Main page: Cisco Unified MeetingPlace, Release 8.0

Back to: Maintenance

Back to: Troubleshooting

- About Alarms
- How to View the Alarm Table and Clear Alarms
- Configuring the System to Call You If There is a Major Alarm
- How to View the Current Status of the System
- Viewing the System Log
- Viewing Log Information about System Backups
- Obtaining and Viewing the System Information Capture (Infocap) Log
- How to Configure Logging Levels

Contents

About Alarms

Alarms are caused by network connectivity failures and are usually software-related. They can also occur when there is a surge of activity on the network, or when the system detects a configuration issue, such as not having conferencing licenses installed.

When the system generates an alarm:

- Similar alarms are aggregated into the Alarm Table.
- The alarm is captured in the Exception Log.
- If SNMP is configured, a notification is sent to any registered management stations.

In general, you can use the Alarm Table to check for any problems, and then look in the Exception Log for details.

Related Topics

- Configuring SNMP on the Cisco Unified MeetingPlace Application Server module
- Viewing the Alarm Table and Clearing Alarms in the Administration Center
- Alarm Severity Levels
- Module Numbers
- *Alarm and Exception Code Reference for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_technical_reference_list.html

Alarm Severity Levels

Alarm Severity	Description

Level	
MAJOR	Action must be taken immediately. A system error occurred that requires manual intervention. You will likely need to contact Cisco TAC. Examples: • Less than 50% of a major resource (audio, video, or web) is functional. • A major feature (such as Microsoft Outlook integration) is nonfunctional or might soon become nonfunctional. • A server is about to run out of disk space.
MINOR	Investigate the issue to determine if immediate action is needed. An error occurred that does not impact the ability of the system to continue to function. Nevertheless, some corrective action is required. Depending on the issue, you might need assistance from Cisco TAC. Examples: • A server has exceeded the recommended threshold of disk space. • A blade failure causes less than 50% of a resource capacity to be lost. • A configuration error prevents dial-out calls.

Related Topics

- About Alarms
- *Alarm and Exception Code Reference for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_technical_reference_list.html
- There is a known issue CSCsk64601, cma.log files uses up all disk space during mpx_sys restart, causes /var partition reaches 100% used. cma.log files are located at /var/spool/compaq/ folder. If you are running into this issue, please apply following as a permanent workaround.

```
Workaround:
1. Delete cma.log and reboot system.
2. Symlink cma.log to /dev/null as a fix by performing below.
  A. cd /var/spool/compaq/
  B. ln -s /dev/null cma.log
```

Alarm Table

You can view the alarm table:

- On the Alarms Page in the Administration Center
- By entering the alarm command
- In the "Alarms" log in the System Information Capture (Infocap) log

The alarm table combines multiple alarms into a single table entry when these values are the same:

- Code
- Unit

- Software Module

The brief description in an alarm table entry can contain values that are specific to one alarm occurrence, such as an IP address or the available disk space on a Web Server. These values might differ for all alarms that are combined into one table entry, but only the values for the *most recent* alarm are displayed. To view all alarm occurrences, view the Exception Log.

Entries remain in the alarm table until you clear them. Therefore, the alarm table can display very old information. In contrast, only the alarms generated during a specified time period are displayed in the "ExLog error logs" or "ExLog detailed logs" in the System Information Capture (Infocap) log.

We recommend that you regularly clear the alarm table, so that:

- You can tell at a glance whether any new alarms have been generated since the last time you looked.
- You can distinguish between individual alarms, because there will be fewer counts per table entry.

Related Topics

- How to View the Alarm Table and Clear Alarms
- About Alarms
- Module Numbers
- Obtaining and Viewing the System Information Capture (Infocap) Log
- *Alarm and Exception Code Reference for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_technical_reference_list.html

Exception Log

The exception log contains alarm and error messages. Clearing alarms in the Alarm Table does not clear alarms in the exception log.

You can view the exception log:

- By entering the errorlog command or the viewexlog command.
- In the "ExLog error logs" or "ExLog detailed logs" in the System Information Capture (Infocap) log.

Related Topics

- Using the Command-Line Interface (CLI) on the Cisco Unified MeetingPlace Application Server module
- Obtaining and Viewing the System Information Capture (Infocap) Log
- About Alarms
- Alarm Severity Levels
- *Alarm and Exception Code Reference for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_technical_reference_list.html
- Module Numbers

Module Numbers

Use Table: Module Numbers to determine which system component corresponds to each module number that might appear in the Alarm Table or Exception Log.

Table: Module Numbers

Internal Error Number	System Component	Module Number	Description
0	IMC_CLASS_NULL	0	Command line utility
1024	IMC_CLASS_COMMON	1	Common functions
2048	IMC_CLASS_SIM	2	System Integrity Manager (SIM)
3072	IMC_CLASS_CP	3	Call Processing-Media Control Protocol (CPMCP), which is a proxy for the Media Server
4096	IMC_CLASS_SM	4	Switch manager
5120	IMC_CLASS_CS	5	Conference scheduler (ConfSchd)
6144	IMC_CLASS_WS	6	Workstation server
7168	IMC_CLASS_EXC	7	Exception handler (in SIM)
8192	IMC_CLASS_VUI	8	Telephone user interface (TUI)
9216	IMC_CLASS_DB	9	The database server
10240	IMC_CLASS_VUI_TESTER	10	TUI tester program
11264	IMC_CLASS_TRACE	11	SIM trace server
12288	IMC_CLASS_WF	12	Workstation front end
13312	IMC_CLASS_UTIL	13	Any command line utility
14336	IMC_CLASS_LSH	14	Shell facility
15360	IMC_CLASS_DBQ	15	Database query server
16384	IMC_CLASS_EMAIL_MSG	16	Class to support an error range
17408	IMC_CLASS_SNMPD	17	Class to support SNMP daemon control
18432	IMC_CLASS_PO	18	Post office server
19456	IMC_CLASS_PO_TESTER	19	Post office server tester program
20480	IMC_CLASS_SIM_MU	20	Multi-unit SIM session control
21504	IMC_CLASS_FAXGW	21	Fax gateway
22528	IMC_CLASS_WEBGW	22	Web publisher (overlaps with pegs)
22528	IMC_CLASS_PEGS	22	Peg server (part of SIM)
23552	IMC_CLASS_SDBS	23	Shadow database server
24576	IMC_CLASS_SDBS_TESTER	24	Shadow database server tester program
25600	IMC_CLASS_GWSIMGR	25	
26624	IMC_CLASS_GWSIMAGENT	26	
27648	IMC_CLASS_STREAMGW	27	Streaming gateway
28672	IMC_CLASS_CCA	28	Call control agent
29696	IMC_CLASS_MPDIRSVC	29	Directory services

30720	IMC_CLASS_MERGED	30	PCI conversion/merge daemon
31744	IMC_CLASS_GSCOPE	31	Gyroscope application
32768	IMC_CLASS_NMPAGENT	32	NMPAgent
33792	IMC_CLASS_TWATCH	33	Trigger watch
34816	IMC_CLASS_POCLIENT	34	Post office client

Related Topics

- *Alarm and Exception Code Reference for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_technical_reference_list.html

How to View the Alarm Table and Clear Alarms

Viewing the Alarm Table and Clearing Alarms in the Administration Center

Procedure

1. Sign in to the Administration Center.
2. Select **Services > Alarms**.
3. (Optional) Clear alarms:
    - To clear one or more alarms, select the entries, and select **Delete Selected**.
    - To clear all alarms, select **Delete All**.

Related Topics

- Table: Field Reference: Alarms Page in the Administration Center Page References for Cisco Unified MeetingPlace (A - C pages)
- Alarm Table
- *Alarm and Exception Code Reference for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_technical_reference_list.html
- Module Numbers
- Alarm Severity Levels

Viewing the Alarm Table and Clearing Alarms By Using the CLI on the Application Server

Procedure

1. Sign in to the CLI of the Application Server.
2. Enter the alarm command.
   The Alarm Table appears.
   Note the reference number (REFNO) for any alarms that you want to clear.

Note: Use the viewexlog or the errorlog command for more accurate information.

1. (Optional) Clear alarms:
   - To clear all alarms, enter the **clearalarm all** command:
   - To clear one alarm, enter this command, specifying the reference number (REFNO) from the alarm table.

     reference-number

Related Topics

- Using the Command-Line Interface (CLI) on the Cisco Unified MeetingPlace Application Server module
- Alarm Table
- *Alarm and Exception Code Reference for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_technical_reference_list.html
- Module Numbers

Configuring the System to Call You If There is a Major Alarm

You can configure Cisco Unified MeetingPlace to call you if a major alarm occurs. When you answer the phone call, you will be provided with this information:

- Notification that an error has occurred that requires attention.
- A request to view the alarms.
- A request to acknowledge the alarm call.

Restriction

Pagers cannot be used to receive alarm calls.

Procedure

1. Sign in to the Administration Center.
2. Select **System Configuration > Usage Configuration**.
3. Configure these fields:
   - Call out on major alarm-Set to **Yes**.
   - Phone number to call on alarm-Enter the phone number of the system administrator.
4. Select **Save**.

Related Topics

- Usage Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace (U - W pages)

How to View the Current Status of the System

Viewing the Current Status of the System in the Administration Center

Use the system status to check the condition of the Cisco Unified MeetingPlace system. The system status shows this information:

- System status details, such as mode, temperature, and power supply
- Each server name
- Each mailbox name and the number of messages that are in each mailbox
- Each module name and its status
- The CPU usage statistics

Note: If you want to view the status of the Cisco Unified MeetingPlace system during a particular time period, see the Obtaining and Viewing the System Information Capture (Infocap) Log.

Procedure

1. Sign in to the Administration Center.
2. Select **Services > System Status**.
3. Select **View Status**.

Related Topics

- Table: Field Reference: System Status Details Page in the Administration Center Page References for Cisco Unified MeetingPlace (R -S pages)
- Module Numbers
- Viewing the Current Status of the Software By Using the CLI on the Application Server

Viewing the Current Status of the Software By Using the CLI on the Application Server

Procedure

1. Sign in to the CLI.
2. Enter the swstatus command.
   If a module or Web Server is unexpectedly down, check the Alarm Table or the Exception Log for the reason.

Example

```
[mpxadmin@example-server ~]$ swstatus

Conference server 7.0.0.872

System mode: Ups

Media control: Up

MODULE NAME STATUS VERSION

SIM UP "07/11/08 18:32 Rel_7_0_0_872"

DBSERVER UP "07/11/08 18:18 Rel_7_0_0_872"

SNMPD UP "07/11/08 18:32 Rel_7_0_0_872"

CPSERVER UP "07/11/08 18:31 Rel_7_0_0_872"

POSERVER UP "07/11/08 18:19 Rel_7_0_0_872"

CONFSCHED UP "07/11/08 18:26 Rel_7_0_0_872"

TRIGGER_WATCH UP "07/11/08 18:33 Rel_7_0_0_872"

POCLIENT UP "07/11/08 18:39 Rel_7_0_0_872"

GWSIMMGR UP "07/11/08 18:33 Rel_7_0_0_872"

VOICESERVER UP "07/11/08 18:30 Rel_7_0_0_872"

NMPAGENT UP "07/11/08 18:32 Rel_7_0_0_872"

CHECKLIC UTIL DONE "07/11/08 18:35 Rel_7_0_0_872"
```

Related Topics

- Using the Command-Line Interface (CLI) on the Cisco Unified MeetingPlace Application Server module
- *Alarm and Exception Code Reference for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_technical_reference_list.html
- Viewing the Current Status of the System in the Administration Center

Viewing the System Log

The system log captures and buffers high-level details about system software activities. You can choose the severity level that you want to see. The output lists the date and time of the exception, the exception code, the file in which the exception occurs, and a text description of the exception.

Note: The system sorts messages by using the date and time that each message was added to the log file. If time is not synchronized across all Cisco Unified MeetingPlace servers, the time used for sorting might differ from the displayed time stamps, and the log messages might seem to appear out of order. The system uses the time stamp for each message to filter out messages that are outside the specified start and end dates.

Procedure

1. Sign in to the Administration Center.
2. Select **Services > Logs > View System Logs**.
3. Configure the fields.
4. Select **View Logs**.

Related Topics

- Table: Field Reference: View System Logs Page in the Administration Center Page References for Cisco Unified MeetingPlace (U - W pages)
- Table: Field Reference: System Logs Page in the Administration Center Page References for Cisco Unified MeetingPlace (R - S pages)
- *Alarm and Exception Code Reference for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_technical_reference_list.html
- Module Numbers

Viewing Log Information about System Backups

You can display the last 20KB of the Informix backup log file, which lists the processes that occurred during the most recent backups.

Procedure

1. Sign in to the Administration Center.
2. Select **Services > Logs > View Backup Logs**.

Related Topics

- Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server module

Obtaining and Viewing the System Information Capture (Infocap) Log

The System Information Capture log provides details about the configuration and failure of the Cisco Unified MeetingPlace system during a particular time period. In general, every bug report should include the System Information Capture log.

Running this log generates a very large zip file that you can send to Cisco TAC, who can help you troubleshoot problems. After you download the zip file, be sure to delete it from the /tmp directory to save space on your system.

Note: To display the current status of the Cisco Unified MeetingPlace system, instead of over a specific period of time, see the Viewing the Current Status of the System in the Administration Center.

Note: During normal system use, you may use the **su** command to switch to the root user level. If you accidentally enter the root password into the command line, it is possible that the root password will be recorded in the BASH history file (~/.bash_history). If this happens, you should use the history -c command to clear the history; otherwise, the root password may be visible to other users and it might be captured as part of the infocap log.

Procedure

1. Sign in to the Administration Center.
2. Select **Services > Logs > System Information Capture**.
3. Enter or change the values on the System Information Capture Page.
   Note: To receive better and faster service from Cisco TAC, enter as much information as you can. The details you provide will help Cisco TAC quickly understand and troubleshoot the problem.
4. Select **Capture Logs**.
5. Select **OK**.
6. Obtain the data by taking one of these actions:
   - Navigate to the zip file specified on the page. The name of the zip file is based on the date and time parameters that you entered on the System Information Capture Page.
   - Select **Export to File**.
7. To view the System Information Capture log:
   1. Extract the files from the zip file.
   2. Open the index.html file.

Related Topics

- Table: Field Reference: System Information Capture Page in the Administration Center Page References for Cisco Unified MeetingPlace (R - S pages)

What To Do Next

We recommend that you delete the zip file from the /tmp directory to save space on your system.

How to Configure Logging Levels

On the Configure Logging Levels Page, you can define log levels for Cisco Unified MeetingPlace web applications and for the Media Server. The system collects messages for the specified log level and all the

levels below it. The higher the log level you specify, the more information is collected. Debug is the highest log level.

Caution! Increasing log levels can severely decrease system performance and even freeze Cisco Unified MeetingPlace. Only change the log levels if Cisco TAC requests that you change them.

This section contains these topics:

Log Levels

All log level changes occur during runtime; restarting is not required. These log levels are available:

- **Debug**-All logs are saved. This is the highest setting level.
- **Info**-Important events are logged. This is the default setting.
- **Error**-Only errors and exceptions are logged.
- **Warn**-Only warning errors are logged.

Related Topics

- Configuring Logging Levels

Configuring Logging Levels

Restriction

To configure Media Server logging levels, the Type of media server must be set to Hardware Media Server.

Procedure

1. Sign in to the Administration Center.
2. Select **Services > Logs > Configure Logging Levels**.
3. Enter or change the values in the fields.
4. Select **Save**.

Related Topics

- Table: Field Reference: Configure Logging Levels Page in the Administration Center Page References for Cisco Unified MeetingPlace (A - C pages)

- Obtaining and Viewing the System Information Capture (Infocap) Log