dns all`	Enables tracing for every DNS event. For example, displays DNS lookups that are performed and results that are given when a domain is verified and resolved using SMTP.
Step 4	**trace dbclient database** { **garbagecollect** | **largeobject** | **mgmt** | **query** | **results** | **transaction** } **Example:** `umg-1# trace dbclient database results`	Enables tracing for client database functions. The following keywords specify the type of traces: • **garbagecollect**—Garbage collection process. • **largeobject**—Large object reads and writes to the database. • **mgmt**—Database management processes. • **query**—Queries performed on the database. • **results**—Results of queries, inserts, and updates. • **transactions**—Start and end of database transactions.
Step 5	**trace srsx** {**gui** | **registration** | **cli** | **controller** | **upload** | **mgmt** | **srsv-engine** | **service-point** | **vm-server-client** | **call-agent-client** | **srsv-secret-syncer** | **site-manager** | **srst-engine** }	Enables tracing for SRSx functions. The following keywords specify the type of traces: • **gui** — SRSx GUI debugging. • **registration** — SRSx device registration debugging • **cli** — SRSx CLI debugging • **controller** — SRSx controller debugging • **upload** — SRSV voicemail upload debugging • **mgmt** — SRSx management interface debugging • **srsv-engine** — SRSV provisioning engine debugging • **service-point** — SRSx service point debugging • **vm-server-client** — SRSx central voicemail server communication debugging • **call-agent-client** — SRSx central call agent server communication debugging • **srsv-secret-syncer** — SRSx shared secret synchronization debugging • **site-manager** — SRSx site manager debugging • **srst-engine** — E-SRST provisioning engine debugging