Main page: Cisco Unified MeetingPlace, Release 7.0

Up one level: Maintenance Page

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.

Contents

Related Topics

- Configuring SNMP on Cisco Unified MeetingPlace
- 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 Level	Description
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 may 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 may 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

- *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 Table

The alarm table can be viewed:

- 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 the following values are the same:

- Code
- Unit
- Software Module

The brief description in an alarm table entry may 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 may differ for all alarms that are combined into one table entry. In Release 7.0.0 - 7.0.2, only the values for the first alarm are displayed. In Release 7.0.3, 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 may 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
- 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) in Cisco Unified MeetingPlace
- 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

Module Numbers

Use Table: Module Numbers to determine which system component corresponds to each module number that may 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

Core Files

Core files are useful for determining what state a program was in before it terminated. In Release 7.0.3 (MR2) a new utility called **checkcores** reports new cores found, raises an alarm (EX_CORESPACE), and compresses/archives the cores to /mpx-record/cores.

Note: Unless the cause of the core file is already known, all core files should be escalated to Cisco TAC.

During startup, if new cores are found, the following message is echoed to the session after "Starting MeetingPlace application":

```
NOTE: new core files found in /var
See /mpx-record/cores/checkcores.log for more information
                                                        [  OK  ]
```

If no cores are found, the utility does not log anything. If run interactively, the utility either echoes the two lines shown above if cores are found, or echoes "no cores found".

A maximum of 10 core files are saved to this location. The approximate total max space requred for compressed core images is 200MB. If there is insufficient space in /mpx-record, an alarm is raised:

```
346) MAJ 10006c    4 Mar 22 05:58  Mar 22 06:00   0 SW MODULE=0
    insufficient space in /mpx-record filesystem to manage cores
```

A logfile, "/mpx-record/cores/checkcores.log" is maintained in /mpx-record/cores. If this logfile grows beyond 100K, it is backed up to "checkcores.log.old" and a new log is started (only one backup is maintained).

Cores are archived in the form:

yymmddhhmmss-path1-path2-path3-core.pid.datetime.gz

- **yymmddhhmmss** is the current date/timestamp
- **path1-path2-path3** is the full path translated to hyphen-separated names, e.g., /var/mp/nmpagent is translated to var-mp-nmpagent
- **pid** is the process id of the aborted process
- **datetime** is the date/timestamp of the core file creation as displayed by "ls -l", but in a compressed form (e.g. Mar2-14:52, Jan22-09:15).

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