Avaya Aura™ Communication Manager Server Alarms

03-602798
Issue 1
May 2009

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya.

End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Websites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Website: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by the said Avaya reseller and not by Avaya.

Licenses

The software license terms available on the Avaya Website, http://support.avaya.com/licenseinfo/ are applicable to anyone who downloads, uses and/or installs Avaya software, purchased from Avaya Inc., any Avaya affiliate, or an authorized Avaya reseller (as applicable) under a commercial agreement with Avaya or an authorized Avaya reseller. Unless otherwise agreed to by Avaya in writing, Avaya does not extend this license if the software was obtained from anyone other than Avaya, an Avaya affiliate or an Avaya authorized reseller, and Avaya reserves the right to take legal action against you and anyone else using or selling the software without a license. By installing, downloading or using the software, or authorizing others to do so, you, on behalf of yourself and the entity for whom you are installing, downloading or using the software (hereinafter referred to interchangeably as "you" and "end user"), agree to these terms and conditions and create a binding contract between you and Avaya Inc. Or the applicable Avaya affiliate ("Avaya").

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

- Designated System(s) License (DS):
  End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU):
  End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.
- Named User License (NU):
  End User may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User" means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (for example, webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR):
  Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License"). (See Third-party Components for more information).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Website: http://support.avaya.com/Copyright.

Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Website:

http://www.support.avaya.com/.

Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to:securityalerts@avaya.com.

Trademarks

Avaya® and Avaya Aura™ are trademarks of Avaya Inc.

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

All non-Avaya trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Website: http://www.avaya.com/support.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Website: http://www.avaya.com/support.

Contents

Server Alarms

This document contains information on server alarms generated on various platforms. These alarms cover such categories as process watchdog, environmental, login, translation monitoring, and power supply alarms. Alarm identifications, levels, and resolutions are given.

During normal operations, software or firmware may detect error conditions pertaining to specific Maintenance Objects (MOs). The system automatically attempts either to fix or circumvent these problems. Errors are detected in two ways:

- By firmware on the component during on-going operations
- A “periodic test” or a “scheduled test” started by software

Tests that are run on demand are generally more comprehensive (and potentially disruptive) than the "scheduled tests".

When an error is detected, it is recorded in the Error Log. If a component incurs too many errors, an alarm is raised.

Alarms on the Linux servers can occur in several areas:

- Media Modules, Servers, the Media Gateway Processor, and the Layer 2 Switching Processor are all capable of detecting internal failures and generating traps and alarms.
- Media Gateways detect faults and alert the Server. The Server then raises an alarm and sends the alarm to an appropriate network management site.
- Communication Manager alarms reflect the health status of network elements such as circuit packs, media modules, and their associated links, ports, and trunks.
- Messaging alarms provide health status of embedded or external messaging systems.

Alarms may be viewed using the following:

- Maintenance Web Interface

  Provides alarms information related to Communication Manager, the server, and messaging.

  Note:

  > For non-Communication Manager alarms, use the Web Page header "Alarms and Notification" and "Diagnostics: View System Log". Choose the appropriate heading and, if necessary, call Avaya support.

- Server bash shell

  Provides alarms information related to Communication Manager, the server, and messaging.

- Server SAT (System Access Terminal) CLI (Command Line Interface)

  Provides alarms information related to Communication Manager.

- MGP CLI (on the Media Gateway)

  Provides alarms and traps information related to the media gateway and its subsystems.
- Layer 2 Switching Processor CLI (on the Media Gateway)

  Provides information related to the media gateway stack.

Information related to Communication Manager, the server, and messaging alarms can be displayed using either the Maintenance Web Interface or the server bash shell.

This document provides information only for server alarms. For messaging alarms and repair procedures, refer to the appropriate documentation for the messaging system.

Server Maintenance

Server maintenance focuses on five functional roles:

1. Provide the alarm logging and reporting service for all other system components.
2. Monitor the health of server components and diagnose problems *at least* to the level of user-replaceable components:
   - Server chassis - contains main board, hard disk, memory, fan/temperature/voltage sensors, network interface cards (NICs), removable storage devices. The entire server box is the user-replaceable component for all components contained within it, e.g., hard disk, memory, power supply, removable media devices, etc. Maintenance software may provide diagnostic information to the subcomponent level, but maintenance procedures will specify *only* entire-server replacement as a remedy.
   - Server uninterruptible power supplies (UPS)
   - Server external modems
   - Server-to-IPSI network Ethernet switches
3. Support specific interface/information needs of server duplication and maintenance software.
4. Provide maintenance commands that the support technicians use to determine the state of health of the system and effect repair/recovery actions.
5. Provide server diagnostic/recovery/notification mechanisms when a server’s processor is down, i.e. is unable to execute the system software.

Alarm Classifications

Alarms are classified depending on their effect on system operation:

- MAJOR alarms identify failures that cause a critical degradation of service. These alarms require immediate attention.
- MINOR alarms identify failures that cause some service degradation but that do not render a crucial portion of the system inoperable. Minor alarms require attention. However, a minor alarm typically affects only a few trunks, stations, or a single feature.
- WARNING alarms identify failures that cause no significant degradation of service or equipment failures external to the switch. These failures are not reported to INADS or to the attendant console.
- ON-BOARD problems originate in the circuitry on the alarmed Media Module or circuit pack.
- OFF-BOARD problems originate in a process or component that is external to the Media Module or circuit pack.

Background Terms

Table 1: Alarming Background Terms gives an explanation of terms used in this document.

Table 1: Alarming Background Terms ***1 of 2***

Term	Explanation
TRAP	An event notification that is sent to the SNMP trap manager and received from the Media Gateway Processor, Layer 2 Switching Processor, or RTCP Monitor (Avaya VisAbility).
ALARM	If a trap is determined to be an alarm, it is sent to an appropriate alarm management site such as INADS.
INADS	The Initialization and Administration System is a software tool used by Avaya services personnel to initialize, administer, and troubleshoot customer communications systems remotely.
SNMP	Simple Network Management Protocol, the industry standard protocol governing network management and the monitoring of network devices and their functions.
RTCP	Real Time Control Protocol, contained in IETF RFC 1889.
	1 of 2

Table 1: Alarming Background Terms ***2 of 2***

Term	Explanation
ISM	Intelligent Site Manager, a VPN gateway on the customer's LAN that provides a means for services personnel to access the customer's LAN in a secure manner via the Internet.
VPN	Virtual Private Network, a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.
	2 of 2

Alarm Content

Alarms can be viewed via the Web Interface, CLI, and SAT command-line interface.

Alarms logged by Communication Manager are stored in an alarm log. The following is an example of a server alarm in the syslog:

20070606:012435000:36096:lxsys:MED:volunteer-srv1 :
>#2,YY,ACT,001,MED-GTWY,n,MAJ,MAJ,N,06/06:01:24:35,none,1,0x0:0x1:5156:31004:!#

When the command **`almdisplay`** is entered on the server command line, the information from the text string is displayed as the following:

```
CommunicaMgr ALARMS
===================

ID   MO          Source      On Bd   Lvl     Ack   Date
1    DLY-MTCE                n       MIN     Y     Fri Jun 08 10:09:07 MDT 2007
2    IPMEDPRO    01A10       y       MIN     Y     Wed Jun 06 09:29:21 MDT 2007
3    MED-GTWY    002         n       MAJ     Y     Wed Jun 06 01:24:35 MDT 2007
4    MED-GTWY    001         n       MAJ     Y     Wed Jun 06 01:24:35 MDT 2007
```

Connection Strategies to a Services Organization

A services organization, such as INADS, receives alarms from the server and connects to the server for troubleshooting. There are currently two product-connect strategies: dialup modem access and Virtual Private Network (VPN) access over the Internet.

For dialup modem access:

1. Connect a USB modem, connected to a telephone line, to the USB port on the faceplate of the server.

2. Enable the modem from the server Web Interface. In addition, use the Setup Modem Interface under the Configure Server pages.
3. With this modem, a client PC uses the Point-to-Point Protocol (PPP) to access the server and connect via telnet to a Linux shell.
4. Once logged into the server, you can telnet out to media gateways such as the G700, and other devices on the network.

   Note:

   > Additionally, this modem can be used to allow the server to call out to the INADS or other alarm receiving system to report alarms. When performing remote diagnostic tests, Services personnel should disable alarm call-outs to INADS to avoid generating unnecessary alarms. Alarm suppression is released after 30 minutes. If you are remotely logged in through the modem, you prevent alarms from being sent because you are using the modem, but you do not prevent an alarm noting the absence of alarm reporting service being logged at the alarm receiving site.

The VPN alternative is achieved by the use of the Intelligent Site Manager (ISM) application. The ISM is a VPN gateway that resides on the customer's LAN and provides a means for services personnel to gain access to the customer's LAN in a secure manner over the Internet. Telnet is then used to access the server and/or media gateways and other IP network equipment.

Alarms in Linux Servers

A Linux-based server can be configured to serve as the trap collector and provide external alarm notification.

For events that require external notification, one option is to call the Avaya technical service center's INADS (Initialization and Administration System). Other options include sending an e-mail to specified destinations or sending an SNMP trap to a specified network management address.

The server has an SNMP trap manager that collects traps from:

- Uploads and downloads to media modules
- VoIP Media Modules
- VoIP engines on media gateway motherboards
- Media gateway-associated UPS systems

Server alarms perform a similar role to Communication Manager alarms in a traditional telephony context. Server alarms:

- Comprise related sets of alarms
- Create an internal record of actual or potential problems

- Notify maintenance personnel of a problem
- Help isolate the source of the problem
- Point to and facilitate local and remote resolution of a problem

Note:

> If a user is logged into a server by an analog modem that is also the server's only alarm-reporting interface, enter **`almsuppress`** on the Linux command line to suppress alarm reporting. Otherwise, the other server logs an occurrence of SME Event ID #1 (see Table 27: SME Alarms).

Clearing Server Alarms

Unlike a Communication Manager alarm, which cannot be cleared unless it is also resolved, a server alarm:

- Can be manually cleared from its log, with the **`almclear`** Linux command
- Should not be considered resolved until it is actually repaired

Displaying Server Alarms

In the following sections, each server alarm is described and its resolution procedure is provided. Like traditional Communication Manager maintenance objects, the 3-column table for each server MO shows an alarm's:

1. Event ID
2. Severity
3. Definition, probable cause, and troubleshooting procedure

To help isolate a server problem, the 3rd column of these tables begins with quoted text for each event (unlike traditional Communication Manager MOs). The text consists of the verbose (-v) output of the **`almdisplay -v`** Linux command. For example, "interchange hand off failed" is the quoted text for Arbiter's Event ID #3.

If the **`almdisplay`** command returns a failure message, such as:
almdisplay: 4: Unable to connect to MultiVantage
enter the **`man almdisplay`** Linux command for command-related information.

Linux Server Alarms

Server-related alarms and their troubleshooting procedures are described in the following sections:

- ARB (Arbiter)
- DAJ1/DAL1/DAL2 (Duplication Memory Board)
- DUP (Duplication Manager)
- ENV (Environment)
- ESS (Enterprise Survivable Server)
- FSY (File Synchronization)
- GAM (Global Alarm Manager)
- HARD DISK (Hard Disk Drive)
- Login Alarms
- _MP (Maintenance Processor)
- NIC (Network Interface Card)
- RMB (Remote Maintenance Board)
- SME (Server Maintenance Engine)
- STD (Standard SNMP Traps)
- SVC_MON (Service Monitor)
- _TM (Translation Manager)
- TlsManager
- UPG (Upgrade)
- UPS (Uninterruptible Power Supply)
- USB1 (Modem)
- _WD (Watchdog)
- S8710 ENV Alarms
- S8710 Server BIOS Error Messages

ARB (Arbiter)

The Arbiter process runs on S8700-series servers to:

- Decide which server is healthier and more able to be active
- Coordinate data shadowing between servers under the Duplication Manager's control

At the physical and data-link layers, three links may serve as redundant inter-arbiter UDP communication paths: the control network A link, the control network B link (if present), or an Ethernet-based duplication link. Two of these links must be present. The redundant inter-arbiter UDP communication paths are used to:

- Enable arbitration between the active and standby servers
- Provide the necessary status signaling for memory refreshes

All inter-arbiter communication links use triple DES encryption for secure communication and control.

Table 2: ARB Alarms describes the Arbiter's alarms and their troubleshooting procedures. See DUP (Duplication Manager) for more information.

Table 2: ARB Alarms *1 of 10*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
3	MIN	"Interchange handoff failed" — The standby server could not process the active server's interchange request. The interchange does not occur, and the active side remains active. Follow steps 1 - 4 if using the Web interface. Follow steps 5 - 8 if using the Linux Command Line Interface. 1. **Using the Web Interface**: From the Web interface's **Server** section, select **View Summary Status** to see if the standby side is RESET. 2. Manually clear the alarm by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** 3. If the problem persists, troubleshoot the standby server: a. Check if the standby side is RESET. From the Web interface's **Server** section, select **View Summary Status** b. Check for application problems by selecting **View Process Status** and restore any applications with problems. c. Check for problems with an Ethernet interface by selecting the **Execute Pingall** diagnostic. Check both sides of each failed link, and make any necessary repairs. 4. If the applications and interfaces are okay **but** the problem persists, escalate the problem. 5. **Using the Linux Command Line Interface**: Enter `server` and check if the standby side is RESET. 6. Enter `almclear -n #id` to manually clear the alarm. 7. If the problem persists, troubleshoot the standby server: a. Enter `server` and check if the standby side is RESET. b. Enter `statapp` and check for application problems. Restore any applications with problems. c. Check for problems with an Ethernet interface by entering `pingall -a.` Check both sides of each failed link, and make any necessary repairs. 8. If the applications and interfaces are okay **but** the problem persists, escalate the problem.
		1 of 10

Table 2: ARB Alarms ***2 of 10***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
7	MAJ	“Arbiter in invalid/unknown state” — Memory corruption or bad code/build 1. Verify that the server’s state is “Corrupt!” by entering the following commands on the Linux command line: **`server`** **`stop -Sf -s arbiter`** **`start -s arbiter`** **`server -c`** If the output no longer shows "Mode: Corrupt!", then the problem has been fixed. Otherwise, proceed to step 2. 2. Compare the suspected `arbiter` with the one in `/root2`. Enter the following Linux command to display the arbiter’s version string: **`/opt/ecs/sbin/acpfindvers /opt/ws/arbiter`** Enter the following command to run a cyclical redundancy check (CRC) against the arbiter and display both the CRC output value and the number of bytes in the arbiter file: **`/sbin/cksum /opt/ws/arbiter`** 3. If the two `arbiter` files differ: a. Get a fresh copy of `arbiter` from the CD. b. Manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***#id*** 4. If the `arbiter` file is OK **or** the problem persists, escalate the problem.
2 of 10		

Table 2: ARB Alarms ***3 of 10***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
8	MIN	“Both servers thought they were active". 1. **If using the Web Interface**: a. From the Web interface’s **Server** section, select **View Summary Status** and verify that both servers are active. b. To distinguish the cause, examine the trace logs for Interarbiter messages with timestamps shortly before to shortly after the loss of heartbeat by 1. Selecting the **View System Logs** diagnostic and **Logmanager Debug** trace 2. Specifying the **Event Range** for the appropriate time frame 3. Matching the **Interarb** pattern c. Depending on the cause, continue with either Step 3 or Step 4. **2. If using the Linux command line:** a. Enter `server` and verify that both servers are active. b. To distinguish the cause, examine the trace logs for Interarbiter messages with timestamps shortly before to shortly after the loss of heartbeat by entering `logv -t ts` c. Depending on the cause, continue with either Step 3 or Step 4.
		3 of 10

Table 2: ARB Alarms *4 of 10*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
8 (cont'd)	MIN	3. A high-priority process caused the active Arbiter to hang for at least 4.1 seconds, causing an interchange. Each Arbiter then realized that the other had assumed the active role. An automatic resolution process should leave the newly active server active, while the other server backs down to the standby role. a. If one server is active and the other is standby, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n #id`** b. If the problem recurs, escalate the problem. 4. Every Interarbiter link is down or mis-configured. a. Check for problems with an Ethernet interface, either from the: - Web interface, by selecting the **Execute Pingall** diagnostic - Linux command line, by entering **`pingall -a`** Check both sides of each failed link, and make any necessary repairs. b. If the links are OK **but** the problem persists, escalate the problem.
9	WRN	<SOH (state-of-health) string> — ***Before*** an interchange, the standby server is ***significantly*** healthier than the active server requesting the interchange. (The active server is probably unable to sustain call processing.) **Understanding ARB Event #9's String Pairs** ARB Event #9 generates pairs of SOH strings, where in each string pair, the: • 1st string represents the active • 2nd string represents the standby server's SOH just ***before*** an interchange. Since – (unless prevented by external circumstances) – Event 9 triggers a server interchange, the 1st string normally represents the less healthy server – which became the standby. So, the 1st string's data is usually more pertinent.
4 of 10		

Table 2: ARB Alarms ***5 of 10***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation

9
(cont'd)
	WRN	The following is a sample string pair generated by ARB Event #9. Within this sample, four pairs of digits in each string have special meaning, and are labeled “aa” through “dd.”
		`     aa     bb cc           dd`
		`     ↓↓     ↓↓ ↓↓           ↓↓`
		`gmm 0700, pcd 00/00, dup 270, wd 81, actv 004`
		`gmm 0700, pcd 06/06, dup 370, wd 01, actv 014`
		• For “aa,” any value other than “00” indicates a hardware problem. (For example, the value “20” is common for a power failure.)
		In the above example, neither server had hardware trouble.
		• “bb” and “cc”: Here, "bb" indicates the number of IPSI’d PNs that the server in question controls (if active) or is prepared to control (if standby), and "cc" indicates the number of connections to PNs with IPSIs. For non-ESS servers, different values within the ***same*** string indicate a problem with controlling one or more IPSI-connected PNs.
		A PN reset can cause both server’s strings to reflect equally degraded health, but that event (in itself) should not trigger a server interchange.
		• For “dd,” any value other than “01” indicates a failed software process. (More precisely, a certain value indicates a problem with a discrete portion of the platform’s process set, including:
		- “21” for a Linux daemon (for example, “atd”, “httpd”, “inetd”, or “xntpd”)
		- “41” for a platform service (for example, “dbgserv”, “prune”, or “syslog”)
		- “81” for reloaded Communication Manager software, as in the previous sample

		5 of 10

Table 2: ARB Alarms ***6 of 10***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
9 (cont'd)	WRN	**Troubleshooting ARB Event #9** 1. compare the health of both servers, either from the: - Web interface's **Server** section, by selecting **View Summary Status** - Linux command line, by entering **`server`** 2. Using the output from Step 1, check the health of each server's individual processes. 3. Check the health of the ***active*** server's individual processes, either from the: - Web interface, by selecting **View Process Status** - Linux command line, by entering **`statapp`** and restore any applications with problems. 4. See if the standby side is RESET, either from the: - Web interface's **Server** section, by selecting **View Summary Status** - Linux command line, by entering **`server`** 5. Check the health of the ***standby*** server's individual processes, either from the: - Web interface, by selecting **View Process Status** - Linux command line, by entering **`statapp`**, and restore any applications with problems. 6. Check for problems with an Ethernet interface, either from the: - Web interface, by selecting the **Execute Pingall** diagnostic - Linux command line, by entering **`pingall -a`** Check both sides of each failed link, and make any necessary repairs. On the Linux command line, enter **`ifconfig -a`** Ensure the IP addresses match /etc/opt/ecs/servers.conf and /etc/hosts, and check that all ethernet ports have been assigned IP addresses. Enter **`/sbin/arp -a`** to ensure that no MAC addresses of "incomplete" appear. 7. If the standby's applications and interfaces are OK **but** the problem persists, escalate the problem.
		6 of 10

Table 2: ARB Alarms ***7 of 10***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
9 (cont'd)	WRN	***After*** the interchange, the newly active server's health should be significantly better than the standby server's. See the SOH values "bb" and "cc" as defined above. The server with the larger "bb" value is generally considered more healthy. If there is a tie, the server with the larger "cc" value is more healthy. If the newly active server's health is significantly better than the standby server's, troubleshoot the standby server. If the newly active server's health is **not** significantly better: 1. Manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering `almclear -n` ***`#id`*** 2. If the problem recurs, escalate the problem.
11	WRN	"Cannot create receive socket;" "Cannot create transmit socket;" "Cannot bind receive socket;" "Cannot (re)bind send socket" Since the Arbiter continuously attempts to create or bind the socket, the problem may resolve itself. Once resolved, the Arbiter can send and receive across every Interarbiter link (no subsequent error messages in the trace log). 1. Examine the alarm log to distinguish between a: Bind or create problem Send or receive socket problem by accessing either the: - Web interface, by: a. Selecting **Alarms and Notification** and the appropriate alarm b. Selecting the **View System Logs** diagnostic c. Selecting the **Logmanager Debug** trace d. Specifying the **Event Range** for the appropriate time frame e. Matching the "cannot create" pattern - Linux command line, by entering `almdisplay -v`
		7 of 10

Table 2: ARB Alarms ***8 of 10***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
11 (cont'd)	WRN	2. Check for both the completeness and consistency of the servers' `hosts` and `servers.conf` files (containing IP addresses of the system's configured components), either from the: - Web interface, by selecting **Configure Server** - Linux command line, by entering: **`more /etc/hosts`** **`more /etc/opt/ecs/servers.conf`** The Arbiter uses port number 1332 for sockets. Enter **`netstat -a | grep 1332`** to see if the alarm is still active. The output should look something like: upd 0 0<server-name>-cnb:1332 *.* upd 0 0<server-name>-cna:1332 *.* upd 0 0<server-name>-dup:1332 *.* 3. If the IP addresses agree and there are no alarms for port 1332, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`*** 4. If this problem affects call processing **or** if the problem persists, continue with Step 5. If **not**, continue only at the customer's convenience. 5. **Escalate** this problem for explicit guidance with Steps 5a through 6. a. Enter **`server`** to verify that the suspected server is the standby. b. If **not**, enter **`server -if`** to force a server interchange. Busy out the standby server from the Linux command line, by entering **`server -b`**. c. Reboot the server (as the standby), either from the: - Web interface, by selecting **Shutdown This Server** - Linux command line, by entering **`/sbin/shutdown -r now`** 6. If rebooting the standby does not help **or** if the problem recurs, escalate the problem to the next higher tier.
		8 of 10

Table 2: ARB Alarms ***9 of 10***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
12	MIN	"Interchange without doing prep" — Since the Arbiter could not create a thread to request a file synchronization, some files did not get shadowed. 1. Examine the trace logs for the entry, `Can't create interchange-prep thread`, either from the: - Web interface by: a. Selecting the **View System Logs** diagnostic and **Logmanager Debug** trace b. Specifying the **Event Range** for the appropriate time frame c. Matching the "interchange-prep" pattern - Linux command line, by entering **`logv -t ts`** 2. Resubmit any translation changes using the **`save_trans`** command. 3. Manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
		9 of 10

Table 2: ARB Alarms ***10 of 10***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
13	MIN	“Heartbeat timeout from ACTIVE” — There are two possible causes for this event: • An unexplained Linux lock-up that starved CPU cycles from all Communication Manager processes for more than 3.3 seconds • A third main server with a server ID that matches one of the other two main servers was somehow started and is accessible from the network In the case of a Linux lock-up, the problem has already corrected itself by the time the problem has been seen. There is no corrective action to take. To investigate the existence of a third main server: 1. On the Linux command line, enter **`/sbin/arp -a`** to determine the MAC addresses of the alternate server ethernet ports associated with the CNA, CNB, and duplication links. 2. Log into the alternate server and verify that the MAC addresses match. Do this from both servers. 3. If the MAC addresses do not match, there may be a third system in the network posing as a doppelganger, and a network sniffer can be used to find it.
14	MIN	"Standby failed to come back up" - The standby server in a duplex system has been down for longer than 15 minutes. The standby server is not able to alarm on its own behalf. Typical causes are: • Rolling Linux reboots. This in turn could be caused by rolling Communication Manager reloads or by a failure to even start Communication Manager. • A server was powered down (manually or UPS failure) for more than 15 minutes without first being taken out of service (busied out). The correct procedure for doing a "stop" on a standby server is to busy it out first, then stop it. Escalate the problem.
		10 of 10

Back to: Linux Server Alarms

CMG (Common Media Gateway)

See *Gateway Traps for the G250/G350/G450/G700 Avaya Media Gateways, 30-602803* for a description of CMG traps.

DAJ1/DAL1/DAL2 (Duplication Memory Board)

The Duplication Memory boards are a NIC (network interface card) serving as the physical and data-link interface for an Ethernet-based duplication link between the servers. This link provides a call-status data path for sending:

- TCP-based communication between each server's Process Manager
- UDP-based communication between each server's Arbiter to:
  - Enable arbitration between the active and standby servers
  - Provide status signaling for memory refreshes

Note:

The Duplication Memory boards are not interchangeable between servers:

The DAJ1 (256 MB) will only work with S8700-series servers.

The DAL1 (256 MB) will only work with S8710 and S8720 Servers with standard configuration.

The DAL2 (512 MB) will only work with:

- S8730 Servers configured for hardware duplication (factory installed)
- S8720 Servers configured for hardware duplication running Communication Manager 4.0 and later
- S8710 Servers configured for hardware duplication running Communication Manager 5.0 and later

Table 3: DAJ1/DAL1/DAL2 Alarms describes Duplication Memory board alarms and their troubleshooting procedures. See also ARB (Arbiter), DUP (Duplication Manager), and NIC (Network Interface Card).

The Linux command `testdupboard` tests the Duplication Memory Board. This command provides the ability to perform a local loop test and to read error registers. The local loop test can only be run on a busied out standby server. To check the status of the servers, use the `server` command. Enter `man server` to get information on how to busy out a server.

See testdupboard for the command usage and possible errors.

Table 3: DAJ1/DAL1/DAL2 Alarms ***1 of 3***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1	MAJ	"Single bit EDC test (bad err register)" - one or more single bit errors have been detected and corrected on an SDRAM operation. The board automatically corrects these errors. If this condition continues to occur, replace the Duplication Memory board.
		1 of 3

Table 3: DAJ1/DAL1/DAL2 Alarms ***2 of 3***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
2	WRN	“Single-bit EDC test (bad SB error counter)” — Single-bit SDRAM error occurred 20 times. Software automatically clears the single-bit error register. This is a log-only indication of the error’s occurrence. 1. Manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
3	MAJ	“Dup board SDRAM Multibit errors” — Catastrophic multibit SDRAM error occurred. This is usually due to a hardware problem. 1. Enter ***`testdupboard`*** on the Linux command line. 2. If the test fails, **escalate** this problem for explicit guidance with Steps 3 through 5. 3. Power-cycle the server. 4. Enter **`testdupboard`** again. 5. If the test still fails, replace the server.
4	MIN	“Local Looparound test failure” — On-demand local loop test failed 3 times. (Cannot read from or write to duplication memory board buffers.) The Local Looparound test only runs on a busied-out standby server. 1. If the on-demand test is failing but a running duplicated system has **no** problems, do nothing. If the running duplicated system has problems, continue with Step 2 2. Enter **`testdupboard -l`** on the Linux command line. 3. If the test fails, **escalate** this problem for explicit guidance with Steps 4 through 6. 4. Power-cycle the server. 5. Enter **`testdupboard`** again. 6. If the test still fails, replace the server.
		2 of 3

Table 3: DAJ1/DAL1/DAL2 Alarms ***3 of 3***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
5	MIN	“Optical Link Receiver CRC errors” — Received multiple CRC errors across the fiber link. 1. Run **`testdupboard`** on both servers. 2. If CRC errors are occurring on both servers, it may be a: • Likely problem with the fiber link • Far less likely problem with both Duplication Memory boards If **not**, the other server’s Duplication Memory board may be faulty. 3. If the running system has duplication-related problems, **escalate** this problem to replace the server. If **not**, ignore and clear the alarm.
6	MAJ	"Fail to open Dup board card" - The Duplication Memory board is missing or the software driver for the Duplication Memory board is not installed. On a new server, either the software configuration is incorrect, or the Duplication Memory board has failed.
		3 of 3

testdupboard

Table 4: testdupboard command syntax describes the command usage and possible errors for the **`testdupboard`** command.

Table 4: testdupboard command syntax

Syntax: `testdupboard [-s | -l] | [-t arg] | [-?]`	
Argument	**Description**
none	Performs the Read Error Register Test.
`-s`	Short test. Performs the Read Error Register Test. This is also the default option
`-l`	Performs the Read Error Register Test and the Duplication Memory Board Local Loop Test
`-t arg`	Specific test to perform. The values for `arg` are: • `read_err_reg` to run the Read Error Register Test • `localloop` to run the Duplication Memory Board Local Loop Test
`-?`	Display the usage statement.
`The following errors may occur:`	
`1`	**Requested tests must be run on a busied out, standby server.** Use the `server` command to busyout a server.
`3`	**Failed to create socket** Command could not allocate a system resource. Wait a minute, then try again.
`4`	**Failed to connect to SME** Command could not connect to the server. Verify that both the Server Maintenance Engine (SME) and Communication Manager are UP by entering the command `statapp` on the server.
`5`	**Failed to send request to SME** Request could not be sent to the server. Verify that both the Server Maintenance Engine (SME) and Communication Manager are UP by entering the command `statapp` on the server.
`6`	**Failed to receive response from SME** The test did not receive a response from the server. Verify that both the Server Maintenance Engine (SME) and Communication Manager are UP a by entering the command `statapp` on the server.

Read Error Register Test

The Read Error Register test queries three registers, then clears them. The registers are:

- Optical line receiver’s CRC error register

  CRC errors indicate problems with the optical interface between the active and standby servers.

- SDRAM’s single-bit error register

  Although the Duplication Memory board can “self heal” single-bit errors in the SDRAM’s error register, chronic problems can indicate a more serious problem.

- SDRAM’s multiple-bit error register

  An SDRAM multiple-bit error condition indicates a problem in the Duplication Memory board’s memory.

The first time **`testdupboard`** is run after a boot or after a certain amount of time, a false FAIL may occur. This may be caused by the command reporting errors and clearing error registers in the duplication memory boards, not from a board error.

Repetitive testdupboard failures indicate problems with the duplication memory board.

The following errors can be detected:

Table 5: Read Error Register Test

Error	Test Result	Description / Recommendation
Open failed to MDD	ABORT	The Memory Duplication Driver (MDD) is the system driver that communicates with the duplication memory board. If this driver cannot be opened, then the duplication memory board’s registers cannot be read. 1. This is a system error, try again.
System Error Dup Memory driver failed to return data	ABORT	The test ran, but for some reason, the MDD could not return data. 1. This is a system error, try again.
Dup board err count query, code=? ?= 1 to 7	FAIL	Code 1 - Single-bit errors occurred. Code 2 – CRC errors occurred. Code 3 - Single-bit and CRC errors occurred. Code 4– Multiple-bit errors occurred. Code 5 - Multiple-bit and Single-bit errors occurred. Code 6 - Multiple-bit and CRC errors occurred. Code 7 - Multiple-bit, Singe-bit, and CRC errors occurred.
Failed to open Dup Memory Board	FAIL	This may be a system error or a problem with the Duplication Memory Board. Try the command again. If the test continues to fail, escalate the problem.

Duplication Memory Board Local Loop Test

Note:

This test runs only if the standby server is busied out.

This test runs a local looparound test on the duplication memory board of the standby server. A 32-bit data number is written to an address and verified for correct transmission. The test reads the contents of the last data received registers and the last address received register, and then compares the data. If the data matches, the test passes. If not, the test fails.

The following errors can be detected:

Table 6: Duplication Memory Board Local Loop Test

Error	Test Result	Description / Recommendation
Open failed to MDD	ABORT	The MDD is the system driver that communicates with the Duplication Memory board. If this driver cannot be opened, the board's registers cannot be read.
Wrong Hardware for this test	ABORT	Verify that the correct Duplication Memory Board is inserted in the system.
Looparound test failed	FAIL	The last address received does not match the address that was written, or the last data received does not match the data that was written.

Back to: Linux Server Alarms

DUP (Duplication Manager)

The Duplication Manager process, via coordination of the Arbiter process, runs on the servers to control data shadowing between them.

At the physical and data-link layers, an Ethernet-based duplication link provides a TCP communication path between each server's Duplication Manager to enable their control of data shadowing. This TCP/IP link provides the actual data shadowing for software duplication. For hardware duplication, there is an additional fiber optic link between the duplication memory boards that provides the data shadowing.

Table 7: DUP Alarms describes the Duplication Manager's alarms and their troubleshooting procedures.

See ARB (Arbiter) and DAJ1/DAL1/DAL2 (Duplication Memory Board) for more information.

Table 7: DUP Alarms *1 of 4*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1	MAJ	"Duplication card error" — The Duplication Manager determined that the duplication card is not functioning, but it cannot distinguish between a bad card, an unplugged card, or a bad fiber link. Follow steps 1 - 7 if using the Web Interface. Follow steps 8 - 14 if using the Linux command line interface. 1. **Using the Web Interface**: Check the physical fiber connectivity at each server. 2. Verify the alarm by accessing the trace log by: a. Selecting the **View System Logs** diagnostic and **Logmanager Debug** trace b. Specifying the **Event Range** for the appropriate time frame c. Matching the "dup" pattern 3. Examine the trace-log query's output for one of these messages: "glbi: couldn't open Dup Card, errno=<#>. ndm exiting" "glbi: mmap failed, errno=<#>. ndm exiting" "Haven't heard from active dupmgr. Dup fiber link down." "san_check_rsp() FAILED: Dup Fiber link down." 4. See if the dup link is **both** "up" and "refreshed" from the Web interface's **Server** section by selecting **View Summary Status** 5. If **so**, manually clear the alarm by selecting **Alarms and Notification**, the appropriate alarm, and **Clear**
		1 of 4

Table 7: DUP Alarms *2 of 4*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1 (cont'd)	MAJ	If **not:** Since the following commands cause a brief service outage, they should *only* be executed at the customer's convenience: a. Force a server interchange to make the suspected server standby by selecting **Interchange Servers** b. Busy out the standby server by selecting **Busy Server** c. Release the standby server by selecting **Release Server** 6. If the problem persists, try: a. Replacing the fiber between the two servers b. Rebooting the standby server 7. If the problem continues to persist, **escalate** for a probable server replacement. 8. **Using the Linux Command Line Interface**: Check the physical fiber connectivity at each server. 9. Enter **`logv -t ts`** to verify the alarm by accessing the trace log. 10. Examine the trace-log query's output for one of these messages: "glbi: couldn't open Dup Card, errno=<#>. ndm exiting" "glbi: mmap failed, errno=<#>. ndm exiting" "Haven't heard from active dupmgr. Dup fiber link down." "san_check_rsp() FAILED: Dup Fiber link down." 11. Enter **`server`** and check if the dup link is **both** "up" and "refreshed". 12. If **`so`**, manually clear the alarm by entering **`almclear -n`** ***`#id`*** If **not:** Since the following commands cause a brief service outage, they should *only* be executed at the customer's convenience: a. Enter **`server -if`** and select the **`force`** option to force a server interchange and make the suspected server standby. b. Enter **`server -b`** to busy out the standby server. c. Enter **`server -r`** to release the standby server. 13. If the problem persists, try: a. Replacing the fiber between the two servers b. Rebooting the standby server 14. If the problem still persists, **escalate** for a probable server replacement.
		2 of 4

Table 7: DUP Alarms ***3 of 4***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
2	MAJ	"Duplication link down" — One server's Duplication Manager cannot communicate with the other server's Duplication Manager. Follow steps 1 - 5 if using the Web Interface. Follow steps 6 - 10 if using the Linux Command Line Interface. 1. **Using the Web Interface**: Access the trace log by a. Selecting the **View System Logs** diagnostic and **Logmanager Debug** trace b. Specifying the **Event Range** for the appropriate time frame c. Matching the "ndm" or "DUPLICATION" pattern 2. Examine the trace-log query's output for one of these messages: "mainlp: get_addrs returned ***. Could not get IP address for other server. Verify name and address in servers.conf. ndm exiting." "san_check_msg() sync_msg failed: DUPLINK DOWN." 3. Check if the dup link is "up" from the Web interface's **Server** section by selecting **View Summary Status** 4. If **so**, manually clear the alarm by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** If **not**, check the duplication interface's Ethernet connectivity by selecting the **Execute Pingall** diagnostic 5. If `pingall` passes, check the other server's applications by selecting **View Process Status**
3 of 4		

Table 7: DUP Alarms *4 of 4*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
2 (cont'd)	MAJ	6. **Using the Linux Command Line Interface**: Access the trace log by entering `logv -t ts` 7. Examine the trace-log query's output for one of these messages: "mainlp: get_addrs returned ***. Could not get IP address for other server. Verify name and address in servers.conf. ndm exiting." "san_check_msg() sync_msg failed: DUPLINK DOWN." 8. Enter `server` and check if the dup link is "up". 9. If **so**, manually clear the alarm by entering `almclear -n` ***`#id`*** If **not**, check the duplication interface's Ethernet connectivity by entering `pingall -d` 10. If `pingall` passes, enter `statapp` and check the other server's applications.
3	MAJ	Duplication Card Error - Double Bit SDRAM error. This alarm is usually seen on the active server and indicates a potential problem with the duplication card on that server. 1. If the alarm occurs multiple times, replace the duplication card.
4	MAJ	Duplication Card Error - Double Frame CRC error. This alarm is usually seen on the standby server and indicates a possible problem with the fiber link between the servers. 1. If the alarm occurs multiple times, replace the fiber link. 2. If the alarm still occurs after replacing the fiber link, there might be a problem with one of the duplication cards. **Escalate** for a probable server replacement.
		4 of 4

Back to: Linux Server Alarms

ENV (Environment)

The ENV environmental maintenance objects are monitored within the server. These include temperature, voltages, and fans.

Event ID’s with an Alarm Level of RES indicate that the problem has been cleared.

Table 8: ENV Alarms ***1 of 14***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1	MIN	“Temperature reached Warning Low” — Motherboard's temperature reached a warning low level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering `environment` 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering `almclear -n #id`
2	MAJ	“Temperature reached Critical Low. Value = xx0C” — Motherboard's temperature reached a critically low level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering `environment` 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering `almclear -n #id`
		1 of 14

Table 8: ENV Alarms ***2 of 14***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
3	WRN	“Temperature reached Warning High. Value = xx0C” — Motherboard's temperature reached a warning high. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering `environment` 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering `almclear -n #id`
4	MAJ	“Temperature reached Critical High. Value = xx0C” — Motherboard's temperature reached a critically high level. 1. Look for any obstructions blocking the server’s fans. 2. Check for any fan alarms, and clear those alarms. 3. Shut down and restart the system. 4. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering `environment` 5. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear**. - Linux command line, by entering `almclear -n #id`
		2 of 14

Table 8: ENV Alarms ***3 of 14***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
5	MIN	"+3.3 voltage reached Warning Low" — Motherboard's nominal +3.3 voltage reached a warning low level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
6	MAJ	"3.3 Voltage reached Critical Low. Value = x.y" — Motherboard's nominal +3.3 voltage reached a critically low level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
7	MIN	"3.3 voltage reached Warning High" — Motherboard's nominal +3.3 voltage reached a warning high level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
		3 of 14

Table 8: ENV Alarms ***4 of 14***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
8	MAJ	"3.3 Voltage reached Critical High. Value = x.y" — Motherboard's nominal +3.3 voltage reached a critically high level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
9	MIN	"+5 voltage reached Warning Low" — Motherboard's nominal +5 voltage reached a warning low level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
10	MAJ	"5 Voltage reached Critical Low. Value = x.y" — Motherboard's nominal +5 voltage reached a critically low level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
		4 of 14

Table 8: ENV Alarms *5 of 14*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
11	MIN	“+5 voltage reached Warning High” — Motherboard's nominal +5 voltage reached a warning high level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering `environment` 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering `almclear -n #id`
12	MAJ	“5 Voltage reached Critical High. Value = x.y” — Motherboard's nominal +5 voltage reached a critically high level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering `environment` 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering `almclear -n #id`
13	MIN	“+12 voltage reached Warning Low” — Motherboard's nominal +12 voltage reached a warning low level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering `environment` 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and Clear - Linux command line, by entering `almclear -n #id`
		5 of 14

Table 8: ENV Alarms ***6 of 14***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
14	MAJ	“+12 Voltage reached Critical Low. Value = x.y” — Motherboard's nominal +12 voltage reached a critically low level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering `environment` 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and Clear - Linux command line, by entering `almclear -n #id`
15	MIN	“+12 voltage reached Warning High” — Motherboard's nominal +12 voltage reached a warning high level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering `environment` 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and Clear - Linux command line, by entering `almclear -n #id`
16	MAJ	“+12 Voltage reached Critical High. Value = x.y” — Motherboard's nominal +12 voltage reached a critically high level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering `environment` 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering `almclear -n #id`
		6 of 14

Table 8: ENV Alarms ***7 of 14***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
17	MIN	"-12 voltage reached Warning Low" — Motherboard's nominal -12 voltage reached a warning low level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
18	MAJ	"-12 voltage reached Critical Low. Value = x.y" — Motherboard's nominal -12 voltage reached a critically low level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
19	MIN	"-12 voltage reached Warning High" — Motherboard's nominal -12 voltage reached a warning high level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
		7 of 14

Table 8: ENV Alarms ***8 of 14***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
20	MAJ	“-12 Voltage reached Critical High. Value = x.y” — Motherboard's nominal -12 voltage reached a critically high level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
21	MIN	“CPU Core Voltage reached Warning Low” — Motherboard's CPU core voltage reached a warning low level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
22	MAJ	“CPU Core Voltage reached Critical Low” — Motherboard's CPU core voltage reached a critically low level. 1. Check the syslog file for any additional log entries. Software cannot tell if the voltage is low or not there (disconnected). 2. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 3. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
		8 of 14

Table 8: ENV Alarms ***9 of 14***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
23	MIN	"CPU Core Voltage reached Warning High" — Motherboard's CPU core voltage reached a warning high level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
24	MAJ	"CPU Core Voltage reached Critical High" — Motherboard's CPU core voltage reached a critically high level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
25	MIN	"CPU I/O Voltage reached Warning Low" — Motherboard's CPU I/O voltage reached a warning low level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
		9 of 14

Table 8: ENV Alarms *10 of 14*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
26	MAJ	"CPU I/O Voltage reached Critical Low" — Motherboard's CPU I/O voltage reached a critically low level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
27	MIN	"CPU I/O Voltage reached Warning High" — Motherboard's CPU I/O voltage reached a warning high level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
28	MAJ	"CPU I/O Voltage reached Critical High" — Motherboard's CPU I/O voltage reached a critically high level. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
		10 of 14

Table 8: ENV Alarms ***11 of 14***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
29	MAJ	"All fans fail alarm" — Every fan is running at a critically low speed. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
30 S8500B S8500C	MIN	+1.5 voltage reached Warning Low. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
31 S8500B S8500C	MAJ	+1.5 voltage reached Critical Low. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
		11 of 14

Table 8: ENV Alarms *12 of 14*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
32 S8500B S8500C	MIN	+1.5 voltage reached Warning High. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
33 S8500B S8500C	MAJ	+1.5 voltage reached Critical High. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
34 S8500B S8500C	MIN	+2.5 voltage reached Warning Low. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
		12 of 14

Table 8: ENV Alarms *13 of 14*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
35 S8500B S8500C	MAJ	+2.5 voltage reached Critical Low. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
36 S8500B S8500C	MIN	+2.5 voltage reached Warning High. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
37 S8500B S8500C	MAJ	+2.5 voltage reached Critical High. 1. See if the alarmed condition is still present, either from the: - Web interface, by selecting the **Temperature/Voltage** diagnostic - Linux command line, by entering **`environment`** 2. If not, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
38 S8510	MAJ	Power supply detected a failure. Sensor location: PS 1
39 S8510	MAJ	Power supply detected a failure. Sensor location: PS 2
		13 of 14

Table 8: ENV Alarms ***14 of 14***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
40 G450	MAJ	G450 Fan Tray 1. There is a problem with the fan tray on the G450. Reinsert or replace the fan tray.
41 G450	MAJ	G450 Power Supply #1. 1. There is a problem with Power Supply #1 on the G450. Reinsert or replace Power Supply #1.
42 G450	MAJ	G450 Power Supply 2. 1. There is a problem with Power Supply #2 on the G450. Reinsert or replace Power Supply #2.
		14 of 14

Back to: Linux Server Alarms

ESS (Enterprise Survivable Server)

Table 9: ESS Alarms describes the alarms for ESS.

Table 9: ESS Alarms ***1 of 2***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1	MIN	ESS not controlling IPSI PN XX: cls RRR 1. Server of cluster RRR is not controlling IPSI port network XX
2	MIN	ESS controlling IPSI PN XX: cls RRR 1. Server of cluster RRR is controlling IPSI port network XX
3	MIN	ESS not controlling non-IPSI PN XX: cls RRR 1. SErver of cluster RRR is not controlling non-IPSI port network XX
4	MIN	ESS controlling non-IPSI PN XX: cls RRR 1. Server of cluster RRR is controlling non-IPSI port network XX
5	MIN	ESS not registered cls YYY: cls RRR 1. ESS cluster ID YYY is not registered to active server of the main cluster. The main active server can send this trap for each ESS in the system (RRR != YYY). An ESS will only report status for itself (RRR = YYY)
6	MIN	ESS registered cls YYY svid ZZZ: cls RRR 1. ESS server ID ZZZ of cluster ID YYY is registered to the active server of the main cluster. The active server of the main cluster can send this trap for each ESS in the system (RRR != YYY). The ESS will only report status for itself (RRR = YYY)
7	MIN	ESS change to disable state: cls RRR 1. ESS cluster RRR has changed to the disabled state.
8	MIN	ESS change to enable state: cls RRR 1. ESS cluster RRR has changed to the enabled state.
		1 of 2

Table 9: ESS Alarms ***2 of 2***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
9	MIN	IPSI (A/B) PN XX disconnected from ESS: cls RRR 1. Server of cluster RRR is not connected to IPSI (A/B) of port network XX. This event is reported by each ESS in the system for all the IPSIs that cluster will connect to, as specified by system administration, i.e. a local only ESS will provide connection event status for the IPSIs assigned tot at ESS's community.
10	MIN	IPSI (A/B) PN XX connected to ESS: cls RRR 1. Server of cluster RRR is connected to IPSI (A/B) of port network XX. This event is reported by each ESS in the system for all the IPSIs that cluster will connect to, as specified by system administration, i.e. a local only ESS will provide connection event status for the IPSIs assigned tot at ESS's community.
		2 of 2

FSY (File Synchronization)

The File Synchronization (FSY) process uses TCP-based communication over 100BaseT Ethernet links to provide synchronized duplication of critical data files, including translations and important Linux files.

Note:

This set of files is separate from the data shadowed between each server's DAJ1/DAL1/DAL2 (Duplication Memory Board).

Table 10: FSY Alarm in Server describes the FSY alarms and their troubleshooting procedures.

Table 10: FSY Alarm in Server

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1	MIN	"File sync failed" — File synchronization operation failed. 1. See if the filesyncd (file sync daemon) process is up, either from the: - Web interface, by selecting **View Process Status** - Linux command line, by entering `statapp` 2. Check the trace log for more granular information. (The file sync daemon can report failures of synchronizing one or more files.) Access the trace log, either from the: - Web interface, by: a. Selecting the **View System Logs** diagnostic and **Logmanager Debug** trace b. Specifying the **Event Range** for the appropriate time frame c. Matching the "file sync failed" pattern - Linux command line, by entering `logv -t ts` 3. (Except S8500) Make sure that the Ethernet duplication link is up, either from the: - Web interface, by selecting the **Execute Pingall** diagnostic - Linux command line, by entering `pingall -a` If **not**, check each side of this failed link, and make any necessary repairs. 4. (Except S8500) Check the physical fiber connectivity at each server to verify that this alarm is not a consequence of other duplication-related problems. 5. If the problem persists, escalate the problem.

Back to: Linux Server Alarms

GAM (Global Alarm Manager)

The Global Alarm Manager determines which events require external alarm notification and notifies the Global Maintenance Manager (GMM).

Table 11: GAM Alarms

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
2	WRN	The GMM is unable to report alarms. The GMM sends out the alarm but never receives any response from INADS. 1. Test the administered reporting mechanisms by entering **`testinads`** on the Linux command line. This test could fail if the modem is bad. 2. If the test fails, enter **`testmodem -l`** on the Linux command line. 3. If the test fails, see Table 36: testmodem command usage for a description of error messages and recommended procedures.

Back to: Linux Server Alarms

GW_ENV (Gateway Environment)

The following alarms apply to the G450 media gateway.

Table 12: GW_ENV Alarms

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1	MAJ	AvEntFanFlt - Fan fault.
2	MAJ	AvEnt48vPwrFlt - 48v Power fault.
3	MAJ	AvEnt5vPwrFlt - 5v Power fault.
4	MAJ	AvEnt3300mvPwrFlt - 3300 mv Power fault.
5	MAJ	AvEnt2500mvPwrFlt - 2500 mv Power fault.
6	MAJ	AvEnt1800mvPwrFlt - 1800 mv Power fault.
7	MAJ	AvEnt1600mvPwrFlt - 1600 mv Power fault.
8	MAJ	AvEntAmbientTempFlt - Ambient temperature fault.
9	MAJ	avEntPhyChFruRemoval - Field replaceable unit removal.
10	MAJ	avEntPhyChFruPsuFlt - Power supply fault.

For the G650 gateway, Communication Manager generates SNMP traps to collect the threshold exception data for the following events:

- Jitter
- Packet Loss
- Round-trip Delay

Communication Manager does not generate any alarm for these events. However, Communication Manager generates a warning and sends it to the Fault and Performance Management (FPM) and/or the Secure Intelligent Gateway (SIG) for Managed Services. The warning message string includes the following information:

- Event Type (for example, Jitter, Packet Loss, and Round-trip Delay)
- Time Stamp of exception (in the month/day/hour:min:sec format)
- Board Type (TN2302 or TN2602)
- Board Location (5 alphanumeric characters)
- Peak threshold level/amount (in decimal notation) for the exceeded threshold

Back to: Linux Server Alarms

HARD DISK (Hard Disk Drive)

The Hard Disk Drive is monitored via the Self Monitoring, Analysis, and Reporting Technology (SMART) capability that is built into the hard disk drive unit. The SMART technology makes status information concerning the disk drive available to monitoring software.

Some hard disk drive problems do not occur suddenly. They are the result of a gradual degradation of disk components. For example, if the value for **Reallocated Event Count** (count of remap operations, both successful and non-successful) for Event ID 21 is going up, it may indicate an impending disk failure. At the very least, it should be monitored closely.

A RAM DISK configuration is used for the Avaya S8500/S8500B/S8500C simplex server and the Avaya S8300B ICC server to support platform reliability during hard disk crashes. Hard drives are among the least reliable hardware components. The RAM DISK feature provides reliable storage for critical resources that are necessary for continued operation in the absence of the hard drive. The server will continue to process calls for up to 72 hours after a hard disk failure has occurred. However, administration additions and changes cannot be made and translations cannot be saved until the hard disk drive has been replaced.

The following tables describe the Hard Disk Event IDs for each server type and their troubleshooting procedures.

Note:

In general, if the alarm severity is MAJ, or MIN, replace the hard drive.

Server Type	Hard Disk Drive Alarm Table
S8300	S8300 and S8500 Hard Disk Drive Alarms
S8300B	SMART Alarms
S8300C	S8300C, S8500B, and S8500C Hard Disk Drive Alarms
S8400	S8400 Hard Disk Drive Alarms
S8500	S8300 and S8500 Hard Disk Drive Alarms
S8500B	S8300C, S8500B, and S8500C Hard Disk Drive Alarms
S8500C	S8300C, S8500B, and S8500C Hard Disk Drive Alarms
S8510	S8510 Hard Disk Drive Alarms
S8710	SMART Alarms
S8720	SMART Alarms
S8730	S8730 Hard Disk Drive Alarms

Table 13: S8300 and S8500 Hard Disk Drive Alarms

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1	MAJ	hda status timeout
2	MAJ	hda drive not ready
3	MAJ	ide0 reset timed out
4	MAJ	hda command given to failed disk
5	WRN	hda BadCRC BadSector
6	WRN	hda SectorIDNotFound
7	WRN	hda Bad Special flag
8	WRN	hda Media type not hard disk
9	WRN	hda Bad device number
10	WRN	hda Block not locked
11	WRN	hda bad access block
12	WRN	hda Ide_set_handler timer
13	WRN	hda Nuking plugged
14	WRN	hda Ide_timer expiry
15	MAJ	hda lost interrupt
16	MAJ	Device Disk has failed
17	MAJ	hda status error
18 - 22		See SMART Alarms

Table 14: S8300C, S8500B, and S8500C Hard Disk Drive Alarms

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1	MAJ	scsi Device offlined not ready
16	SUP	Device Disk has failed
18 - 22		See SMART Alarms

Table 15: S8400 Hard Disk Drive Alarms

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1	MAJ	hdc status timeout status
2	MAJ	hdc drive not ready
3	MAJ	ide0 reset timed out
4	MAJ	hdc command given to failed disk
5	WRN	hdc BadCRC BadSector
6	WRN	hdc SectorIdNotFound
7	WRN	hdc Bad Special flag
8	WRN	hdc Media type
9	WRN	hdc Bad device number
10	WRN	hdc Block not locked
11	WRN	hdc bad access block
12	WRN	hdc Ide_set_handler timer
13	WRN	hdc Nuking plugged
14	WRN	hdc Ide_timer_expiry
15	MAJ	hdc lost interrupt
16	SUP	Device Disk has failed
17	MAJ	hdc status error
18 - 22		See SMART Alarms

Table 16: S8510 Hard Disk Drive Alarms *1 of 2*

Event ID	Alarm Level	Alarm Cause
1	MAJ	Physical drive 1 failed.
2	MAJ	Physical drive 2 failed.
18 - 22		See SMART Alarms
25	MAJ	Physical disk initialization failed.

Table 16: S8510 Hard Disk Drive Alarms ***2 of 2***

Event ID	Alarm Level	Alarm Cause
26	MAJ	Physical disk Rebuild failed.
27	MAJ	SMART configuration change.
28	MAJ	Rebuild completed with error(s).
29	MAJ	The physical disk Clear operation failed.
30	MAJ	Patrol Read found an uncorrectable media error.
31	MAJ	A block on the physical disk has been punctured by the controller.
32	MAJ	Hot spare SMART polling failed.
33	MAJ	Bad block table is full. Unable to log block.
34	MAJ	The rebuild failed due to errors on the source physical disk.
35	MAJ	The rebuild failed due to errors on the target physical disk.
36	MAJ	A bad disk block could not be reassigned during a write operation.
37	MAJ	Unrecoverable disk media error during the rebuild or recovery operation.

Table 17: S8730 Hard Disk Drive Alarms

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1	MAJ	Physical drive 1 failed. 1. Replace the hard drive.
2	MAJ	Physical drive 2 failed. 1. Replace the hard drive.
3	MAJ	Physical Drive Status Change Slot 3 Port 1I Box 1 Bay 2 Status is now Predictive Failure 1. The Hard Disk Drive in Bay 2 has failed. The drive is being used but it needs to be replaced. Replace the hard disk drive.
4	MAJ	Physical Drive Status Change Slot 3 Port 1I Box 1 Bay 1 Status is now Predictive Failure 1. The Hard Disk Drive in Bay 1 has failed. The drive is still being used but needs to be replaced. Replace the hard disk drive.
5	WRN	Rebuild aborted write error Logical drive 0 Port: 1I Box: 1 1. The Hard Disk Drive that is being rebuilt has failed. Refer to /var/log/messages for log entries to find the exact Hard Disk Drive that has failed while being rebuilt. 2. Replace the Hard Disk Drive.
6 7	MIN MIN	Recovery of logical drive configured on was aborted Logical drive uncorrected read error between logical block 1. Check syslog entries to get the exact disk that failed. The disk failed while it was being rebuilt. 2. Unplug and re-plug the affected disk. Re-plugging the disk causes it to rebuild. This takes about 30 minutes. 3. After 30 minutes, check if the error occurred again. If it did, replace the disk. If it did not, the disk is working properly.
8	MAJ	Logical drive I/O request fatal error 1. Check syslog entries to determine the exact disk drive that failed. 2. Replace the failed hard disk drive.
18 - 22		See SMART Alarms

Table 18: SMART Alarms ***1 of 5***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
18	MAJ	ide0 reset master error 1. The hard disk drive has failed. Replace the hard disk drive.
19	WRN	Device: device_name, Failed attribute: attr_number 1. The attribute has exceeded its threshold value. The user very likely has a drive problem and should definitely consider replacing the drive.
20	WRN	Device: device_name, Read Smart Values Failed 1. The SMART utility was unable to read the current SMART values or thresholds for the drive. This may result in SMART not executing and the values that are reported may be stale (or outdated). See also Event ID 22.
21	WRN	Device: /dev/had, ALARMABLE attribute, SMART Attribute: attr_number Changed chng_value. 1. The value for the specified attribute number (attr_number) has changed by the specified value (chng_value). Posting of this alarm may/may not indicate drive problems. Definitions for the attributes are as follows:

	Num	Name	Description
21 (cont'd)	**Num**	**Name**	**Description**
	1	Raw Read Error	Indicates the rate of hardware read errors that occur when reading data from the disk surface. **This error is critical. An increasing error rate may indicate a failing disk drive.** (Samsung, Seagate, IBM (Hitachi), Fujitsu, Maxtor, Western Digital)

1 of 5

Table 18: SMART Alarms ***2 of 5***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation		
		2	Throughput Performance	Overall throughput performance of the hard disk.
		3	Spin Up Time	Raw value average of time to spin up drive spindle. (Samsung, Seagate, IBM (Hitachi), Fujitsu, Maxtor, Western Digital)
		4	Start Stop Count	Count of hard disk spindle start/stop cycles. (Samsung, Seagate, IBM (Hitachi), Fujitsu, Maxtor, Western Digital)
		5	Reallocated Sector Count	Amount of remapped sectors.
		6	Read Channel Margin	No explanation of attribute available
		7	Seek Error Rate	Average rate of seek errors: if this value continues to increase it indicates there may be a problem with the disk surface or a mechanical problem. (Samsung, Seagate, IBM (Hitachi), Fujitsu, Maxtor, Western Digital)
		8	Seek Time Performance	Disk seek system performance. (Samsung, Seagate, IBM (Hitachi), Fujitsu, Maxtor, Western Digital)

2 of 5

Table 18: SMART Alarms ***3 of 5***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation		
21 (cont'd)		9	Power_On_Hours	Number of hours of the power-on state of the drive. This value indicates aging. (Samsung, Seagate, IBM (Hitachi), Fujitsu, Maxtor, Western Digital)
		10	Spin_Retry_Count	Count of retry of drive spindle spine start up attempts. (Samsung, Seagate, IBM (Hitachi), Fujitsu, Maxtor, Western Digital)
		11	Recalibration Retries	Number of times recalibration was requested after initial request. (Samsung, Seagate, IBM (Hitachi), Fujitsu, Maxtor, Western Digital)
		12	Device Power Cycle Count	Count of full hard disk power on/off cycles. (Samsung, Seagate, IBM (Hitachi), Fujitsu, Maxtor, Western Digital)
		13	Soft Read Error Rate	Rate of program read errors when reading data from disk. (Samsung, Seagate, IBM (Hitachi), Fujitsu, Maxtor, Western Digital)
		193	Load/Unload Cycle	Count of load/unload cycles into landing zone position. (Samsung, Seagate, IBM (Hitachi), Fujitsu, Maxtor, Western Digital)
		194	Temperature	Hard disk drive temperature. (Samsung, Seagate, IBM (Hitachi), Fujitsu, Maxtor, Western Digital - select models)
		196	Reallocated Event Count	Count of remap operations (transferring of data from bad sector to reserved disk area) successful and non-successful. **This error is critical. An increasing count for this error may indicate a failing disk drive.** (Samsung, Seagate, IBM (Hitachi), Fujitsu, Maxtor, Western Digital - select models)
		197	Current Pending Sector Count	Current count of unstable sectors (waiting for remap). **This error is critical. An increasing count for this error may indicate a failing disk drive.** (Samsung, Seagate, IBM (Hitachi), Fujitsu, Maxtor, Western Digital)
				3 of 5

Table 18: SMART Alarms *4 of 5*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation		
21 (cont'd)		198	Uncorrectable Sector Count	Count of uncorrectable errors when reading/writing a sector. **This error is critical. An increasing count for this error may indicate a failing disk drive.** (Samsung, Seagate, IBM (Hitachi), Fujitsu, Maxtor, Western Digital)
		199	UltraDMA CRC Error Count	Count of Cyclic Redundancy Check (CRC) errors during UltraDMA mode (Samsung, Seagate, IBM (Hitachi), Fujitsu - select models, Maxtor, Western Digital - select models)
		200	Write Error Rate (Multi Zone Error Rate	Total number of errors found when writing a sector. (Samsung, Seagate, IBM (Hitachi), Fujitsu, Maxtor, Western Digital)
		220	Disk Shift	Indicates how much the disk has shifted (unit of measure unknown). **This error is critical. An increasing value for this error may indicate a failing disk drive.** (Seagate)
		221	G-Sense Error Rate	Rate of errors occurring as a result of impact loads such as dropping the drive or wrong installation. (Seagate, Hitachi)
		222	Loaded Hours	Loading on magnetic heads actuator caused by the general operating time.
		223	Load/Unload Retry Count	Loading on magnetic heads actuator caused by numerous recurrences of operations such as reading, recording, or positioning.
		224	Load Friction	Loading of magnetic heads actuator caused by friction in mechanical part of the store.
		226	Load-in Time	Total time of loading on the magnetic heads actuator.

4 of 5

Table 18: SMART Alarms ***5 of 5***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation		
21 (cont'd)		227	Torque Amplification Count	Count of efforts of the rotating moment of a drive
		228	Power-Off Retract Count	Count of the number of times the drive was powered off.
		230	GMR Head Amplitude	Amplitude of the heads trembling in running mode.
22	WRN	Failed to read SMART values/thresholds 1. The SMART utility was not able to read the SMART values/thresholds from the drive. The SMART utility is unable to function due to drive access problems.		
				5 of 5

Back to: Linux Server Alarms

_LX (Linux)

Table 19: LX Server Alarms describes the server alarms for _LX.

Table 19: LX Server Alarms

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
3	WRN	OVERLOAD CONTROL LEVEL 1 - The average CPU occupancy for the last 20 seconds exceeded 92.5%. New call originations from either stations or trunks are denied until the average CPU occupancy drops below 92.5% for at least 30 seconds.
4	WRN	OVERLOAD CONTROL LEVEL 2 - The average CPU occupancy for the last 30 seconds exceeded 92.5%. All new call originations and terminations are denied until the average CPU occupancy drops below 92.5% for at least 30 seconds.
5	MIN	The system firewall may not be running on the system. ⚠ **CAUTION:** Not having a system firewall operational is a serious security risk. 1. Restart iptables by issuing the following command as root: **`/etc/init.d/iptables restart`** 2. Ensure that there is execute permissions on the **/opt/ws/iptables** file.

Back to: Linux Server Alarms

Login Alarms

The system monitors access to the server and alarms suspicious activity. Table 20: Login Alarms describes the Login alarms and their troubleshooting procedures.

For the S8300 Server, see Table 21: S8300 Login Alarms

Table 20: Login Alarms ***1 of 2***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1	WRN	Successful CM login.
2	MIN	"SAT_auth:Login for [inads] invalid password" 1. A SAT login to Communication Manager failed. Verify the alarm, either from the: - Web interface, by selecting **View Current Alarms** - Linux command line, by entering **`almdisplay -v`** 2. Since mis-typing a login sequence usually causes this alarm, enter **`almclear -n`** ***`#id`*** to clear the alarm. 3. If this alarm is perceived as a security threat (often due to its persistence or frequent recurrence), notify the customer.
3	WRN	Successful Linux login
4	MIN	"Login for [linux] – failed – password check" 1. A login to a server's Linux command line failed. Verify the alarm, either from the: - Web interface, by selecting **View Current Alarms** - Linux command line, by entering **`almdisplay -v`** 2. Since mis-typing a login sequence usually causes this alarm, enter **`almclear -n`** ***`#id`*** to clear the alarm. 3. If this alarm is perceived as a security threat (often due to its persistence or frequent recurrence), notify the customer.
		1 of 2

Table 20: Login Alarms ***2 of 2***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
5	MAJ	"Probation interval for login ends – lockout interval begins" — Multiple consecutive login failures. 1. If this alarm is perceived as a security threat, notify the customer. 2. Using a services login, enter the command `userlock -s` on the Linux command line. This will display all of the logins in the system, the number of failed logins, and if the login in question is currently locked out.
6	WRN	Lacfile missing
7	MAJ	lacfile error - corrupt or expired authentication data
8	MAJ	Access denied. Linux login failure. Access through illegal port.
		2 of 2

Back to: Linux Server Alarms

S8300 Login Alarms

Table 21: S8300 Login Alarms describes the S8300 Server login alarms and their troubleshooting procedures.

Table 21: S8300 Login Alarms ***1 of 2***

Event ID	Alarm Level	Cause/Description, Recommendation
1	WRN	Using the Web Interface, select **View Current Alarms**. 1. Notify the customer.
2	WRN	Using the Web Interface, select **View Current Alarms**. 1. Notify the customer.
3	MIN	Security violation. 1. Using the Web Interface, select **View Current Alarms**. 2. Notify the customer.
		1 of 2

Table 21: S8300 Login Alarms ***2 of 2***

Event ID	**Alarm Level**	**Cause/Description, Recommendation**
4	MIN	Security violation. 1. Using the Web Interface, select **View Current Alarms**. 2. Notify the customer.
5	MAJ	Security violation. 1. Using the Web Interface, select **View Current Alarms**. 2. Notify the customer.
		2 of 2

Back to: Linux Server Alarms

_MP (Maintenance Processor)

This alarm only applies to the S8400, S8500B, and S8500C servers.

Table 22: _MP Alarm in Server

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1	MAJ	SAMP/MPC is in a rolling reboot state. 1. The problem may be related to corruption. On the server, enter **`sampcmd cme load < /etc/agxcm.xml`** on the Linux command line. 2. Reboot the SAMP/MPC by entering **`sampcmd sudo reboot`** on the Linux command line. 3. If the rolling reboot persists, escalate the problem.
2	MAJ	SAMP rolling reboot counter cleared.

Back to: Linux Server Alarms

NIC (Network Interface Card)

The NICs provide the physical and data-link interfaces for Ethernet-based links.

Table 23: NIC Alarms describes NIC alarms and their troubleshooting procedures.

See DAJ1/DAL1/DAL2 (Duplication Memory Board) for more information.

Table 23: NIC Alarms

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1	MIN	"eth0 NIC Link is Down" — Ethernet link on native NIC 0 is down. 1. Verify Ethernet connectivity, either from the: - Web interface, by selecting the **Execute Pingall** diagnostic - Linux command line, by entering **`pingall -a`** Check both sides of each failed link, and make any necessary repairs. 2. If the ping test fails, check the physical connections of NIC 0's Ethernet cable. If the test passes, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
2	MIN	"eth1 NIC Link is Down" — Ethernet link on native NIC 1 is down. 1. Verify Ethernet connectivity, either from the: - Web interface, by selecting the **Execute Pingall** diagnostic - Linux command line, by entering **`pingall -a`** Check both sides of each failed link, and make any necessary repairs. 2. If the ping test fails, check the physical connections of NIC 1's Ethernet cable. If the test passes, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and "Clear" - Linux command line, by entering **`almclear -n`** ***`#id`***

Back to: Linux Server Alarms

RMB (Remote Maintenance Board)

RMB alarms are reported for the S8400, S8500, S8500B, and S8500C servers. The functionality of the Remote Maintenance Board (RMB) is to:

- Monitor the server environmental state of health: fans, voltages, and temperature.
- Report server failures.
- Provide the ability to perform remote server power-on, power off, and reset functionality.

RMB alarms are not recorded on the server. Alarms are reported to INADS when certain failure conditions are detected.

S8400: The Maintenance Processor Complex (MPC) board is integrated in the S8400 server. It monitors the S8400 server temperature and provides reset control. See Table 24: RMB Alarms in the S8400 Server for this server.

S8500: The RMB functionality for the S8500 server is implemented by the Remote Supervisor Adapter (RSA) board. It is installed in PCI-X slot 1 of the server. See Table 25: RMB Alarms in the S8500 Server for this server.

S8500B and S8500C: The RMB functionality for the S8500B and S8500C servers is implemented by the Augmentix Server Availability Management Processor™ (A+SAMP) board. See Table 26: RMB Alarms in the S8500B and S8500C Servers for this server.

Table 24: RMB Alarms in the S8400 Server

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
0	MIN	Test Alarm. Hardware Platform Interface (HPI) User Event - for testing modem setup.
2	MIN	Host boot failure. Hardware Platform Interface (HPI) OEM Event - host is not booting.
3	MAJ	Host Alarm. Hardware Platform Interface (HPI) User Event - Communication Manager detects rolling reboot.
5	MAJ	Host failure timeout. Hardware Platform Interface (HPI) Watchdog Event - Communication Manager is hung.

Back to: Linux Server Alarms

Table 25: RMB Alarms in the S8500 Server ***1 of 3***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1	MIN	"RMB driver missing - handshake Failed" - The driver for communicating with the RSA card cannot be found. Several failures can generate this fault: • the Linux bash command **`/sbin/lsmod`** is missing • the results from running **`/sbin/lsmod`** could not be read • **`/sbin/lsmod`** returned nothing • the RSA device driver was not loaded • the RSA device driver does not exist The recommendations are: 1. Be sure **`/sbin/ibmod`** exists and is executable. 2. Be sure **`/tmp`** exists as a directory and can be written. 3. Be sure **`/lib/modules/ibmasm/ibmasm.o`** exists and has read permission. 4. Run the bash command "service ibmasm start".
2	MIN	"RMB cli is not loaded on the server." - The program that talks to the RSA card could not be found. Several failures generate this fault: • the Linux bash command **`/bin/ls`** is missing or not working properly • the bash command /opt/ecs/rmb/rsa/rsacli is missing or is not executable The recommendations are: 1. Be sure all the above files and directories exist and have read and execute permissions. 2. Reload any missing files from the distribution.
		1 of 3

Table 25: RMB Alarms in the S8500 Server *2 of 3*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
3	MAJ	"RMB reset command failed" - The RSA card did not respond to a reset command. Several failures generate this fault: • the bash command `opt/IBMmpcli/bin/mpcli` is missing or is not executable • the directory **/usr/java/latest** is missing or not symbolically linked to the Java runtime environment (JRE) • the file **/opt/ecs/rmb/rsareset** does not exist or cannot be read • no response from the RSA card • the RSA card did not execute the request The recommendations are: 1. Be sure all the above files and directories exist and have read and execute permissions. 2. Reload any missing files from the distribution. 3. Be sure the RSA card is installed by looking at the back and checking that the green power LED on the RSA card is on, and that the amber error LED is off. 4. Verify that the RSA card is working by dialing into it or logging on to it over the service's port of the RSA card. 5. Restart the RSA card from the RSA modem or service's port and check the LEDs on the back of the card. 6. Verify that the RSA card is plugged into the PCI-X slot of the server. 7. Verify that the flat ribbon cable from the RSA card to the server motherboard has been installed and is firmly seated in the connectors at both ends. 8. Replace the RSA card.
		2 of 3

Table 25: RMB Alarms in the S8500 Server ***3 of 3***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
4	MAJ	"RMB failed handshake test" - The RSA card did not respond to commands from the server. Several failures generate this fault: • the bash command **`/opt/IBMmpcli/bin/mpcli`** is missing or is not executable • the directory **/usr/java/latest** is missing or not symbolically linked to the Java runtime environment (JRE) • the file **/opt/ecs/rmb/rsagetip1** does not exist or cannot be read • no response from the RSA card • the RSA card did not execute the request The recommendations are: 1. Be sure all the above files and directories exist and have read and execute permissions. 2. Reload any missing files from the distribution. 3. Be sure the RSA card is installed by looking at the back and checking that the green power LED on the RSA card is on, and that the amber error LED is off. 4. Verify that the RSA card is working by dialing into it or logging on to it over the service's port of the RSA card. 5. Restart the RSA card from the RSA modem or service's port and check the LEDs on the back of the card. 6. Verify that the RSA card is plugged into the PCI-X slot of the server. 7. Verify that the flat ribbon cable from the RSA card to the server motherboard has been installed and is firmly seated in the connectors at both ends. 8. Replace the RSA card.
		3 of 3

Back to: Linux Server Alarms

Table 26: RMB Alarms in the S8500B and S8500C Servers

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
0	MIN	Test Alarm. Hardware Platform Interface (HPI) User Event
1	MIN	Loss of power to host. Hardware Platform Interface (HPI) Sensor Event.
2	MAJ	Host boot failure. Hardware Platform Interface (HPI) OEM Event
3	MAJ	Host Alarm. Hardware Platform Interface (HPI) User Event
4	MIN	Loss of External Power to SAMP. Hardware Platform Interface (HPI) Sensor Event
5	MAJ	Host failure timeout. Hardware Platform Interface (HPI) Watchdog Event

Back to Linux Server Alarms

SME (Server Maintenance Engine)

The Server Maintenance Engine (SME) is a Linux process which provides error analysis, periodic testing, and demand testing for the server.

Table 27: SME Alarms describes the alarms and troubleshooting procedures.

Table 27: SME Alarms

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1	MAJ	"Far end alarm service is down" — No remote alarm service is available. The other server is unable to report alarms due to a failure of either the GMM or its administered reporting mechanisms (SNMP and/or modem). It is also possible that the modem has been in use for more than 50 minutes by someone dialing into the server for troubleshooting purposes. 1. Look for any GMM failures on the **other** server, either using the: - Web interface, by selecting **Diagnostics > View System Logs** and **Watchdog Logs** - Linux command line, by entering **`logv -w`** or, directly, by examining `/var/log/ecs/wdlog`. 2. If a GMM failure was found: a. See if the GMM application is up, either from the: - Web interface, by selecting **View Process Status** - Linux command line, by entering **`statapp`** b. If so, continue with Step 3. If **not**, try to restart this application by entering **`start -s GMM`** on the Linux command line. c. If the GMM application successfully restarts, continue with Step 4. If **not**, **escalate** the problem to the next higher tier. 3. If a GMM failure was **not** found, see if alarm reporting failed by looking in the trace log for a string that includes "snd2Inads", either from the: - Web interface, by: a. Selecting the **View System Logs** diagnostic and **Logmanager Debug** trace b. Specifying the "Event Range" for the appropriate time frame c. Matching the "snd2Inads" pattern - Linux command line, by entering **`logv -t ts`** 4. Test the administered reporting mechanisms by entering **`testinads`** on the Linux command line. This test could fail if the modem is bad. 5. Once the alarm is resolved, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
2	WRN	For security only. If the IP address in the trap doesn't match UPS translations, this server is getting a trap from an illegal source. No action is needed.

Back to: Linux Server Alarms

STD (Standard SNMP Traps)

Table 28: STD Alarms describes STD traps and their troubleshooting procedures.

Table 28: STD Alarms

Event ID	Alarm Level	Type	Cause/Description
1	MIN	ACT	"coldStart" - Agent Up with Possible Changes. A coldStart trap indicates that the entity sending the protocol (SNMPv2) is re initializing itself in such a way as to potentially cause the alteration of either the agent's configuration or the entity's implementation.
2	MIN	ACT	“warmStart" - Agent Up with No Changes. A warmStart trap indicates that the entity sending the protocol (SNMPv2) is re initializing itself in such a way as to keep both the agent configuration and the entity's implementation intact.
3	MIN	ACT	"linkDown" - Agent Interface Down. A linkDown trap indicates that the entity sending the protocol (SNMPv2) recognizes a failure in one of the communication links represented in the agent's configuration. The data passed within the event is 1) The name and value of the ifIndex instance for the affected interface. 2) The name of the interface can be retrieved via an snmpget of .1.3.6.1.2.1.2.2.1.2.INST, where INST is the instance returned with the trap. The state is indicated by the included value of ifOperStatus.
3	MIN	RES	"linkUP" - Agent Interface Up. A linkUp trap indicates that the entity sending the protocol (SNMPv2) recognizes that one of the communication links represented in the agent's configuration has come up. The data passed within the event is 1) The name and value of the ifIndex instance for the affected interface. 2) The name of the interface can be retrieved via an snmpget of .1.3.6.1.2.1.2.2.1.2.INST, where INST is the instance returned with the trap. The state is indicated by the included value of ifOperStatus.

Back to: Linux Server Alarms

SVC_MON (Service Monitor)

SVC_MON is a server process, started by the Watchdog, that monitors Linux services and processes. It also starts up threads to communicate with a hardware-sanity device.

Table 29: SVC_MON Alarms describes SVC_MON alarms and their troubleshooting procedures.

For information about the Watchdog, see _WD (Watchdog).

Table 29: SVC_MON Alarms ***1 of 8***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1	MIN	“service atd could not be restarted” — The Linux at daemon is down. Scheduled services such as session cleanup or daily filesync will not work. 1. From the `/sbin` directory, enter `service atd restart` to restart the "at" daemon. 2. If the daemon restarts, manually clear the alarm, either from the: • Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** • Linux command line, by entering `almclear -n #id` If not, **escalate** this problem for explicit guidance with steps 2a through 3 a. Enter `grep svc_mon /var/log/messages` to investigate why the daemon failed. ⚠ **CAUTION:** Since the following commands cause a brief service outage, they should only be executed at the customer’s convenience. b. If the `grep` command’s output does not help: • S8700 | S8710 | S8720: enter `server` to verify that the suspected server is the standby. If necessary **and** at the customer’s convenience, enter `server -if` to force a server interchange. • S8500: Proceed to Step d. If necessary **and** at the customer’s convenience, enter `server -if` to force a server interchange. c. S8700 | S8710 | S8720: Reboot the standby server, either from the: • Web interface, by selecting **Shutdown This Server** • Linux command line, entering `/sbin/shutdown -r now` d. S8500: Reboot the server, either from the: • Web interface, by selecting **Shutdown This Server** • Linux command line, entering `/sbin/shutdown -r now` 3. If rebooting the standby does not help **or** if the problem recurs, escalate the problem to the next higher tier.
		1 of 8

Table 29: SVC_MON Alarms *2 of 8*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
2	MIN	"service crond could not be restarted" — The Linux cron daemon is down. Periodic services such as session cleanup or daily filesync will not work. 1. Enter **`/sbin/service cron restart`** to restart the cron daemon. 2. If the daemon restarts, manually clear the alarm, either from the: • Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** • Linux command line, by entering **`almclear -n`** ***`#id`*** If not, **escalate** this problem for explicit guidance with steps 2a through 3 a. Enter **`grep svc_mon /var/log/messages`** to investigate why the daemon failed. Since the following commands cause a brief service outage, they should only be executed at the customer's convenience. b. If the **`grep`** command's output does not help: • **S8700 | S8710 | S8720**: enter **`server`** to verify that the suspected server is the standby. If necessary **and** at the customer's convenience, enter **`server -if`** to force a server interchange. • **S8500**: Proceed to Step d. If necessary **and** at the customer's convenience, enter **`server -if`** to force a server interchange. c. **S8700 | S8710 | S8720**: Reboot the standby server, either from the: • Web interface, by selecting **Shutdown This Server** • Linux command line, entering **`/sbin/shutdown -r now`** d. **S8500**: Reboot the server, either from the: • Web interface, by selecting **Shutdown This Server** • Linux command line, entering **`/sbin/shutdown -r now`** 3. If rebooting the standby does not help **or** if the problem recurs, escalate the problem to the next higher tier.
		2 of 8

Table 29: SVC_MON Alarms ***3 of 8***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
3	MIN	“service inet could not be restarted” — The Linux internet server daemon is down. Networking services will not work. 1. Enter **`/sbin/service inet restart`** to restart the inet daemon. 2. If the daemon restarts, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`*** If **not**, **escalate** this problem for explicit guidance with steps 2a through 3. a. Enter **`grep svc_mon /var/log/messages`** to investigate why the daemon failed. b. If this problem affects call processing, continue with the following steps now. If **not**, continue only at the customer’s convenience – since the following commands cause a brief service outage. The following commands cause a brief service outage. c. If the **`grep`** command’s output does not help: • S8700 | S8710 | S8720: enter **`server`** to verify that the suspected server is the standby. If necessary **and** at the customer’s convenience, enter **`server -if`** to force a server interchange. • S8500: Proceed to Step e. If necessary **and** at the customer’s convenience, enter **`server -if`** to force a server interchange. d. S8700 | S8710 | S8720: Reboot the standby server, either from the: • Web interface, by selecting **Shutdown This Server** • Linux command line, entering **`/sbin/shutdown -r now`** e. S8500: Reboot the server, either from the: • Web interface, by selecting **Shutdown This Server** • Linux command line, entering **`/sbin/shutdown -r now`** 3. If rebooting the standby does not help **or** if the problem recurs, escalate the problem to the next higher tier.
		3 of 8

Table 29: SVC_MON Alarms ***4 of 8***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
4	MIN	“service syslog could not be restarted” — Linux “syslog” service is down. Event logging to syslog and alarm generation will fail. 1. Enter **`/sbin/service syslog restart`** to restart the syslog service. 2. If the service restarts, manually clear the alarm, either from the: • Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** • Linux command line, by entering **`almclear -n`** ***`#id`*** If not, **escalate** this problem for explicit guidance with steps 2a through 3 a. Enter **`grep svc_mon /var/log/messages`** to investigate why the daemon failed. Since the following commands cause a brief service outage, they should only be executed at the customer’s convenience. b. If the **`grep`** command’s output does not help: • **S8700 | S8710 | S8720**: enter **`server`** to verify that the suspected server is the standby. If necessary **and** at the customer’s convenience, enter **`server -if`** to force a server interchange. • **S8500**: Proceed to Step d. If necessary **and** at the customer’s convenience, enter **`server -if`** to force a server interchange. c. **S8700 | S8710 | S8720**: Reboot the standby server, either from the: • Web interface, by selecting **Shutdown This Server** • Linux command line, entering **`/sbin/shutdown -r now`** d. **S8500**: Reboot the server, either from the: • Web interface, by selecting **Shutdown This Server** • Linux command line, entering **`/sbin/shutdown -r now`** 3. If rebooting the standby does not help **or** if the problem recurs, escalate the problem to the next higher tier.
		4 of 8

Table 29: SVC_MON Alarms ***5 of 8***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
5	MIN	"service xntpd could not be restarted" — The Linux network time protocol daemon is down. The server's clock and recently logged time stamps may be inaccurate. 1. Enter **`/sbin/service xntpd restart`** to restart the xntpd daemon. 2. If the daemon restarts, manually clear the alarm, either from the: • Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** • Linux command line, by entering **`almclear -n`** ***`#id`*** If not, **escalate** this problem for explicit guidance with steps 2a through 3 a. Enter **`grep svc_mon /var/log/messages`** to investigate why the daemon failed. b. If this problem affects call processing, continue with the following steps now. If **not**, continue only at the customer's convenience – since the following commands cause a brief service outage. The following commands cause a brief service outage. c. If the **`grep`** command's output does not help: • S8700 | S8710 | S8720: enter **`server`** to verify that the suspected server is the standby. If necessary **and** at the customer's convenience, enter **`server -if`** to force a server interchange. • S8500: Proceed to Step e. If necessary **and** at the customer's convenience, enter **`server -if`** to force a server interchange. d. S8700 | S8710 | S8720: Reboot the standby server, either from the: • Web interface, by selecting **Shutdown This Server** • Linux command line, entering **`/sbin/shutdown -r now`** e. S8500: Reboot the server, either from the: • Web interface, by selecting **Shutdown This Server** • Linux command line, entering **`/sbin/shutdown -r now`** 3. If rebooting the standby does not help **or** if the problem recurs, escalate the problem to the next higher tier.
		5 of 8

Table 29: SVC_MON Alarms *6 of 8*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
6	MIN	"service dbgserv could not be restarted" — Debug server is down, and Gemini debugger may not work. Although losing this service does not affect operations, the debugging of a running system is prevented. 1. Enter **`/sbin/service dbgserv restart`** to restart the dbgserv service. 2. If the service restarts, manually clear the alarm, either from the: • Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** • Linux command line, by entering **`almclear -n`** ***`#id`*** If not, **escalate** this problem for explicit guidance with steps 2a through 3 a. Enter **`grep svc_mon /var/log/messages`** to investigate why the daemon failed. Since the following commands cause a brief service outage, they should only be executed at the customer's convenience. b. If the **`grep`** command's output does not help: • **S8700 | S8710 | S8720**: enter **`server`** to verify that the suspected server is the standby. If necessary **and** at the customer's convenience, enter **`server -if`** to force a server interchange. • **S8500**: Proceed to Step d. If necessary **and** at the customer's convenience, enter **`server -if`** to force a server interchange. c. **S8700 | S8710 | S8720**: Reboot the standby server, either from the: • Web interface, by selecting **Shutdown This Server** • Linux command line, entering **`/sbin/shutdown -r now`** d. **S8500**: Reboot the server, either from the: • Web interface, by selecting **Shutdown This Server** • Linux command line, entering **`/sbin/shutdown -r now`** 3. If rebooting the standby does not help **or** if the problem recurs, escalate the problem to the next higher tier.
		6 of 8

Table 29: SVC_MON Alarms *7 of 8*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
7	MIN	“service prune could not be restarted” — The prune service is not running. The hard disk’s partition usage is not being monitored or cleaned. 1. Enter **`/sbin/service prune restart`** to restart the prune service. 2. If the service restarts, manually clear the alarm, either from the: • Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** • Linux command line, by entering **`almclear -n`** ***`#id`*** If not, **escalate** this problem for explicit guidance with steps 2a through 3 a. Enter **`grep svc_mon /var/log/messages`** to investigate why the daemon failed. b. If this problem affects call processing, continue with the following steps now. If **not**, continue only at the customer’s convenience – since the following commands cause a brief service outage. The following commands cause a brief service outage. c. If the **`grep`** command’s output does not help: • S8700 | S8710 | S8720: enter **`server`** to verify that the suspected server is the standby. If necessary **and** at the customer’s convenience, enter **`server -if`** to force a server interchange. • S8500: Proceed to Step e. If necessary **and** at the customer’s convenience, enter **`server -if`** to force a server interchange. d. S8700 | S8710 | S8720: Reboot the standby server, either from the: • Web interface, by selecting **Shutdown This Server** • Linux command line, entering **`/sbin/shutdown -r now`** e. S8500: Reboot the server, either from the: • Web interface, by selecting **Shutdown This Server** • Linux command line, entering **`/sbin/shutdown -r now`** 3. If rebooting the standby does not help **or** if the problem recurs, escalate the problem to the next higher tier.
		7 of 8

Table 29: SVC_MON Alarms *8 of 8*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
8	MIN	“service httpd could not be restarted” — The hypertext transfer protocol daemon is down. The Web interface will not work. 1. Enter `/sbin/service httpd restart` to restart the http daemon. 2. If the daemon restarts, manually clear the alarm, either from the: • Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** • Linux command line, by entering `almclear -n #id` If not, **escalate** this problem for explicit guidance with steps 2a through 3 a. Enter `grep svc_mon /var/log/messages` to investigate why the daemon failed. Since the following commands cause a brief service outage, they should only be executed at the customer’s convenience. b. If the `grep` command’s output does not help: • S8700 | S8710 | S8720: enter `server` to verify that the suspected server is the standby. If necessary **and** at the customer’s convenience, enter `server -if` to force a server interchange. • S8500: Proceed to Step d. If necessary **and** at the customer’s convenience, enter `server -if` to force a server interchange. c. S8700 | S8710 | S8720: Reboot the standby server, either from the: • Web interface, by selecting **Shutdown This Server** • Linux command line, entering `/sbin/shutdown -r now` d. S8500: Reboot the server, either from the: • Web interface, by selecting **Shutdown This Server** • Linux command line, entering `/sbin/shutdown -r now` 3. If rebooting the standby does not help **or** if the problem recurs, escalate the problem to the next higher tier.
		8 of 8

Back to: Linux Server Alarms

_TM (Translation Manager)

The Translation Manager monitors the server's ability to read Communication Manager translations. Table 30: TM Alarm describes the _TM alarms and their troubleshooting procedures.

Table 30: TM Alarm

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1	MAJ	"Cannot read translations" — Server could not read translations. Usually, indicates a failure loading translations, but can also infrequently occur on a running system. S8700 | S8710 | S8720: The servers spontaneously interchanged. S8300 | S8400 | S8500: The server rebooted. 1. Check the integrity of the translation files xln1 and xln2 in /etc/opt/defty, and verify that they are of the same non-zero length. 2. From the /etc/opt/defty directory, enter the Linux command **`cksum`** ***`xln1 xln2`*** to verify that the checksums of the files are identical. 3. S8700 | S8710 | S8720: Copy the translation files from the backup or the other server. 4. S8300 | S8400 | S8500: Copy the translation files from the backup. 5. If Steps 1 to 3 do not help, load the system with null translations. 6. If the system comes up, this is probably a translation problem. If **not**, escalate the problem. 7. Once resolved, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***

Back to: Linux Server Alarms

TlsManager

The Transport Layer Security Manager allows third-party certificates to be loaded. It will not allow a corrupt certificate to be loaded.

A security log message is generated as a result of a Communication Manager telephony application installing CA certificates from /etc/opt/ecs/certs/CA/all-ca.crt. Successful and failed attempts are noted in /var/log/secure.*. The format is

> logmanager: gip(26/1) CA_certs: load of CA certificates from /etc/opt/ecs/certs/CA/all-ca.crt succeeded (or failed).

The event also generates an alarm to notify the administrator of partial or complete outages (some or all CA certificates failed to install), and also when the system is operating properly (i.e., any error condition cleared).

If the telephony application fails to install any or all specified CA certificates, the Communication Manager log will contain one or more of the following error messages (where x is the Communication Manager release number):

> CMx_proc_err: pro=7204, err=201, seq=22145,da1=<n>,da2=<max> - This indicates that the number of CA certificates specified exceeds the number supported by the telephony application. <n> is the overlimit value and <max> is the maximum number of certificates supported. To resolve, use **`tlscertmanage`** to edit the list, then restart the telephony application.
>
> CMx_proc_err: pro=7204, err=201, seq=22146,da1=<n>,da2=0 - This indicates that a failure occurred when attempting to install the n’th CA certificate into the telephony application. <n> is the index of the CA certificate list item that failed to install. To resolve, use **`tlscertmanage`** to remove, then re-add the certificate. Once re-added, restart the telephony application.
>
> CMx_proc_err: pro=7204, err=201, seq=22147,da1=0,da2=0 - This indicates that the CA certificate list file, /etc/opt/ecs/certs/CA/all-ca.crt, cannot be opened. This may be due to a user privilege issue or a missing/corrupted file. Use **`tlscertmanage`** to reconstruct the CA certificate list, then restart the telephony application.

Table 31: TlsManager Alarms

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
2	MIN	The load of TlsManager CA certificates failed.

Back to: Linux Server Alarms

UPG (Upgrade)

The UPG raises an alarm if the upgrade was not made permanent within a certain amount of time after the upgrade.

Table 32: UPG Alarms

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1	MAJ	The upgrade was not made permanent within two hours. No commit error. 1. Make the upgrade permanent by using the web interface. Select **Server Upgrade**, then select **Make Upgrade Permanent**

Back to: Linux Server Alarms

UPS (Uninterruptible Power Supply)

This section contains tables which explain UPS Traps to the Server and UPS Alarms to the Server.

When a UPS event occurs, an alarm will be raised and the server state of health will be degraded. The server will not shut down as long as battery power is available. It is the goal of Communication Manager to provide call processing service for as long as possible.

Given the highly reliable file systems and recovery mechanisms in place, it is expected that no damage will be done to the server. The server is expected to recover normally even if the UPS runs of out battery backup and the server catastrophically loses power.

After power has been restored and the system has been up for approximately 1 hour 15 minutes, the alarm will be resolved automatically.

UPS Traps to the Server

Table 33: Enterprise-Specific UPS Traps to Server contains the various UPS-generated SNMP traps to the server.

Table 33: Enterprise-Specific UPS Traps to Server ***1 of 3***

SNMP Trap from UPS	Event ID	Definition of Trap
Trap (1)	#1–8	Alarm string = #1, ACT, UPS, A, Event ID #, MAJ, Warning, system power failure: Possible UPS exhaustion in 1 - 8 minutes. The UPS battery’s power is in a critically low condition, with an estimated 8 minutes or less of remaining holdover. • A warning is sent to every logged-in user of the server. For troubleshooting procedures, see Events #1–8
Trap (3) upsAlarmShutdownPending	#11	Alarm string = #1, ACT, UPS, A, 11, WRN, Miscellaneous trap, e.g., bad battery. For troubleshooting procedures, see Event #11
Trap (3) upsAlarmShutdownPending	#12	Alarm string = #1, ACT, UPS, A, 12, WRN, Miscellaneous trap, e.g., bad battery. For troubleshooting procedures, see Event #12
Trap (3)[1] upsAlarmShutdownImminent	#13	Alarm string = #1,ACT, UPS, A, 13, MAJ, Miscellaneous trap, e.g., bad battery. For troubleshooting procedures, see Event #13
		1 of 3

Table 33: Enterprise-Specific UPS Traps to Server ***2 of 3***

SNMP Trap from UPS	Event ID	Definition of Trap
Trap (3)[1] upsAlarmDepletedBattery	#14	Alarm string = #1,ACT,UPS,A,14,MAJ,Miscellaneous trap, e.g., bad battery. For troubleshooting procedures, see Event #14
Trap (3)[1] upsAlarmBatteryBad	#15	Alarm string = #1,ACT,UPS,A,15,MIN,Miscellaneous trap, e.g., bad battery For troubleshooting procedures, see Event #15
Trap (3) upsAlarmInputBad	#16	Alarm string = #1,ACT,UPS,A,16,MIN,Miscellaneous trap, e.g., bad battery For troubleshooting procedures, see Event #16
Trap (3) upsAlarmTempBad	#17	Alarm string = #1,ACT,UPS,A,17,WRN,Miscellaneous trap, e.g., bad battery For troubleshooting procedures, see Event #17
Trap (3) upsAlarmCommunicationsLost	#18	Alarm string = #1,ACT,UPS,A,18,WRN,Miscellaneous trap, e.g., bad battery For troubleshooting procedures, see Event #18
Trap (3) upsAlarmBypassBad	#19	Alarm string = #1,ACT,UPS,A,19,MIN,Miscellaneous trap, e.g., bad battery For troubleshooting procedures, see Event #19
Trap (3) upsAlarmLowBattery	#20	Alarm string = #1,ACT,UPS,A,20,WRN,Miscellaneous trap, e.g., bad battery For troubleshooting procedures, see Event #20
Trap (3) upsAlarmUpsOutputOff	#21	Alarm string = #1,ACT,UPS,A,21,WRN,Miscellaneous trap, e.g., bad battery For troubleshooting procedures, see Event #21
Trap (3) upsAlarmOutputBad	#22	Alarm string = #1,ACT,UPS,A,22,WRN,Miscellaneous trap, e.g., bad battery For troubleshooting procedures, see Event #22
		2 of 3

Table 33: Enterprise-Specific UPS Traps to Server *3 of 3*

SNMP Trap from UPS	Event ID	Definition of Trap
Trap (3) upsAlarmOutputOverload	#23	Alarm string = #1,ACT,UPS,A,23,WRN,Miscellaneous trap, e.g., bad battery For troubleshooting procedures, see Event #23
Trap (3) upsAlarmChargerFailed	#24	Alarm string = #1,ACT,UPS,A,24,WRN,Miscellaneous trap, e.g., bad battery For troubleshooting procedures, see Event #24
Trap (3) – upsAlarmFanFailure	#25	Alarm string = #1,ACT,UPS,A,25,WRN,Miscellaneous trap, e.g., bad battery For troubleshooting procedures, see Event #25
Trap (3) – upsAlarmFuseFailure	#26	Alarm string = #1,ACT,UPS,A,26,WRN,Miscellaneous trap, e.g., bad battery For troubleshooting procedures, see Event #26
Trap (3) – upsAlarmGeneralFault	#27	#1,ACT,UPS,A,27,WRN,Miscellaneous trap, e.g., bad battery For troubleshooting procedures, see Event #27
Trap (4), Event ID #9 upsAlarmOnBattery	9	Alarm string = #1, ACT, UPS, A, 9,WRN, Miscellaneous trap, e.g., bad battery. This UPS trap [Event #9] is a miscellaneous environmental alarm sent from the UPS that supports server A. For example, the battery may be bad and should be replaced.
		3 of 3

[1] This event degrades the server's state of health.

Back to: Linux Server Alarms

UPS Alarms to the Server

Table 34: UPS Alarms describes the server's UPS-related alarms and their troubleshooting procedures.

Table 34: UPS Alarms ***1 of 3***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1–8	MAJ	"upsEstimatedMinutesRemaining" — The UPS is supplying power and there are only 1 - 8 minutes of batter life remaining. The UPS does not have an AC-power source. 1. Restore AC power to the UPS.
11	WRN	"upsAlarmonBattery" — The UPS is drawing power from the batteries. This message should be accompanied by a "upsEstimatedMinutesRemaining" message. 1. Restore AC power to the UPS.
12	MAJ	"upsAlarmShutdownPending" — A shutdown-after-delay countdown is underway (i.e., the UPS has been commanded off). 1. Stop countdown timer. (Can be done via SNMP messages.)
13	MAJ	"upsAlarmShutdownImminent" — The UPS will turn off power to the load in < 5 seconds. 1. Restore AC power to the UPS.
14	MAJ	"upsAlarmDepletedBattery" — If primary power is lost, the UPS could not sustain the current load. 1. Charge or replace the batteries in the UPS. See the appropriate manual for the UPS model.
15	MAJ	"upsAlarmBatteryBad" — One or more batteries needs to be replaced. 1. Replace any defective batteries in the UPS. See the appropriate manual for the UPS model.
16	MIN	"upsAlarmInputBad" — An input condition is out of tolerance. 1. Provide appropriate AC power to the UPS.
		1 of 3

Table 34: UPS Alarms ***2 of 3***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
17	MIN	"upsAlarmTempBad" — The internal temperature of a UPS is out of tolerance. (On the UPS, the "over temperature" alarm indicator flashes, and the UPS changes to Bypass mode for cooling. Either: 1. Look for and remove any obstructions to the UPS's fans. 2. Wait at least 5 minutes, and restart the UPS. 3. Check for and resolve any fan alarms (Event ID 25) against the UPS. 4. Either: • Change (increase or decrease) the environment's temperature. • Change the alarming thresholds.
18	MIN	"upsAlarmCommunicationsLost" — The SNMP agent and the UPS are having communications problems. (A UPS diagnosis may be required.) 1. Behind the UPS in its upper left-hand corner, verify that an SNMP card (with an RJ45 connector) resides in the UPS — instead of a serial card with DB9 and DB25 connectors. 2. Verify that the server is physically connected to the UPS via the RJ45 connector. 3. Verify that the SNMP card is properly administered according to the procedures in its users guide, provided by the vendor. 4. If necessary, replace the SNMP card in the UPS. 5. If the problem persists, replace the UPS, and diagnose it later.
19	WRN	"upsAlarmBypassBad" — The "source" power to the UPS, which (during a UPS overload or failure) also serves as "bypass" power to the load, is out of tolerance — incorrect voltage by > ±12% or frequency > ±3%. This on-line UPS normally regenerates its source power into clean AC power for the load. However, the source power's quality is currently unacceptable as bypass power to the load). 1. Verify that the UPS expects the correct "nominal input voltage" from its power source. 2. If **so**, restore acceptable AC power to the UPS. If **not**, reconfigure the UPS to expect the correct voltage. See the appropriate manual for the UPS model.
		2 of 3

Table 34: UPS Alarms ***3 of 3***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
20	WRN	“upsAlarmLowBattery” — The battery’s remaining run time ≤ specified threshold. 1. Restore AC power to the UPS.
21	WRN	“upsAlarmUpsOutputOff” — As requested, UPS has shut down output power. The UPS is in Standby mode. 1. Turn on output power. (Can be done via SNMP messages.)
22	WRN	“upsAlarmOutputBad” — A receptacle’s output is out of tolerance. (A UPS diagnosis is required.) 1. Replace the UPS, and diagnose it later.
23	WRN	“upsAlarmOutputOverload” — The load on the UPS exceeds its output capacity. The UPS enters Bypass mode. 1. Reduce the load on the UPS. 2. Verify that the UPS returns to Normal mode.
24	WRN	“upsAlarmChargerFailed” — The UPS battery charger has failed. (A UPS diagnosis is required.) 1. Replace the UPS, and diagnose it later.
25	WRN	“upsAlarmFanFailure” — One or more UPS fans have failed. Unless lightly loaded, the UPS enters Bypass mode. 1. Replace the UPS, and diagnose it later.
26	WRN	“upsAlarmFuseFailure” — One or more UPS fuses have failed. 1. Replace the UPS, and diagnose it later.
27	WRN	“upsAlarmGeneralFault” — A general fault occurred in the UPS. (A UPS diagnosis is required.) 1. Replace the UPS, and diagnose it later.
		3 of 3

Back to: Linux Server Alarms

USB1 (Modem)

Table 35: USB1 Event IDs and Alarm Text contains the Event IDs, alarm text, and recommended command to enter for examining USB1 alarms.

Table 35: USB1 Event IDs and Alarm Text

Event ID	Alarm Level	Alarm Text	Test To Investigate	Command to Enter
1	MIN	USB Modem Handshake Test Failed	Handshake Test	testmodem -t handshake
2	MIN	USB Modem Offhook Test Failed	Off-Hook Test	testmodem -t off-hook
3	MAJ	None	Reset USB Test	testmodem -t reset_usb

The **`testmodem`** command provides the ability to reset the modem and perform offhook, handshake, and looparound tests. The command is described in Table 36: testmodem command usage.

Table 36: testmodem command usage

Usage: **`testmodem [-s]	[-l]	[-t arg]	[-?]`**	
no argument	Performs short tests (offhook and handshake)
`-s`	Performs short tests (offhook and handshake)
`-l`	Performs long tests (offhook, handshake, and looparound to INADS)
`-t` *reset_usb*	Resets the modem
`-t` *handshake*	Handshakes with the modem
`-t` *offhook*	Requests the modem to go offhook
`-t` *looparound*	Dials out to INADS and waits for a response
`-?`	Displays the command usage
`The following errors may be displayed:`	
`1: Run almcall command to administer the telephone numbers`	Alarm configuration has not been done. Use the oss command to configure the phone number and try again.
`2: No telephone number configured - Use almcall to administer`	The OSS phone number was not configured. Use the oss command to configure the phone number and try the command again.
`3: Failed to create socket`	A system resource could not be allocated. Wait a few minutes and try the command again.
`4: Failed to connect to SME`	The command could not connect to the server to process the command. Verify that Communication Manager is running and the Server Maintenance Engine (SME) is running by entering the Linux command **`statapp`**
`5: Failed to send request to SME`	The request could not be sent to the server. Verify that Communication Manager is running and the Server Maintenance Engine (SME) is running by entering the Linux command **`statapp`**
`6: Failed to receive response from SME`	The test did not receive a response from the server. The system may be hung. Verify that Communication Manager and the SME are running by entering the Linux command **`statapp`**

Back to: Linux Server Alarms

Handshake Test

This test is **destructive**.

This test verifies that the system can "handshake" with the attached modem hardware.

The following messages can be displayed:

Table 37: Handshake Test

Error Message	Test Result	Description / Recommendation
Modem in use, try again later	ABORT	Another application is currently using the modem. Try again later.
Could not open USB port	ABORT	System error: An attempt to open the USB device failed. 1. Retry the test in about 5 minutes. 2. If the test still aborts, escalate the problem.
Read error, could not run test	ABORT	A probable system error aborted the test. 1. Retry the test in about 5 minutes. 2. If the test still aborts, escalate the problem.
Modem Handshake Test Failed	FAIL	The modem did not handshake with the system. 1. Retry the test in about 5 minutes. 2. If the test still fails, escalate the problem.

Off-Hook Test

This test is **destructive**.

This test runs an off-hook test for the modem attached to the USB port on the server. The test verifies that a line is connected to the modem. The following messages can be displayed:

Table 38: Off-Hook Test ***1 of 2***

Error Message	Test Result	Description / Recommendation
Modem in use, try again later	ABORT	Another application is currently using the modem. Try again later.
		1 of 2

Table 38: Off-Hook Test ***2 of 2***

Error Message	Test Result	Description / Recommendation
Could not open USB port	ABORT	An attempt to open the USB device failed. Try again later
Read error, could not run test	ABORT	A probable system error aborted the test. Try again. If the test continues to abort, escalate the problem.
Modem Off-Hook Test Failed	FAIL	Modem Off-Hook test failed. Dial tone was not detected in the time allowed. 1. Retry the test. 2. If the test still aborts, escalate the problem.
		2 of 2

Back to: Linux Server Alarms

Reset USB Test

This test is **destructive**.

This test causes the modem to be reset if the modem is not in use. The following messages can be displayed:

Table 39: Reset USB

Error Code	Test Result	Description / Recommendation
Could not open USB port	ABORT	System error: An attempt to open the USB device failed. Try again later.
Modem in use, try again later	ABORT	Another application is using the modem. Try the test at a later time.
Modem Reset Test Failed	FAIL	The modem was not reset. Try the command again. If the test continues to fail, escalate the problem.
Modem has been reset	PASS	The modem was successfully reset.

Back to: Linux Server Alarms

_WD (Watchdog)

The Watchdog is a server process that:

- Creates other Communication Manager processes
- Monitors process sanity
- Can recover process failures

Watchdog also communicates with a hardware-sanity device. For alarm-related information about these services, see SVC_MON (Service Monitor).

Table 40: _WD Alarms describes the _WD alarms and their troubleshooting procedures.

Table 40: _WD Alarms ***1 of 16***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
4 S8300	MAJ	"Application <name> (pid) TOTALLY FAILED" — An application is present but not launching. The application could not start the maximum allowed number of times. (This alarm usually occurs with Event ID #20.) 1. To verify the alarm, look for the application's name or process ID (PID)," either using the: - Web interface, by selecting **Diagnostics > View System Logs** and **Watchdog Logs** - Linux command line, by entering **`logv -w`** or, directly, by examining `/var/log/ecs/wdlog` 2. If the application is down, enter **`start -s`** ***`application`*** to start the application. 3. If the application comes up, continue with Step 7. If the application does **not** come up, check the trace log to further investigate why the application fails, either from the: - Web interface by: a. Selecting the **View System Logs** diagnostic and **Logmanager Debug** trace b. Specifying the **Event Range** for the appropriate time frame c. Matching the application's PID as the pattern - Linux command line, by entering **`logv -t ts`** Look for a related core-dump file in `/var/crash`, and **escalate** for an analysis of this file. 4. Verify that the file named in the log exists and is executable. To locate the application's executable file, enter the Linux command: **`ls -l /opt/ecs/sbin/`*`appl`*** If the executable is present, Linux returns a symbolic link to its location.
		1 of 16

Table 40: _WD Alarms ***2 of 16***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
4 (cont'd)	MAJ	5. If **so** (**less** common): a. Enter `ls -l` on the symbolic link's address. b. Verify that the executable has "execution" permissions. c. If not, enter **`chmod +x`** to enable execution of the application. If **not** — Linux has returned a "null link" (**more** common): - Acquire the executable from the CD. 6. Enter **`start -s`** ***`application`*** to start the application. 7. Manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`*** 8. If the problem recurs, escalate the problem.
		2 of 16

Table 40: _WD Alarms *3 of 16*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
5	MIN	"WARNING: timeout waiting for reqsvr to initialize" — During each server's boot process, the server's Watchd process waits up to 2 minutes for its "reqsvr" (request server) thread to initialize. If the 2-minute waiting interval elapses, this server logs this alarm, and its boot process hangs. (Meanwhile, if the other server is already booted or subsequently boots, it assumes the active role.) In that (when this alarm occurs) a server hangs during its booting process, this alarm's external symptoms resemble those of two other _WD alarms, #13 (Except S8500) and #14 (Except S8500). Therefore, carefully discriminate between these three events. 1. To inspect the symptoms of this problem, verify that the: a. Linux OS and the Web interface are **up** (including the commands: **`telnet`**, **`statapp`**, **`server`**, **`logv`**, **`cat`**, **`grep`**, **`tail`**, **`vi`**, etc.) b. Watchdog application is **partially up**, but **no** other Communication Manager software is up c. The **`almdisplay`** command displays **no** alarms. Instead, the command returns the message: `"almdisplay: 4: Unable to connect to MultiVantage"` Since the following commands cause a brief service outage, they should only be executed at the customer's convenience. 2. **Escalate** this problem for explicit guidance with the following steps. 3. Enter **`server`** to verify that the suspected server is the standby. If necessary **and** at the customer's convenience, enter **`server -if`** to force a server interchange. 4. Reboot the standby server, either from the: - Web interface, by selecting **Shutdown This Server** - Linux command line, by entering **`/sbin/shutdown -r now`** 5. Once the standby server has booted, verify that Event ID #5 was logged, either using the: - Web interface, by selecting **Diagnostics > View System Logs** and **Watchdog Logs** - Linux command line, by entering **`logv -w`** or, directly, by examining `/var/log/ecs/wdlog`.
		3 of 16

Table 40: _WD Alarms ***4 of 16***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
5 (cont'd)	MIN	6. If rebooting the server does not help **or** if the problem recurs, escalate the problem to the next higher tier.
6 S8300	MAJ	"Application <name> (pid) not started, config parm errors" — Watchdog cannot read its configuration file, `/etc/opt/ecs/watchd.conf`. 1. To verify the alarm, look for the application's name or process ID (PID), either using the: - Web interface, by selecting **Diagnostics > View System Logs** and **Watchdog Logs** - Linux command line, by entering **`logv -w`** or, directly, by examining `/var/log/ecs/wdlog.` 2. Get a fresh copy of `watchd.conf` from the CD. 3. Verify that every executable file listed in `watchd.conf` exists and is executable. 4. Enter **`start -s`** ***`application`*** to start the application. 5. Manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
		4 of 16

Table 40: _WD Alarms *5 of 16*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
7 S8300	MAJ	“Application <name> not started, parm file errors” — Since an application’s specified location in `watchd.conf` is incorrect, Watchdog cannot start the application. 1. To verify the alarm, look for the application’s or process ID (PID), either using the: - Web interface, by selecting **Diagnostics > View System Logs** and **Watchdog Logs** - Linux command line, by entering **`logv -w`** or, directly, by examining `/var/log/ecs/wdlog`. 2. Verify that the executable file named in the log exists and is executable. To locate the application’s executable file, enter the Linux command: **`ls -l /opt/ecs/sbin/`*`appl`*** If the executable is present, Linux returns a symbolic link to its location. 3. If **so** (**less** common): a. Enter **`ls -l`** on the symbolic link’s address. b. Verify that the executable has “execution” permissions. c. If not, enter **`chmod +x`** to enable execution of the application. If **not** — Linux has returned a “null link” (**more** common): - Acquire the executable from the CD. 4. Verify that the string in `watchd.conf` is correct. 5. Enter **`start -s`** ***`application`*** to start the application. 6. Manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
		5 of 16

Table 40: _WD Alarms ***6 of 16***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
13 (Except S8500)	MIN	“ERROR: could not dup socket fd in reqsvr.c, heartbeat thread not created, errno=<x>” — As either a: • Booting application initiates • Restarting application re-initiates heart beating with Watchdog (see Event ID #5), the “reqsvr” (request server) thread tries to create a duplicate socket for the heartbeating thread. This alarm indicates that reqsvr could not create the socket. (Meanwhile, if the other server is already started or subsequently starts, it assumes the active role.) In that (when this alarm occurs) a server hangs, this alarm’s external symptoms resemble those of two other _WD alarms, #5 and #14 (Except S8500). Therefore, carefully discriminate between these three events. 1. To inspect the symptoms of this problem, verify that the: a. Linux OS and the Web interface are **up** (including the commands: **telnet**, **statapp**, **server**, **logv**, **cat**, **grep**, **tail**, **vi**, etc.) b. Watchdog application is **partially up**, and **some** other Communication Manager processes may be up, either using the: - Web interface, by selecting **View Process Status** - Linux command line, by entering **statapp** c. If the GMM process is up, the **almdisplay -v** command shows Event #13’s message string. If **not**, the Watchdog log shows the message string, either using the: - Web interface, by selecting **Diagnostics > View System Logs** and **Watchdog Logs** - Linux command line, by entering **logv -w** or, directly, by examining `/var/log/ecs/wdlog`. Since the following commands cause a brief service outage, they should only be executed at the customer’s convenience. 2. **Escalate** this problem for explicit guidance with the following steps. 3. Enter **server** to verify that the suspected server is the standby. If necessary **and** at the customer’s convenience, enter **server -if** to force a server interchange.
		6 of 16

Table 40: _WD Alarms *7 of 16*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
13 (Except S8500) (cont'd)	MIN	4. Reboot the standby server, either from the: - Web interface, by selecting **Shutdown This Server** - Linux command line, by entering **`/sbin/shutdown -r now`** 5. If rebooting the server does not help **or** if the problem recurs, escalate the problem to the next higher tier.
14 (Except S8500)	MIN	"ERROR in req2svr.p trying to create heartbeat thread, errno=<x>" — After the "reqsvr" (request server) creates a duplicate socket (see Event ID #13 (Except S8500)), it tries to create a heart beating thread. This alarm indicates that reqsvr could not create the thread. (Meanwhile, if the other server is already started or subsequently starts, it assumes the active role.) In that (when this alarm occurs) a server hangs, this alarm's external symptoms resemble those of two other _WD alarms, #5 and #13 (Except S8500). Therefore, carefully discriminate between these three events. 1. To inspect the symptoms of this problem, verify that the: a. Linux OS and the Web interface are **up** (including the commands: **`telnet`**, **`statapp`**, **`server`**, **`logv`**, **`cat`**, **`grep`**, **`tail`**, **`vi`**, etc.) b. Watchdog application is **partially up**, but **all** other Communication Manager processes are up, either using the: - Web interface, by selecting **View Process Status** - Linux command line, by entering **`statapp`** c. The **`almdisplay -v`** command shows Event #14's message string Since the following commands cause a brief service outage, they should only be executed at the customer's convenience. 2. **Escalate** this problem for explicit guidance with the following steps. 3. Enter **`server`** to verify that the suspected server is the standby. If necessary **and** at the customer's convenience, enter **`server -if`** to force a server interchange. 4. Reboot the standby server, either from the: - Web interface, by selecting **Shutdown This Server** 5. If rebooting the server does not help **or** if the problem recurs, escalate the problem to the next higher tier.
		7 of 16

Table 40: _WD Alarms *8 of 16*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
15 S8300	MAJ	"Detected a rolling reboot" — Watchdog has detected "x" number of Linux reboots within "y" minutes (where x and y are configurable in `/etc/opt/ecs/watchd.conf`). Rolling reboots have a wide variety of possible causes. 1. To verify the alarm, look for the message, "WARNING: Rolling reboot detected!!,"either using the: - Web interface, by selecting **Diagnostics > View System Logs** and **Watchdog Logs** - Linux command line, by entering **`logv -w`** or, directly, by examining `/var/log/ecs/wdlog`. 2. **Escalate** this problem for explicit guidance with the following steps. 3. Paying special attention to Communication Manager errors, continue examining the Watchdog log (from Step 1), and try to determine which application failed. 4. Verify that every executable file listed in `watchd.conf` exists and is executable. Rolling reboots are often caused by executables in unexpected locations. 5. If the files and their locations are OK, investigate the trace log to isolate the cause, either from the: - Web interface by: a. Selecting the **View System Logs** diagnostic and **Logmanager Debug** trace b. Specifying the **Event Range** for the appropriate time frame c. Matching the "rolling reboot" pattern - Linux command line, by entering **`logv -t ts`**
		8 of 16

Table 40: _WD Alarms *9 of 16*

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
18 S8300	WRN	“Application <name> restarted. Retry <retry count>, New Pid: <pid>” — An application has failed, and Watchdog successfully restarted it. 1. To verify the alarm, look for the application’s name or process ID (pid), either using the: - Web interface, by selecting **Diagnostics > View System Logs** and **Watchdog Logs** - Linux command line, by entering **`logv -w`** or, directly, by examining `/var/log/ecs/wdlog`. 2. **No** resolution. Manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
		9 of 16

Table 40: _WD Alarms ***10 of 16***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
19 S8300	MIN	“Application failed unintentionally” — Watchdog is bringing the system down because an application failed to start correctly. The application may have failed to start either because: • The file did not exist (coincident with Event ID #7). • Required application parameters were missing or invalid in `watchd.conf`. 1. To verify the alarm, look for the message, “Application num <#> (<application path>) not started. Watchdog exiting NOW,” either using the: - Web interface, by selecting **Diagnostics > View System Logs** and **Watchdog Logs** - Linux command line, by entering **`logv -w`** or, directly, by examining `/var/log/ecs/wdlog`. 2. Verify that the file named in the log exists and is executable. 3. Verify that the string in `watchd.conf` is correct. 4. If Steps 2 and 3 are OK, investigate the trace log to see why the application fails, either from the: - Web interface by: a. Selecting the **View System Logs** diagnostic and **Logmanager Debug** trace b. Specifying the **Event Range** for the appropriate time frame c. Matching the application’s number as the pattern - Linux command line, by entering **`logv -t ts`** 5. Once resolved, manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`***
		10 of 16

Table 40: _WD Alarms ***11 of 16***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
20 S8300	MAJ	“Application <name> (pid) TOTALLY FAILED” — Application failed the maximum allowed number of times. (This alarm usually occurs with Event ID #4.) 1. To verify the alarm, look for the application’s name or process ID (PID), either using the: - Web interface, by selecting **Diagnostics > View System Logs** and **Watchdog Logs** - Linux command line, by entering **`logv -w`** or, directly, by examining `/var/log/ecs/wdlog`. - See if the application is up, either from the: - Web interface, by selecting **View Process Status** - Linux command line, by entering **`statapp`** 2. If the application is down, enter **`start -s`** ***`application`*** to start the application. 3. If the application comes up, continue with Step 7. If **not**, check the trace log to further investigate why the application fails, either from the: - Web interface by: a. Selecting the **View System Logs** diagnostic and **Logmanager Debug** trace b. Specifying the **Event Range** for the appropriate time frame c. Matching the application’s PID as the pattern - Linux command line, by entering **`logv -t ts`** 4. To locate the application’s executable file, enter the Linux command: **`ls -l /opt/ecs/sbin/`*****`appl`*** If the executable is present, Linux returns a symbolic link to its location.
		11 of 16

Table 40: _WD Alarms ***12 of 16***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
20 (cont'd)	MAJ	5. If so (less common): a. Enter `ls -l` on the symbolic link's address. b. Verify that the executable has "execution" permissions. c. If not, enter `chmod +x` to enable execution of the application. If not — Linux has returned a "null link" (more common): - Acquire the executable from the CD 6. Enter `start -s` ***`application`*** to start the application. 7. Manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering `almclear -n` ***`#id`*** 8. If the problem recurs, escalate the problem.
		12 of 16

Table 40: _WD Alarms ***13 of 16***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
22 S8300	MIN	“Application <name> (<pid>) terminated” — Watchdog successfully shut down the named application, and (if appropriate) watchdog will try to restart it. 1. To verify the alarm, look for the application’s name or process ID (PID), either using the: - Web interface, by selecting **Diagnostics > View System Logs** and **Watchdog Logs** - Linux command line, by entering **`logv -w`** 2. On the standby server, look for occurrences of the **`stop`** command, either from the: - Web interface, by: a. Selecting **View System Logs** b. Selecting **Platform command history log** c. Specifying the **Event Range** for the appropriate time frame d. Matching the “Stop” pattern - Linux command line, by entering **`listhistory`** 3. If a **`stop`** command was **in**appropriately executed, prevent any future misuse of the **`stop`** command. **Note:** From the system’s perspective, this is normal behavior. However, in terms of potential service outage due to human error, this is quite irregular. (Shutting down a server effectively downgrades a duplex-, high- or critical-reliability system to an unsupported standard-reliability system.) 4. If **`listhistory`** shows no **`stop`** commands, then Watchdog responded to abnormal internal processes by shutting down the application. Check the trace log for information about this application, either from the: - Web interface, by: a. Selecting the **View System Logs** diagnostic and **Logmanager Debug** trace b. Specifying the **Event Range** for the appropriate time frame c. Matching the application’s PID as the pattern - Linux command line, by entering **`logv -t ts`**
		13 of 16

Table 40: _WD Alarms ***14 of 16***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
22 S8300 (cont'd)	MIN	5. Manually clear the alarm, either from the: - Web interface, by selecting **Alarms and Notification**, the appropriate alarm, and **Clear** - Linux command line, by entering **`almclear -n`** ***`#id`*** 6. Watch to see if the alarm recurs. If so, escalate the problem.
23 S8300	MAJ	"Watchd high-monitor thread is rebooting the system" — The: 1. Lo-monitor thread is missing heartbeats (can't get CPU time). 2. Hi-monitor thread has tried 3 times to recover the system by killing any infinitely looping processes. If after 3 CPU-occupancy profiles and recoveries, the lo-monitor thread is still not heartbeating, then Watchd reboots the server. 3. To verify the alarm, look for messages: Containing the CPU profiling results and attempted recoveries Stating that Watchd is rebooting the server using either the: - Web interface, by selecting **Diagnostics > View System Logs** and **Watchdog Logs** - Linux command line, by entering **`logv -w`** or, directly, by examining `/var/log/ecs/wdlog`. A resolution is probably unnecessary. The server has usually rebooted by the time a technician can analyze the system. (A reboot clears the alarm and normally fixes problems with unresponsive software.) 4. Watch to see if the alarm recurs. If so, escalate the problem.
		14 of 16

Table 40: _WD Alarms ***15 of 16***

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
24 S8300	MAJ	“Watchd’s high-monitor thread is stopping tickling of hw” — Event ID #23’s call to reboot the server was unsuccessfully invoked. (A Linux kernel’s semaphore is possibly stuck.) After this happens, Watchd stops tickling the HW sanity timer so that the HW sanity watchdog executes a hard reboot of the processor. 1. To verify that the alarm occurred, look for messages about: Stopping the tickling of the HW sanity timer CPU occupancy profiling using either the: - Web interface, by selecting **Diagnostics > View System Logs** and **Watchdog Logs** - Linux command line, by entering **`logv -w`** or, directly, by examining `/var/log/ecs/wdlog`. - If the HW sanity watchdog successfully executed a hard reboot, the alarm was cleared. (This reboot normally fixes problems due to unresponsive software.) If **not**, power cycle the server to release it from this condition and to clear the alarm. 2. Watch to see if the alarm recurs. If **`so`**, escalate the problem.
26	MIN	“Watchd handshake error” — IF USB alarms are also present, this strongly points to a global SAMP or networking problem. This error implies: • the SAMP is missing • the SAMP is malfunctioning • the SAMP is not configured properly • the firewall on the server is not configured • the SAMP firmware is not correct for the Communication Manager version • the server Ethernet port is misconfigured. 1. Refer to the SAMP User Guide for troubleshooting procedures (03-300322). 2. Escalate the problem.
		15 of 16

Table 40: _WD Alarms ***16 of 16***

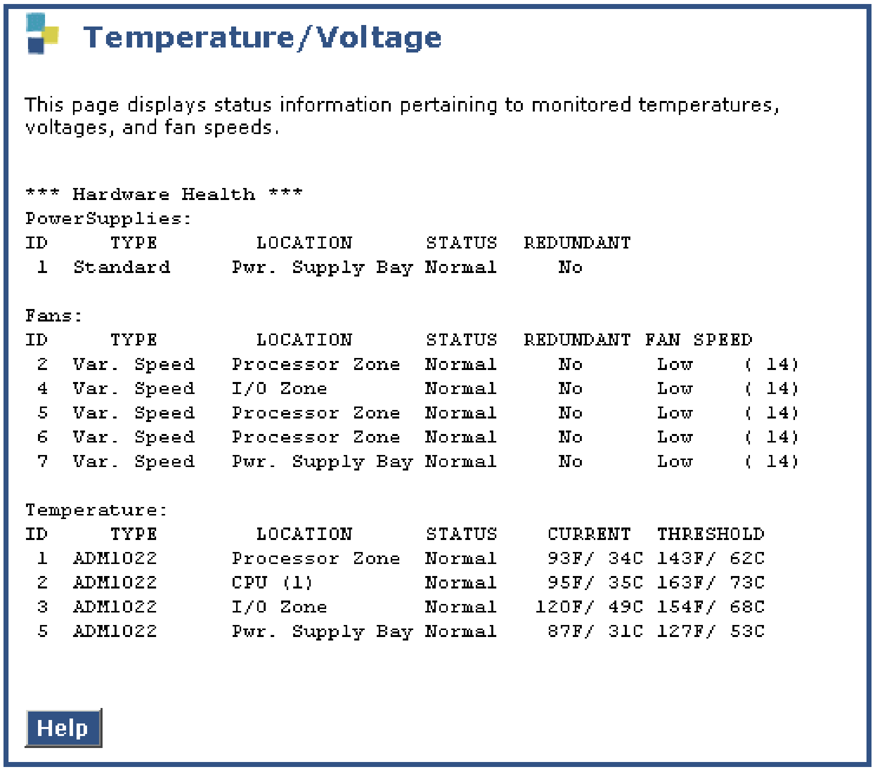
Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
27	MAJ	"Free memory on the system is low" — 1. To verify that the alarm occurred, look for messages about: Stopping the tickling of the HW sanity timer CPU occupancy profiling using either the: - Web interface, by selecting **Diagnostics > View System Logs** and **Watchdog Logs** - Linux command line, by entering **`logv -w`** or, directly, by examining `/var/log/ecs/wdlog`.
		16 of 16

Back to: Linux Server Alarms

S8710 ENV Alarms

To check the S8710 server temperature and voltage readings:

1. On the Maintenance Web Page, select **Diagnostics > Temperature/Voltage**.
2. The **Temperature/Voltage** page is displayed.



This page displays status information pertaining to monitored temperatures, voltages, and fan speeds.

```
*** Hardware Health ***
PowerSupplies:
ID      TYPE         LOCATION      STATUS   REDUNDANT
 1  Standard     Pwr. Supply Bay Normal     No

Fans:
ID      TYPE         LOCATION      STATUS   REDUNDANT FAN SPEED
 2  Var. Speed   Processor Zone  Normal     No       Low    ( 14)
 4  Var. Speed   I/O Zone        Normal     No       Low    ( 14)
 5  Var. Speed   Processor Zone  Normal     No       Low    ( 14)
 6  Var. Speed   Processor Zone  Normal     No       Low    ( 14)
 7  Var. Speed   Pwr. Supply Bay Normal     No       Low    ( 14)

Temperature:
ID      TYPE         LOCATION      STATUS     CURRENT  THRESHOLD
 1  ADM1022      Processor Zone  Normal    93F/ 34C 143F/ 62C
 2  ADM1022      CPU (1)         Normal    95F/ 35C 163F/ 73C
 3  ADM1022      I/O Zone        Normal   120F/ 49C 154F/ 68C
 5  ADM1022      Pwr. Supply Bay Normal    87F/ 31C 127F/ 53C
```

3. Use the descriptions in Table 41 to interpret the report.

Table 41: S8710 Temperature and voltage report

Field	Description
ID	An identification number automatically generated by the system.
Type	**Power supply**: • **Intelligent**—power regulating • **Standard**—other **Fan**: speeds include • **Var Speed**—variable speed • **Basic Fan**—fixed speed • **Auto. Speed**—automatic speed fan • **Pwr Supply**—power supply • **Unknown** **Temperature**: **Basic Sensor**—generic; **ADM1022**; **Internal PS**; **Unknown Type**
Location	The device location in the server.
Status	For power supplies and fans: • **Normal**—operating normally • **Alarm**—having a problem
Redundant	For all types: **Yes**, **No**, or **NA**
Fan Speed	**Fans**: percentage of full speed. • **Unknown** • **Automatic**—For Auto. Speed Fans, no speed state • **Low**—< 30% • **Medium**—30%–70% • **High**—> 70%, reporting state: High state • **Normal**—reporting state: Normal state • **Off**
Current	**Temperature**: current temperature of the device, in degrees Fahrenheit and Celsius.
Threshold	**Temperature**: above for which an alarm is generated, in degrees Fahrenheit and Celsius.

S8710 Server BIOS Error Messages

The S8710 server BIOS error messages are listed and interpreted in Table 42: S8710 BIOS error messages.

Table 42: S8710 BIOS error messages

Error Code	Description	Audible Beeps	Possible Problem	Possible Action
207	Memory configuration warning; DIMM in DIMM Socket X is not 4 bytes wide (32 bits) and only supports standard ECC.	None	Installed DIMMs are 8 bytes wide (64 bits).	Escalate; replace the server
209	Online spare memory configuration; spare bank is invalid. Mixing of DIMMs with 4 and 8 byte widths is not allowed in this mode.	One long and one short	Installed DIMMs for online spare bank are of a different primary width than the DIMMs in other banks.	Escalate; replace the server
NA	A mixture of 533-MHz and 400-MHz front side bus speed processors detected. All processors must have the same front side bus speed. System halted.	One long and one short	Wrong processors; Processors have different front side bus speeds.	Escalate; replace the server
NA	server only supports 400-MHz front side bus speed processors. One or more 533-MHz front side bus speed processors have been initialized at 400 MHz.	One long and one short	Wrong processors; server does not support a front side bus speed of 533 MHz.	Escalate; replace the server

Back to: Linux Server Alarms

RAID controller cache mode and battery condition alarm

The S8800 and HP DL360 G7 servers raise an alarm for the RAID cache backup battery condition and cache mode. If the battery fails or the RAID controller is in write through mode the S8800 and HP DL360 G7 servers raise a major alarm.

Use **`almdisplay -v`** to display the list of outstanding messaging, Communication Manager, and server alarms.

The following two alarms are an example of the HP DL360G7 and S8800 servers alarms:

```
ID   Source     EvtID  Lvl  Ack  Date                            Description
1    HARD DISK  77     MAJ  N    Thu Oct 13 12:26:55    RAID Controller is
                                 EDT 2011              currently in write through mode

0    HARD DISK  78     MAJ  Y    Sun May 05 15:29:27    RAID Controller RAID battery
                                  EDT 2002              capacity is too low
```

The following alarm is an example of the S8800 server only alarm:

```
ID  Source     EvtID  Lvl  Ack   Date                          Description
0   HARD DISK  68     MIN  Y     Sun May 05 15:29:27    RAID Controller default cache
                                 EDT 2002                     setting is write through
```

Table 1: RAID Controller cache mode alarms

Event ID	Alarm Level	Alarm Text, Cause/Description, Recommendation
1	MAJ	RAID Controller is currently in write through mode. The RAID controller can be in write through mode due to low battery. You must first replace the battery. For more information about how to replace the battery, contact your Avaya Support Representative.
0	MAJ	RAID Controller RAID battery capacity is too low. You must replace the battery.

For more information about how to replace the HP DL360G7 battery, see *Maintaining and Troubleshooting the HP ProLiant DL360 G7 Server*, 03-603803.

Back to: Linux Server Alarms