Avaya Aura® Communication Manager Server Alarms

Release 6.3
03-602798
Issue 6
June 2014

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.

For full support, please see the complete document, Avaya Support Notices for Hardware Documentation, document number 03–600759.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees 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 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 its hardware and Software (“Product(s)”). 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://support.avaya.com.

Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto.

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; 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 you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. 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 you. “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.

License type(s)

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order 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.

Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Named User License (NU). You 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 (e.g., 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). You 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”)

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product 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 unless expressly authorized by Avaya. 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.

Virtualization

Each virtual appliance has its own ordering code. Note that each instance of a virtual appliance must be ordered separately. If the end-user customer or Business Partner wants to install two of the same type of virtual appliances, then two virtual appliances of that type must be ordered.

Third-party components

Certain software programs or portions thereof included in the Software may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for those product that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/ThirdPartyLicense/

You agree to the Third Party Terms for any such Third Party Components.

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

How to Get Help

For additional support telephone numbers, go to the Avaya support website: http://support.avaya.com. If you are:

- Within the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the appropriate link for the type of support that you need.
- Outside the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the International Services link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that can be accessed by this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it might result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you — Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers must carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

- IEC 60950-1 latest edition, including all relevant national deviations as listed in the IECEE Bulletin—Product Category OFF: IT and Office Equipment.
- CAN/CSA-C22.2 No. 60950-1 / UL 60950-1 latest edition.

This product may contain Class 1 laser devices.

- Class 1 Laser Product
- Luokan 1 Laserlaite
- Klass 1 Laser Apparat

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards, as applicable:

- CISPR 22, including all national standards based on CISPR 22.
- CISPR 24, including all national standards based on CISPR 24.
- IEC 61000-3-2 and IEC 61000-3-3.

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment is the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. might void the user's authority to operate this equipment.

Federal Communications Commission Part 15 Statement:

For a Class A digital device or peripheral:

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

For a Class B digital device or peripheral:

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Equipment With Direct Inward Dialing ("DID"):

Allowing this equipment to be operated in such a manner as to not provide proper answer supervision is a violation of Part 68 of the FCC's rules.

Proper Answer Supervision is when:

1. This equipment returns answer supervision to the public switched telephone network (PSTN) when DID calls are:

- answered by the called station,
- answered by the attendant,
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user
- Routed to a dial prompt

2. This equipment returns answer supervision signals on all (DID) calls forwarded back to the PSTN.

Permissible exceptions are:

- A call is unanswered
- A busy tone is received
- A reorder tone is received

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

Automatic Dialers:

When programming emergency numbers and (or) making test calls to emergency numbers:

- Remain on the line and briefly explain to the dispatcher the reason for the call.
- Perform such activities in the off-peak hours, such as early morning or late evenings.

Toll Restriction and least Cost Routing Equipment:

The software contained in this equipment to allow user access to the network must be upgraded to recognize newly established network area codes and exchange codes as they are placed into service.

Failure to upgrade the premises systems or peripheral equipment to recognize the new codes as they are established will restrict the customer and the customer's employees from gaining access to the network and to these codes.

For equipment approved prior to July 23, 2001:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For equipment approved after July 23, 2001:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council on Terminal Attachments (ACTA). On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXX. If requested, this number must be provided to the telephone company.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0.

L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas cinq.

To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXX. The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Means of Connection:

Connection of this equipment to the telephone network is shown in the following table:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2.T	AS.2	RJ2GX, RJ21X, RJ11C
CO trunk	02GS2	0.3A	RJ21X, RJ11C
	02LS2	0.3A	RJ21X, RJ11C
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9.BN	6.0F	RJ48C, RJ48M
	04DU9.1KN	6.0F	RJ48C, RJ48M
	04DU9.1SN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9.DN	6.0Y	RJ48C

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242-2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Installation and Repairs

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. It is recommended that repairs be performed by Avaya certified technicians.

FCC Part 68 Supplier's Declarations of Conformity

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

Canadian Conformity Information

This Class A (or B) digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A (ou B) est conforme à la norme NMB-003 du Canada.

This product meets the applicable Industry Canada technical specifications/Le présent materiel est conforme aux specifications techniques applicables d'Industrie Canada.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (Conformité Europeénne) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (2004/108/EC) and Low Voltage Directive (2006/95/EC).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

European Union Battery Directive

Avaya Inc. supports European Union Battery Directive 2006/66/EC. Certain Avaya Inc. products contain lithium batteries. These batteries are not customer or field replaceable parts. Do not disassemble. Batteries may pose a hazard if mishandled.

Japan

The power cord set included in the shipment or associated with the product is meant to be used with the said product only. Do not use the cord set for any other purpose. Any non-recommended usage could lead to hazardous incidents like fire disaster, electric shock, and faulty operation.

本製品に同梱または付属している電源コードセットは、本製品専用です。本製品以外の製品ならびに他の用途で使用しないでください。火災、感電、故障の原因となります。

If this is a Class A device:

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラス Ａ 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

If this is a Class B device:

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラス Ｂ 情報技術装置です。この装置は，家庭環境で使用することを目的としていますが，この装置がラジオやテレビジョン受信機に近接して使用されると，受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation 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 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.

"Avaya" and "Avaya Aura" are the registered trademarks of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading documents

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

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product.

For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

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. The document also lists alarm identifications, levels, and resolutions.

Intended audience

The intended audience of this document are telecommunications managers and telephony administrators.

Document changes since last issue

The following change have been made to this document since the last issue:

- Added TGP-USG alarms

Related resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Maintenance and Troubleshooting		
Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers, 03-300430	Describes the alarms for Communication Manager.	Implementation Engineers, Support Personnel
Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers, 03-300431	Describes the alarms for Communication Manager.	Implementation Engineers, Support Personnel
Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers, 03-300432	Describes the maintenance procedures for Communication Manager.	Implementation Engineers, Support Personnel

Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Course code	Course title
AT101672	Avaya Aura® Communication Manager Fundamentals
AT102348	Avaya Aura® Communication Manager Implementation

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com, select the product name, and select the videos checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Note:

Videos are not available for all products.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. On the Avaya Support website at http://support.avaya.com, search for notices, release notes, downloads, user guides, and resolutions to issues. Use the Web service request system to create a service request. Chat with live agents to help answer questions. If an issue requires additional expertise, agents can quickly connect you to a support team.

Warranty

Avaya provides a 90-day limited warranty on Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at http://support.avaya.com

under **Help & Policies> Policies & Legal > Maintenance and Warranty Information**. See also **Help & Policies > Policies & Legal > License Terms**.

Chapter 2: Server Alarms

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 ongoing 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*.

The Error Log records all the errors. Communication Manager raises an alarm if a component incurs too many errors.

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 condition of network elements such as circuit packs, media modules, and their associated links, ports, and trunks.
- Messaging alarms provide the condition of embedded or external messaging systems.

Alarms may be viewed using the following:

- System Management Interface (SMI): 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.

To display information related to Communication Manager, the server, and messaging alarms, use the System Management Interface (SMI) or the server bash shell.

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

Server maintenance

Server maintenance focuses on the following functional roles:

- Provide the alarm logging and reporting service for all other system components.
- Provide support-specific interface and information for server duplication and maintenance software.
- Provide maintenance commands that the support technicians use to determine the condition of the system and perform repair or recovery actions or both.
- Provide server diagnostic, recovery, or notification mechanisms when a server processor is nonfunctional, that is, unable to execute the system software.

Alarm classifications

Alarms are classified depending on their impact 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 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.

Terminology

The following table gives an explanation of terms used in this document.

Table 1: Alarm terminology

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	A trap that is determined to be an alarm 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.
ISM	Intelligent Site Manager, a VPN gateway on customer LAN that provides a means for services personnel to access the customer 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.

Alarm logs

A user can view alarms using 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 you enter the command **almdisplay** on the server command line, the system displays information from the text string in the following manner:

```
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
```

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, you can perform one of the following:

- Call INADS of the Avaya technical service center.
- Send an e-mail to specified destinations.
- Send 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

To clear a Communication Manager alarm, you must resolve the alarm. You can also use the **almclear** command to manually clear an alarm from the alarm log.

To help isolate a server problem, the third 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 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.

Chapter 3: Linux Server Alarm Types

ARB (Arbiter)

The Arbiter process runs on duplicated servers to:

- Decide which server is in good condition and more able to be active
- Coordinate data shadowing between servers under the control of Duplication Manager

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 perform the following functions:

- 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.

ARB alarms

The following table lists the Arbiter alarms and the related troubleshooting procedures.

Table 2: ARB alarms

Event ID	Link to description
3	See ARB Event ID 3 on page 20.
7	See ARB Event ID 7 on page 21.
8	See ARB Event ID 8 on page 21.
9	See ARB Event ID 9 on page 22.
11	See ARB Event ID 11 on page 24.
12	See ARB Event ID 12 on page 25.
13	See ARB Event ID 13 on page 26.
	1 of 2

Table 2: ARB alarms

Event ID	Link to description
14	See ARB Event ID 14 on page 27
	2 of 2

ARB Event ID 3

Alarm level

MIN

Alarm text

`Interchange handoff failed`

Cause

The standby server could not process the interchange request of the active server. The interchange does not occur, and the active side remains active.

Resolution

- Using the Web interface:
  1. From the **Server** section of the Web interface, select **View Summary Status** to see if the standby side is RESET.
  2. To manually clear the alarm, select **Alarms and Notification** and the appropriate alarm, and click **Clear**.
  3. If the problem persists, troubleshoot the standby server:
     a. Check if the standby side is RESET. From the **Server** section of the Web interface, 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 necessary repairs.
  4. If the applications and interfaces are okay but the problem persists, go to the Avaya Support website at http://support.avaya.com to open a service request.
- Using the Linux command line interface
  1. Enter `server` and check if the standby side is RESET.
  2. Enter `almclear -n #id` to manually clear the alarm.
  3. 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.

4. If the applications and interfaces are okay but the problem persists, go to the Avaya Support website at http://support.avaya.com to open a service request.

ARB Event ID 7

Alarm level

MAJ

Alarm text

`Arbiter in invalid/unknown state`

Cause

Memory corruption or bad code/build.

Resolution

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 is fixed. Otherwise, proceed to step 2.

2. If the `arbiter` file is OK or if the problem persists, go to the Avaya Support website at http://support.avaya.com to open a service request.

ARB Event ID 8

Alarm level

MIN

Aalrm text

`Both servers thought they were active`

Resolution

- Using the Web interface:

1. From the **Server** section of the Web interface, select **View Summary Status** and verify that both the servers are active.
2. To distinguish the cause, examine the trace logs for Interarbiter messages with timestamps shortly before to shortly after the loss of heartbeat by:
   - Selecting the **View System Logs** diagnostic and **Logmanager Debug** trace.
   - Specifying the **Event Range** for the appropriate time frame.
   - Matching the **Interarb** pattern.
3. Depending on the cause, continue with either Step 1 or Step 2.

- Using the Linux command line interface:
  1. Enter **`server`** and verify that both servers are active.
  2. 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`**.
  3. Depending on the cause, contiue with either Step 1 or Step 2.
- 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 must leave the newly active server active, while the other server backs down to the standby role.
  1. If one server is active and the other is standby, manually clear the alarm:
     - From the Web interface, select **Alarms and Notification** and the appropriate alarm, and click **Clear.**
     - From the Linux command line, enter **`almclear -n #id.`**
  2. If the problem persists, go to the Avaya Support website at http://support.avaya.com to open a service request.
- Every Interarbiter link is down or misconfigured.
  1. Check for problems with an Ethernet interface:
     - From the Web interface, select the **Execute Pingall** diagnostic.
     - From the Linux command line, enter **`pingall -a.`**

     Check both sides of each failed link, and make necessary repairs.
  2. If the links are OK but the problem persists, go to the Avaya Support website at http://support.avaya.com to open a service request.

ARB Event ID 9

Alarm level

WRN

Cause

Before an interchange, the standby server is significantly in better condition than the active server requesting the interchange. The active server is probably unable to sustain call processing.

Resolution

1. Compare the condition of both servers:
   - From the **Server** section of the Web interface, select **View Summary Status.**
   - From the Linux command line, enter **`server.`**
2. Using the output from Step 1, check the status of the individual processes of each server.
3. Check the status of the individual processes of the active server:
   - From the Web interface, select **View Process Status.**
   - From the Linux command line, enter **`statapp.`**

   After checking the status of the individual processes, restore any applications that have problems.
4. Check if the standby side is RESET:
   - From the **Server** section of the Web interface, select **View Summary Status.**
   - From the Linux command line, enter **`server.`**
5. Check the status of the individual processes of the standby server:
   - From the Web interface, select **View Process Status.**
   - From the Linux command line, enter **`statapp.`**

   After checking the status of the individual processes, restore any applications that have problems.
6. Check for problems with an Ethernet interface:
   - From the Web interface, select the **Execute Pingall** diagnostic.
   - From the Linux command line, enter **`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 if all ethernet ports have been assigned IP addresses. Enter **`/sbin/arp -a`** to ensure that none of the MAC addresses display the `incomplete` message.
7. If the applications and interfaces of the standby server are OK but the problem persists, go to the Avaya Support website at http://support.avaya.com to open a service request.

   After the interchange, the condition of the newly active server must be better than the condition of the standby server. See the SOH values "bb" and "cc". See String pairs of ARB Event #9. The server with the larger "bb" value is considered to be in better condition. If the value of "bb" is the same for both the servers, the server with the larger "cc" value is considered to be in better condition. If the condition of the newly active server is better than the condition of the standby server, troubleshoot the standby server.

   If the condition of the standby server is better than the newly active server:

a. Manually clear the alarm:
   - From the Web interface, select **Alarms and Notification** and the appropriate alarm, and click **Clear.**
   - From the Linux command line, enter **`almclear -n #id.`**

b. If the problem persists, go to the Avaya Support website at http://support.avaya.com to open a service request.

ARB Event ID 11

Alarm level

WRN

Alarm text

`Cannot create receive socket.`

`Cannot create transmit socket.`

`Cannot bind receive socket.`

`Cannot (re)bind send socket.`

Cause

Since the Arbiter continuously attempts to create or bind the socket, the problem might resolve itself. Once resolved, the Arbiter can send and receive every Interarbiter link with no subsequent error messages in the trace log.

Resolution

1. To examine the alarm log to distinguish between a bind or create problem or a send or receive problem:
   - From the Web interface:
     a. Select **Alarms and Notification** and the appropriate alarm
     b. Select the **View System Logs** diagnostic
     c. Select the **Logmanager Debug** trace
     d. Specify the **Event Range** for the appropriate time frame
     e. Match the “cannot create” pattern
   - From the Linux command line, enter **`almdisplay -v.`**
2. Check for completeness and consistency of the `hosts` and `servers.conf` files (containing IP addresses of the configured components of the system) located on the servers:
   - From the Web interface select **Configure Server.**

- From the Linux command line, enter:

  ```
  more /etc/hosts
  more /etc/opt/ecs/servers.conf
  ```

  The Arbiter uses port number 1332 for sockets. Enter **`netstat -a | grep 1332`** to check if the alarm is still active. This command displays an output similar to the following:

  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 match and there are no alarms for port 1332, manually clear the alarm:
   - From the Web interface, select **Alarms and Notification** and the appropriate alarm, and click **Clear.**
   - From the Linux command line, enter **`almclear -n #id.`**
4. If this problem affects call processing or if the problem persists, continue with Step 6. If this problem does not affect call processing or if the problem has resolved, continue only at the convenience of the customer.
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 the suspected server is not the standby, enter **`server -if`** to force a server interchange. Busyout the standby server from the Linux command line by entering **`server -b`**.
   c. Reboot the server (as the standby):
      - From the Web interface, select **Shutdown This Server.**
      - From the Linux command line, enter

        ```
        /sbin/shutdown -r now
        ```
6. If rebooting the standby server does not help *or* if the problem persists, go to the Avaya Support website at http://support.avaya.com to open a service request.

ARB Event ID 12

Alarm level

MIN

Alarm text

```
Interchange without doing prep
```

Cause

Since the Arbiter cannot create a thread to request file synchronization, some files did not get shadowed.

Resolution

1. Examine the trace logs for the entry, `Can't create interchange-prep thread`:
   - From the Web interface:
     a. Select the **View System Logs** diagnostic and **Logmanager Debug** trace
     b. Specify the **Event Range** for the appropriate time frame
     c. Match the “interchange-prep” pattern
   - From the Linux command line, enter **`logv -t ts`**
2. Resubmit any translation changes using the **`save_trans`** command.
3. Manually clear the alarm:
   - From the Web interface, select **Alarms and Notification** and the appropriate alarm, and click **Clear.**
   - From Linux command line, enter **`almclear -n #id.`**

ARB Event ID 13

Alarm level

MIN

Alarm text

`Heartbeat timeout from ACTIVE`

Cause

The two possible causes for this event are:

- 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 corrects itself by the time the problem is detected and corrective action is not required.

Resolution

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 in to the alternate server and verify that the MAC addresses match. Do this from both servers.
3. Check for a mismatch in the MAC addresses that indicates the presence of a third system posing as a doppelganger.
4. Use a network sniffer to find the third main server.

ARB Event ID 14

Alarm level

MIN

Alarm text

`Standby failed to come back up`

Cause

The standby server in a duplex system is nonoperational for longer than 15 minutes and cannot generate alarm on its own behalf. Typical causes are:

- The rolling Linux reboots due to reloading of a rolling Communication Manager or a failure to start Communication Manager.
- A server was turned 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.

Resolution

Go to the Avaya Support website at http://support.avaya.com to open a service request.

Related topics

String pairs of ARB Event # 9 on page 27

String pairs of ARB Event # 9

ARB Event #9 generates pairs of SOH strings. In each string pair, the first string represents the active and the second string represents the standby SOH of the server just *before* an interchange.

Since, unless prevented by external circumstances, Event 9 triggers a server interchange, the first string normally represents a less efficient server – which became the standby. So, the data of the first string is more pertinent.

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.

- For “bb” and “cc,” "bb" indicates the number of PNs with IPSI 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-Survivable Core Servers, different values within the *same* string indicate a problem with controlling one or more IPSI-connected PNs.

  A PN reset can cause both the strings of the server to reflect equally degraded condition, but that event (in itself) must 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

BKP (Backup)

The system generates a backup (BKP) alarm only when a scheduled backup job fails. A backup now job does not have a BKP alarm.

The following table lists the Backup alarms and the related troubleshooting procedures.

Table 3: BKP Alarms

Event ID	Link to description
10	See BKP Event ID 10 on page 28.

BKP Event ID 10

Alarm level

MAJ

Alarm text

`Scheduled backup was terminated`

Resolution

1. Log in to Communication Manager System Management Interface.
2. Click **Data Backup/Restore** > **Backup Logs**.

Attempting another scheduled backup

1. Log in to Communication Manager System Management Interface.
2. Click **Data Backup/Restore** > **Schedule Backup**.

CAUTION:
Attempting to restore a failed backup is not a valid recommendation since there is no backup image to restore.

CMG (Common Media Gateway)

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

DUP (Duplication Manager)

The Duplication Manager process in coordination with the Arbiter process runs on the servers to control data shadowing between the servers.

At the physical and data-link layers, an Ethernet-based duplication link provides a TCP communication path between the Duplication Manager of each server to control 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.

DUP alarms

The following table lists the Duplication Manager alarms and the related troubleshooting procedures.

Table 4: DUP alarms

Event ID	Link to description
2	See DUP Event ID 2 on page 30.
6	See DUP Event ID 6 on page 31.

DUP Event ID 2

Alarm level

MAJ

Alarm text

`Duplication link down`

Cause

One Duplication Manager server cannot communicate with the other Duplication Manager server.

Resolution

- Using the Web interface:
  1. Access the trace log:
     a. Select the **View System Logs** diagnostic and **Logmanager Debug** trace
     b. Specify the **Event Range** for the appropriate time frame
     c. Match the “ndm” or "DUPLICATION" pattern
  2. Examine the output of the trace-log query for one of the following 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 status is “up” from the **Server** section of the Web interface by selecting **View Summary Status.**
  4. If the dup link status is "up", manually clear the alarm by selecting **Alarms and Notification** and the appropriate alarm, and click **Clear.**

     If the dup link status does not show "up", check the Ethernet interface of the duplication interface by selecting the **Execute Pingall** diagnostic.
  5. If **`pingall`** passes, check the applications of the other server by selecting **View Process Status.**
- Using the Linux command line interface
  1. Access the trace log by entering **`logv -t ts.`**
  2. Examine the output of trace-log query for one of the following 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. Enter **`server`** and check if the dup link is "up."
  4. If the dup link status shows "up", manually clear the alarm by entering **`almclear -n #id.`**

5. If the dup link status does not show "up", check the Ethernet connectivity of the duplication interface by entering **pingall -d.**
6. If **pingall** passes, enter **statapp** and check the applications of the other server.

DUP Event ID 6

Alarm text

Incorrect duplication link speed

Cause

This alarm is generated when the NIC (Network Interface Card) that is used for the duplication does not have 1 GB capacity, when the cable is not functioning properly, or when Communication Manager does not have Ethernet with 1 GB capacity.

ENV (Environment)

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

Release 6.0 and later, ENV alarms are generated by System Platform.

Event IDs with an alarm level of RES indicate that the problem has been cleared.

The following table lists the Environment alarms and the related troubleshooting procedures.

Table 5: ENV Alarms

Event ID	Link to description
32 G450	See ENV Event ID 32 G450 on page 32.
33 G450	See ENV Event ID 33 G450 on page 32.
34 G450	See ENV Event ID 34 G450 on page 32.
38	See ENV Event ID 38 on page 33.
39	See ENV Event ID 39 on page 33.

ENV Event ID 32 G450

Alarm level

MAJ

Alarm text

`G450 Fan Tray`

Cause

There is a problem with the fan tray on the G450.

Resolution

Reinsert or replace the fan tray.

ENV Event ID 33 G450

Alarm level

MAJ

Alarm text

`G450 Power Supply # 1`

Cause

There is a problem with Power Supply # 1 on the G450.

Resolution

Reinsert or replace Power Supply #1.

ENV Event ID 34 G450

Alarm level

MAJ

Alarm text

`G450 Power Supply # 2`

Cause

There is a problem with Power Supply # 2 on the G450.

Resolution

Reinsert or replace Power Supply #2.

ENV Event ID 38

Alarm level

MIN

Alarm text

`ENV_SP_HEALTH_DEGRADED`

Cause

When this alarm is generated, the system checks the cdom to see why the alarm was passed from System Platform to Communication Manager.

ENV Event ID 39

Alarm level

MAJ

Alarm text

`ENV_SP_HEALTH_GRAVE`

Cause

When this alarm is generated, the system checks the cdom to see why the alarm was passed from System Platform to Communication Manager.

Survivable Core Server

The following table describes the Survivable Core Server alarms and the related troubleshooting procedures.

Table 6: Survivable Core Server Alarms ***1 of 2***

Event ID	Link to description
1	See Survivable Core Server Event ID 1 on page 34.
2	See Survivable Core Server Event ID 2 on page 34.
3	See Survivable Core Server Event ID 3 on page 35.
	1 of 2

Table 6: Survivable Core Server Alarms ***2 of 2***

Event ID	Link to description
4	See Survivable Core Server Event ID 4 on page 35.
5	See Survivable Core Server Event ID 5 on page 35.
6	See Survivable Core Server Event ID 6 on page 35.
7	See Survivable Core Server Event ID 7 on page 36.
8	See Survivable Core Server Event ID 8 on page 36.
9	See Survivable Core Server Event ID 9 on page 36.
10	See Survivable Core Server Event ID 10 on page 37.
	2 of 2

Survivable Core Server Event ID 1

Alarm level

MIN

Alarm text

`Survivable Core Server not controlling IPSI PN XX: cls RRR`

Cause

Server of cluster RRR does not control IPSI port network XX

Survivable Core Server Event ID 2

Alarm level

MIN

Alarm text

`Survivable Core Server controlling IPSI PN XX: cls RRR`

Cause

Server of cluster RRR controls IPSI port network XX

Survivable Core Server Event ID 3

Alarm level

MIN

Alarm text

`Survivable Core Server not controlling non-IPSI PN XX: cls RRR`

Cause

Server of cluster RRR does not control non-IPSI port network XX

Survivable Core Server Event ID 4

Alarm level

MIN

Alarm text

`Survivable Core Server controlling non-IPSI PN XX: cls RRR`

Cause

Server of cluster RRR controls non-IPSI port network XX

Survivable Core Server Event ID 5

Alarm level

MIN

Alarm text

`Survivable Core Server not registered cls YYY: cls RRR`

Cause

Survivable Core Server cluster ID YYY is not registered to the active server of the main cluster. The main active server sends this trap for each Survivable Core Server in the system (RRR != YYY). A Survivable Core Server will only report status for itself (RRR = YYY).

Survivable Core Server Event ID 6

Alarm level

MIN

Alarm text

`Survivable Core Server registered cls YYY svid ZZZ: cls RRR`

Cause

Survivable Core Server server ID ZZZ of cluster ID YYY is registered to the active server of the main cluster. The active server of the main cluster sends this trap for each Survivable Core Server in the system (RRR != YYY). The Survivable Core Server will only report status for itself (RRR = YYY). A Survivable Core Server will only report status for itself (RRR = YYY).

Survivable Core Server Event ID 7

Alarm level

MIN

Alarm text

`Survivable Core Server changed to disable state: cls RRR`

Cause

Survivable Core Server cluster RRR is changed to the disable state.

Survivable Core Server Event ID 8

Alarm level

MIN

Alarm text

`Survivable Core Server changed to enable state: cls RRR`

Cause

Survivable Core Server cluster RRR is changed to the enable state.

Survivable Core Server Event ID 9

Alarm level

MIN

Alarm text

`IPSI (A/B) PN XX disconnected from Survivable Core Server: cls RRR`

Cause

Server of cluster RRR is not connected to IPSI (A/B) of port network XX. Each Survivable Core Server in the system reports this event for all the IPSIs that the RRR cluster connects to as specified by system administration, i.e., a local only Survivable Core Server will provide connection event status for the IPSIs assigned to it at Survivable Core Server's community.

Survivable Core Server Event ID 10

Alarm level

MIN

Alarm text

IPSI (A/B) PN XX connected to Survivable Core Server: cls RRR

Cause

Server of cluster RRR is connected to IPSI (A/B) of port network XX. Each Survivable Core Server in the system reports this event for all the IPSIs that the cluster connects to, as specified by system administration, i.e., a local only Survivable Core Server will provide connection event status for the IPSIs assigned to it at Survivable Core Server's community.

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.

There are two classes of FSY alarms, one class is associated with server communication failures and the other is associated with fileset configuration file errors.

The following table describes the FSY alarms and the related troubleshooting procedures.

Table 7: FSY Alarm in Server

Event ID	Link to description
1 - 999	See FSY Event ID 1 - 999 on page 38.
1000 - 1999	See FSY Event ID 1000 - 1999 on page 38.

FSY Event ID 1 - 999

Alarm level

MIN

Alarm text

`event string (server): [server address] type`

Examples:

- `filesync failure (server): 10.115.9.12 ESS`
- `alarm resolved (server): 10.115.9.36 ESS`
- `filesync failure (server): 10.115.9.25 LSP`

Description

Server communication errors use Event IDs in the of range of 1 - 999, where each Event ID is associated with a particular server and the IP address of the server. The source of these alarms is always server, which indicates the server connection problems.

The event string can be one of the following:

- `filesync failure` - The alarm is generated because of a failure.
- `alarm cleared` - The alarm has been cleared by using a command.
- `alarm resolved` - The latest filesync has succeeded.

The alarm text also includes the type of the server and the IP address of the server. The following are the different types of server:

- DUP
- ESS
- LSP

Cause

File synchronization operation failed due to a server communication error. The IP address and server type indicate which connection to diagnose.

Resolution

The type of the server and the IP address of the server indicate which connection should be diagonosed. For ESS and LSP server types, make sure that the server connection is working. For DUP server type, make sure that the Ethernet duplication link is working.

FSY Event ID 1000 - 1999

Alarm level

MIN

Alarm text

`event string (prescript): [fileset name] type`

Example:

- `filesync failure (prescript): trans DUP`

Description

Fileset configuration errors use Event IDs in the range of 1000 - 1999, where each Event ID is assiciated with a fileset. The source of these alarms is always prescript, which indicates that the prescript associated with the named fileset has failed on the local server.

Note:
The system does not detect postscript failures.

The event string can be one of the following:

- `filesync failure` - the alarm is generated because of a failure.
- `alarm cleared` - the alarm has been cleared by using a command.
- `alarm resolved` - a filesync that was previously failing is now no longer failing. The latest filesync has succeeded.

The alarm text also includes the type of the server and the name of the fileset. The name of the fileset is taken from the fileset configuration file, that is /etc/opt/ecs/filesync.conf. The following are the different types of server:

- DUP
- ESS
- LSP

Resolution

Go to the Avaya Support website at http://support.avaya.com to open a service request.

GW_ENV (Gateway Environment)

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 alarms for these events. However, Communication Manager generates a warning and sends the warning to the Fault and Performance Management (FPM) or the Secure Intelligent Gateway (SIG) or both 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

GW_ENV alarms

The following alarms apply to the G450 media gateway.

Table 8: GW_ENV Alarms

Event ID	Link to description
1	See GW_ENV Event ID 1 on page 40.
2	See GW_ENV Event ID 2 on page 41.
3	See GW_ENV Event ID 3 on page 41.
4	See GW_ENV Event ID 4 on page 41.
5	See GW_ENV Event ID 5 on page 41.
6	See GW_ENV Event ID 6 on page 42.
7	See GW_ENV Event ID 7 on page 42.
8	See GW_ENV Event ID 8 on page 42.
9	See GW_ENV Event ID 9 on page 42.
10	See GW_ENV Event ID 10 on page 42.

GW_ENV Event ID 1

Alarm level

MAJ

Alarm text

AvEntFanFlt - Fan fault

GW_ENV Event ID 2

Alarm level

MAJ

Alarm text

AvEnt48vPwrFlt - 48v Power fault

GW_ENV Event ID 3

Alarm level

MAJ

Alarm text

AvEnt48vPwrFlt - 48v Power faultAvEnt5vPwrFlt - 5v Power fault

GW_ENV Event ID 4

Alarm level

MAJ

Alarm text

AvEnt3300mvPwrFlt - 3300 mv Power fault

GW_ENV Event ID 5

Alarm level

MAJ

Alarm text

AvEnt2500mvPwrFlt - 2500 mv Power fault

GW_ENV Event ID 6

Alarm level

MAJ

Alarm text

AvEnt1800mvPwrFlt - 1800 mv Power fault

GW_ENV Event ID 7

Alarm level

MAJ

Alarm text

AvEnt1600mvPwrFlt - 1600 mv Power fault

GW_ENV Event ID 8

Alarm level

MAJ

Alarm text

AvEntAmbientTempFlt - Ambient temperature fault

GW_ENV Event ID 9

Alarm level

MAJ

Alarm text

avEntPhyChFruRemoval - Field replaceable unit removal

GW_ENV Event ID 10

Alarm level

MAJ

Alarm text

`avEntPhyChFruPsuFlt - Power supply fault.`

_LX (Linux)

The following table describes the server alarms for Linux and the related troubleshooting procedures.

Table 9: LX Server Alarms

Event ID	Link to description
3	See LX Event ID 3 on page 43.
4	See LX Event ID 4 on page 43.
5	See LX Event ID 5 on page 44.

LX Event ID 3

Alarm level

WRN

Alarm text

`OVERLOAD CONTROL LEVEL 1`

Cause

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.

LX Event ID 4

Alarm level

WRN

Alarm text

`OVERLOAD CONTROL LEVEL 2`

Cause

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.

LX Event ID 5

Alarm level

WRN

Cause

The system firewall might not be running on the system.

CAUTION:
Not having a fully functional system firewall is a serious security risk.

Resolution

1. Restart iptables by issuing the following command as root:
   `/etc/init.d/iptables restart`
2. Ensure that execute permission is enabled for the **/opt/ws/iptables** file.

Login Alarms

The system monitors access to the server and alarms suspicious activity. The following table lists the Login alarms and their related troubleshooting procedures.

For S8300D Server, see S8300 Server Login Alarms.

Table 10: Login Alarms ***1 of 2***

Event ID	Link to description
1	See Login Event ID 1 on page 45.
2	See Login Event ID 2 on page 45.
3	See Login Event ID 3 on page 45.
5	See Login Event ID 5 on page 46.
6	See Login Event ID 6 on page 46.
	1 of 2

Table 10: Login Alarms ***2 of 2***

Event ID	Link to description
7	See Login Event ID 7 on page 46.
8	See Login Event ID 8 on page 47.
10, 11, 12, and 13	See Login Event IDs 10, 11, 12, and 13 on page 47.
	2 of 2

Login Event ID 1

Alarm level

WRN

Cause

Successful Communication Manager login.

Login Event ID 2

Alarm level

MIN

Alarm text

`SAT_auth:Login for [inads] invalid password`

Resolution

1. Verify the alarm:
   - From the System Management Interface, select **Current Alarms**
   - From the Linux command line, enter **`almdisplay -v`**
2. Incorrectly typing a login sequence causes this alarm. Enter **`almclear -n`** ***`#id`*** to clear the alarm.
3. If this alarm occurs frequently, it may indicate a security threat. Notify the customer.

Login Event ID 3

Alarm level

WRN

Cause

Successful Linux login.

Login Event ID 5

Alarm level

MAJ

Alarm text

`Probation interval for login ends - lockout interval begins`

Cause

This alarm may indicate a security threat. Notify the customer.

Resolution

1. Using a services login, enter the command **`userlock -s`** on the Linux command line. This will display all active logins in the system, the number of failed logins, and whether the incorrect login attempt that raised the alarm is currently locked out.

Login Event ID 6

Alarm level

WRN

Cause

Lacfile missing.

Login Event ID 7

Alarm level

MAJ

Cause

Lacfile error - corrupt or expired authentication data

Login Event ID 8

Alarm level

MAJ

Cause

Access denied. Linux login failure. Access through illegal port.

Login Event IDs 10, 11, 12, and 13

Alarm level

MIN

Alarm text

`Login for [linux] - failed - password check`

Cause

A login attempt to access the Linux command line of a server failed.

Resolution

1. Verify the alarm:
   - From the System Management Interface, select **Current Alarms**
   - From the Linux command line, enter `almdisplay -v`
2. Incorrectly typing the login sequence causes this alarm. Enter `almclear -n #id` to clear the alarm.
3. If this occurs frequently, it may indicate a security threat. Notify the customer.

S8300D Server Login Alarms

The following table lists the S8300D Server login alarms and their troubleshooting procedures.

Table 11: S8300D Server Login Alarms *1 of 2*

Event ID	Link to description
1	See S8300D Event ID 1 on page 48.
	1 of 2

Table 11: S8300D Server Login Alarms *2 of 2*

Event ID	Link to description
2	See S8300D Event ID 2 on page 48.
3	See S8300D Event ID 3 on page 48.
4	See S8300D Event ID 4 on page 49.
5	See S8300D Event ID 5 on page 49.
	2 of 2

S8300D Event ID 1

Alarm level

WRN

Resolution

1. Using the Web Interface, select **View Current Alarms**.
2. Notify the customer.

S8300D Event ID 2

Alarm level

WRN

Resolution

1. Using the Web Interface, select **View Current Alarms**.
2. Notify the customer.

S8300D Event ID 3

Alarm level

MIN

Cause

Security violation.

Resolution

1. Using the Web Interface, select **View Current Alarms**.
2. Notify the customer.

S8300D Event ID 4

Alarm level

MIN

Cause

Security violation.

Resolution

1. Using the Web Interface, select **View Current Alarms**.
2. Notify the customer.

S8300D Event ID 5

Alarm level

MIN

Cause

Security violation.

Resolution

1. Using the Web Interface, select **View Current Alarms**.
2. Notify the customer.

_PE (Processor Ethernet) Alarms

The _PE Processor Ethernet alarms are raised on servers running the duplex template.

The following table lists Processor Ethernet alarms and the related troubleshooting procedures.

Table 12: PE alarms

Event ID	Link to description
_PE 1	See _PE 1 Minor alarm: PE Health Check device is not responding on page 50.
_PE 2	See _PE 2 Minor alarm: PE on the other server is not responding on page 50.
_PE 3	See _PE 3 Major alarm: Processor Ethernet service is down on page 51.
_PE 4	See _PE 4 Minor alarm: PE Priority configuration mismatch between servers on page 52.

_PE 1 Minor alarm: PE Health Check device is not responding

MO name in log

_PE 1

Alarm level

MIN

Alarm text

`Can't ping the PE Health Check device.`

Cause

Processor Ethernet (PE) Health Check device is not responding. Cannot ping the PE Health Check device.

Resolution

1. Log in to Communication Manager System Management Interface.
2. From the Installation menu, click **Configure Server**. The Configure Server wizard opens.
3. On the Configure Interfaces screen, verify if **IP address for PE Health Check** is set to the gateway address.

Execute the Ping diagnostics test to verify that the endpoint used for the PE Health Check device (the gateway) responds to a ping request. For more information about the Ping diagnostics test, see the System Management Interface **Help**.

_PE 2 Minor alarm: PE on the other server is not responding

MO name in log

_PE 2

Alarm level

MIN

Alarm text

`Can't ping the other server over the network used by the PE Interface.`

Cause

Processor Ethernet (PE) on the other server is not responding. Cannot ping the other server over the network used by the Processor Ethernet interface.

Resolution

1. Log in to Communication Manager System Management Interface.
2. Click the **Administration** tab and select **Server (Maintenance)**.
3. On the left navigation menu, click **Status Summary**. The system displays Status Summary screen.
4. Verify that the other server in the duplicated server pair is running and that the Processor Ethernet status is not **Down**.
   - If the other server in the duplicated server pair is not running, the status of Mode is **Not Ready** and the display of items such as "Alarms" are blank.
   - If he Processor Ethernet status is not **Down**, run the troubleshooting procedures for the alarms on the other server.

Execute the Ping diagnostic test to verify that the other server responds to a ping test. If it does not, execute the Ping diagnostics test from the other server to verify that it is connected to the corporate LAN.

_PE 3 Major alarm: Processor Ethernet service is down

MO name in log

_PE 3

Alarm level

MAJ

Alarm text

`Can't ping the device used for the PE Health Check or the IP interface used for the PE on the other server.`

Cause

Processor Ethernet service is down. Cannot ping the PE Health Check device and the IP interface used for the PE on the other server.

Resolution

1. Run the tests listed for the alarms associated with _PE 1 and _PE 2.
2. Verify if that the server is connected to the corporate LAN.
3. If NIC alarms are present, follow the troubleshooting procedures for those alarms. For more information, see Verify NIC Options Test (#1511) in *Maintenance Alarms for Avaya Aura® Communication Manager (03-300430)*.
4. Verify that the corporate LAN is working.

_PE 4 Minor alarm: PE Priority configuration mismatch between servers

MO name in log

_PE 4

Alarm level

MIN

Cause

The PE Interchange Priority setting on the Configure Interfaces page of the System Management Interface of one of the servers of a duplicated pair of server does not match the PE Interchange Priority setting on the Configure Interfaces page of the System Management Interface of the other server.

Resolution

1. On the Status Summary screen of System Management Interface, verify that the PE Interchange Priority setting on the active server is the same as the PE Interchange Priority setting on the standby server.
2. On the Configure Interface screen of System Management Interface (that displays the incorrect value) change the incorrect value of the PE Interchange Priority setting.

Note:
Make sure that the server on which you are changing the settings on the Configure Interface screen is on the standby server.

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.

The following table lists the Service Maintenance Engine alarms and the related troubleshooting procedures.

Table 13: SME Alarms

Event ID	Link to description
1	See SME Event ID 1 on page 53.
2	See SME Event ID 2 on page 54.

SME Event ID 1

Alarm level

MAJ

Alarm text

`Far end alarm service is down`

Cause

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).

Resolution

1. Look for any GMM failures on the other server, either using the:
   - From the Web interface, select **Diagnostics > View System Logs > Watchdog Logs**
   - From the Linux command line, enter **`logv -w`** or by examining the `/var/log/ecs/wdlog` log file.
2. If a GMM failure was found:
   a. Check if the GMM application is active:
      - From the Web interface, select **View Process Status**
      - From the Linux command line, enter **`statapp`**
   b. If the GMM application is active, continue with Step 3.

      If the GMM application is not active, try to restart this application by entering **`start -s GMM`** on the Linux command line.
   c. If the GMM application restarts successfully, continue with Step 4.

      If the GMM application fails to restart, go to the Avaya Support website at http://support.avaya.com to open a service request.
3. If a GMM failure was not found, check if alarm reporting failed by searching for the string “snd2Inads” in the trace log:

- From the Web interface:
  a. Select **View System Logs** diagnostic and **Logmanager Debug** trace
  b. Specify the “Event Range” for the appropriate time frame
  c. Match the “snd2Inads” pattern
- From the Linux command line, enter `logv -t ts`

4. Test the administered reporting mechanisms by entering `testinads` on the Linux command line.
5. Once the alarm is resolved, manually clear the alarm:
   - From the Web interface, select **Alarms and Notification** and the appropriate alarm, and click **Clear**
   - From the Linux command line, enter `almclear -n #id`

SME Event ID 2

Alarm level

WRN

Cause

For security only. If the IP address in the trap does not match UPS translations, this server is receiving a trap from an illegal source.

No action is needed.

STD (Standard SNMP Traps)

The following table lists STD traps and the related troubleshooting procedures.

Table 14: STD Alarms

Event ID	Description
1	See STD Event ID 1 *on page 55*.
2	See STD Event ID 2 *on page 55*.
3	See STD Event ID 3 *on page 55*.
3	See STD Event ID 3 *on page 56*.

STD Event ID 1

Alarm level

MIN

Alarm type

ACT

Alarm text

"coldStart" - Agent Up with Possible Changes

Cause

A coldStart trap indicates that the entity sending the protocol (SNMPv2) is reinitializing itself and this reinitialization process can either alter the agent configuration or entity implementation.

STD Event ID 2

Alarm level

MIN

Alarm type

ACT

Alarm text

"warmStart" - Agent Up with No Changes

Cause

A warmStart trap indicates that the entity sending the protocol (SNMPv2) is reinitializing itself and this reinitialization process keeps both the agent configuration and the entity implementation intact.

STD Event ID 3

Alarm level

MIN

Alarm type

ACT

Alarm text

"linkDown" - Agent Interface Down

Cause

A linkDown trap indicates that the entity sending the protocol (SNMPv2) recognizes a failure in one of the communication links represented in the agent 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.

STD Event ID 3

Alarm level

MIN

Alarm type

RES

Alarm text

`"linkUP" - Agent Interface Up`

Cause

A linkUp trap indicates that the entity sending the protocol (SNMPv2) recognizes that one of the communication links represented in the agent 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.

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.

The following table lists SVC_MON alarms and the related troubleshooting procedures.

Table 15: SVC_MON Alarms ***1 of 2***

Event ID	Link to description
2	See SVC MON Event ID 2 on page 57.
3	See SVC MON Event ID 3 on page 57.
	1 of 2

Table 15: SVC_MON Alarms *2 of 2*

Event ID	Link to description
4	See SVC MON Event ID 4 on page 58.
6	See SVC MON Event ID 6 on page 58.
5	See SVC MON Event ID 5 on page 58.
6	See SVC MON Event ID 6 on page 59.
7	See SVC MON Event ID 7 on page 59.
8	See SVC MON Event ID 8 on page 60.
	2 of 2

SVC MON Event ID 2

Alarm level

MIN

Alarm text

`service atd could not be restarted`

Cause

The Linux at daemon is down. Scheduled services such as session cleanup or daily filesync will not work.

Resolution

Enter **`service atd restart`** from the **`/sbin`** directory to restart the "at" daemon, and see Resolving SVC MON Event.

SVC MON Event ID 3

Alarm level

MIN

Alarm text

`service crond could not be restarted`

Cause

The Linux cron daemon is down. Periodic services such as session cleanup or daily filesync will not work.

Resolution

Enter **/sbin/service cron restart** from the **/sbin** directory to restart the cron daemon, and see Resolving SVC MON Event.

SVC MON Event ID 4

Alarm level

MIN

Alarm text

service xinetd could not be restarted

Cause

The Linux internet server daemon is down. Networking services will not work.

Resolution

Enter **/sbin/service inet restart** from the **/sbin** directory to restart the inet daemon, and see Resolving SVC MON Event.

SVC MON Event ID 6

Alarm level

MIN

Alarm text

service rsyslog could not be restarted

Cause

Linux “syslog” service is down. Event logging to syslog and alarm generation fails.

Resolution

Enter **/sbin/service rsyslog restart** from the **/sbin** directory to restart the syslog service, and see Resolving SVC MON Event.

SVC MON Event ID 5

Alarm level

MIN

Alarm text

service xintetd could not be restarted

Cause

The Linux network time protocol daemon is down. The server clock and recently logged time stamps may be inaccurate.

Resolution

Enter **/sbin/service xntpd restart** from the **/sbin** directory to restart the xntpd daemon, and see Resolving SVC MON Event.

SVC MON Event ID 6

Alarm level

MIN

Alarm text

service dbgserv could not be restarted

Cause

Debug server is down, and the Gemini debugger may not work. If this service stops running, debugging of a currently functional server is prevented, but the normal operations of a server are not affected.

Resolution

Enter **/sbin/service dbgserv restart** from the **/sbin** directory to restart the dbgserv service, and see Resolving SVC MON Event.

SVC MON Event ID 7

Alarm level

MIN

Alarm text

service prune could not be restarted

Cause

The prune service is not running. The partition usage of the hard disk is not being monitored or cleaned.

Resolution

Enter **/sbin/service prune restart** from the **/sbin** directory to restart the prune service, and see Resolving SVC MON Event.

SVC MON Event ID 8

Alarm level

MIN

Alarm text

`service ntpd could not be restarted`

Cause

The hypertext transfer protocol daemon is down. The Web interface will not work.

Resolution

Enter **`/sbin/service httpd restart`** from the **`/sbin`** directory to restart the http daemon, and see Resolving SVC MON Event.

Related Topics

Resolving SVC MON Event **on page 60**

Resolving SVC MON Event

1. If the daemon or the service restarts successfully, manually clear the alarm:
   - From the Web interface, select **Alarms and Notification** and the appropriate alarm, and click **Clear**
   - From the Linux command line, enter **`almclear -n #id`**

   If the daemon or the service fails to restart, go to the Avaya Support website at http://support.avaya.com to open a service request.

   a. Enter **`grep svc_mon /var/log/messages`** to determine why the daemon failed to restart.

   CAUTION:
   The following procedure causes a brief service outage and must be executed only at the convenience of the customer.

   b. If the output of the **`grep`** command does not help:
      - For duplicated servers, enter **`server`** to verify that the suspected server is the standby. If necessary and at the convenience of the customer, enter **`server -if`** to force a server interchange.
      - For non-duplicated servers, proceed to Step d.

   c. For duplicated servers, reboot the standby server:

- From the Web interface, select **Shutdown This Server**
- From the Linux command line, enter `/sbin/shutdown -r now`

d. For non-duplicated servers, reboot the server:

- From the Web interface, select **Shutdown This Server**
- From the Linux command line, enter `/sbin/shutdown -r now`

2. If rebooting the standby does not help or if the problem recurs, go to the Avaya Support website at http://support.avaya.com to open a service request.

TGP-USG (Trunk Group Usage)

The Trunk Group Usage alarm is observed on SIP type trunk groups when the administered threshold value for incoming or outgoing calls has been reached.

Note:
You can view the administered threshold value on the SIP trunk group screens only when MLPP and ASAC are enabled on the system.

The following table lists the TGP-USG alarms and the related troubleshooting procedures.

Table 16: TGP-USG alarms

Event ID	Link to description
1	See TGP-USG Event ID 1 on page 61.
2	See TGP-USG Event ID 2 on page 62.

TGP-USG Event ID 1

Alarm level

WRN

Cause

The administered threshold value for incoming calls has been reached.

Resolution

Ensure that the number of incoming calls is less than the administered threshold value.

TGP-USG Event ID 2

Alarm level

WRN

Cause

The administered threshold value for outgoing calls has been reached.

Resolution

Ensure that the number of outgoing calls is less than the administered threshold value.

TM (Translation Manager)

The Translation Manager monitors the ability of the server to read Communication Manager translations. The following table lists the TM alarms and the related troubleshooting procedures.

Table 17: TM Alarm

Event ID	Link to description
1	See TM Event ID 1 on page 62.

TM Event ID 1

Alarm level

MAJ

Alarm text

`Cannot read translations`

Cause

Server could not read translations. Usually, indicates a failure loading translations, but can also infrequently occur on a running system.

Duplicated servers: The servers spontaneously interchanged.

S8300 | S8500: The server rebooted.

Resolution

1. Check the integrity of the translation files xln1 and xln2 in /etc/opt/defty, and verify that they are of 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. Duplicated servers: Copy the translation files from the backup or the other server.
4. S8300 | S8510: 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 does not start, go to the Avaya Support website at http://support.avaya.com to open a service request.
7. After the error is resolved, manually clear the alarm:
   - From the Web interface, select **Alarms and Notification** and the appropriate alarm, and click **Clear**
   - From the Linux command line, enter **`almclear -n #id`**

UPG (Upgrade)

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

Table 18: UPG Alarms

Event ID	Link to description
1	See UPG Event ID 1 on page 63.

UPG Event ID 1

Alarm level

MAJ

Cause

The upgrade was not made permanent within two hours. No commit error.

Resolution

1. Make the upgrade permanent by using the web interface. Select **Server Upgrade > Make Upgrade Permanent**.

WD (Watchdog)

The Watchdog is a server process that performs the following:

- Creates other Communication Manager processes
- Monitors process status
- Recover process failures

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

The following table lists the Watchdog alarms and the related troubleshooting procedures.

Table 19: _WD Alarms

Event ID	Link to Description
4 S8300D	See WD Event ID 4 S8300D on page 65.
5	See WD Event ID 5 on page 66.
6 S8300D	See WD Event ID 6 S8300D on page 67.
7 S8300D	See WD Event ID 7 S8300D on page 68.
13 (Except S8500)	See WD Event ID 13 (Except S8500) on page 69.
14 (Except S8500)	See WD Event ID 14 (Except S8500) on page 70.
15 S8300D	See WD Event ID 15 S8300D on page 71.
18 S8300D	See WD Event ID 18 S8300D on page 72.
19 S8300D	See WD Event ID 19 S8300D on page 72.
20 S8300D	See WD Event ID 20 S8300D on page 73.
22 S8300D	See WD Event ID 22 S8300D on page 74.
23 S8300D	See WD Event ID 23 S8300D on page 76.
24 S8300D	See WD Event ID 24 S8300D on page 76.
26	See WD Event ID 26 on page 77.
27	See WD Event ID 27 on page 77.

WD Event ID 4 S8300D

Alarm level

MAJ

Alarm text

`Application <name> (pid) TOTALLY FAILED`

Cause

The application is present but cannot start. The application cannot start the maximum allowed number of times. This alarm occurs with Event ID #20.

Resolution

1. To verify the alarm, locate the application name or process ID (PID):
   - From the Web interface, select **Diagnostics > View System Logs > Watchdog Logs**
   - From the Linux command line, enter **`logv -w`** or by examining the `/var/log/ecs/wdlog` log file .
2. If the application is not running, enter **`start -s`** ***`application`*** to start the application.
3. If the application starts successfully, continue with Step 7.

   If the application fails to start, check the trace log to determine the reason why the application fails to start:
   - From the Web interface:
     a. Select **View System Logs** diagnostic and **Logmanager Debug** trace
     b. Specify the **Event Range** for the appropriate time frame
     c. Match the application PID as the pattern
   - From the Linux command line, enter **`logv -t ts`**

   Locate a related core-dump file in `/var/crash` directly, and go to the Avaya Support website at http://support.avaya.com to open a service request.
4. Check if the file named in the log exists and is executable.

   To locate the executable file of the application, enter the Linux command:

   **`ls -l /opt/ecs/sbin/`*`appl`*

   If the file is present, Linux returns a symbolic link to its location.
5. If the file is present:
   a. Enter **`ls -l`** on the address of the symbolic link.

b. Check if the file has “execute” permissions. If the file does not have execute permission, enter **chmod +x** to enable execution permission for the application.

If the file is not present, Linux has returned a “null link."

— Acquire the executable from the CD.

6. Enter **start -s *application*** to start the application.
7. Manually clear the alarm:
   — From the Web interface, select **Alarms and Notification** and the appropriate alarm, and click **Clear**
   — From the Linux command line, enter **almclear -n #*id***
8. If the problem persists, go to the Avaya Support website at http://support.avaya.com to open a service request.

WD Event ID 5

Alarm level

MIN

Alarm text

WARNING: timeout waiting for reqsvr to initialize

Cause

During the boot process of each, the Watchd process of the server waits for 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 boots subsequently, it becomes the active server.

If a server hangs during boot process when this alarm occurs, the external symptoms of this alarm resemble those of two other _WD alarms, #13 (Except S8500) and #14 (Except S8500). Therefore, you must carefully discriminate between these three events.

Resolution

1. To determine the cause of this problem:
   a. Check if the Linux OS and the Web interface are running, including the commands: **telnet**, **statapp**, **server**, **logv**, **cat**, **grep**, **tail**, **vi**, etc.
   b. Check if the Watchdog application is *active*, but no other Communication Manager software is running
   c. The **almdisplay** command displays *no* alarms, instead, the command returns the message:

“almdisplay: 4: Unable to connect to MultiVantage”

CAUTION:
The following procedure causes a brief service outage and must executed only at the convenience of the customer.

2. go to the Avaya Support website at http://support.avaya.com to open a service request.
3. Enter **`server`** to check if 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:
   - From the Web interface, select **Shutdown This Server**
   - From the Linux command line, enter **`/sbin/shutdown -r now`**
5. Once the standby server restarts, check if the Event ID #5 was logged:
   - From the Web interface, select **Diagnostics > View System Logs > Watchdog Logs**
   - From the Linux command line, enter **`logv -w`** or by examining `/var/log/ecs/wdlog` log file.
6. If rebooting the server does not help *or* if the problem persists, go to the Avaya Support website at http://support.avaya.com to open a service request.

WD Event ID 6 S8300D

Alarm level

MAJ

Alarm text

`Application <name> (pid) not started, config parm errors`

Cause

Watchdog cannot read its configuration file, **`/etc/opt/ecs/watchd.conf`**.

Resolution

1. To verify the alarm, locate the name of the application process ID (PID):
   - From the Web interface, select **Diagnostics > View System Logs > Watchdog Logs.**
   - From the Linux command line, enter **`logv -w`** or by examining the `/var/log/ecs/wdlog` log file .
2. Retrieve a fresh copy of `watchd.conf` from the distribution.
3. Check if all the files listed in `watchd.conf` exists and are executable.
4. Enter **`start -s application`** to start the application.
5. Manually clear the alarm:

- From the Web interface, select **Alarms and Notification** and the appropriate alarm, and click **Clear**
- From the Linux command line, enter **`almclear -n #id`**

WD Event ID 7 S8300D

Alarm level

MAJ

Alarm text

`Application <name> not started, parm file errors`

Cause

Since an application's specified location in watchd.conf is incorrect, Watchdog cannot start the application.

Resolution

1. To verify the alarm, locate the application name or process ID (PID):
   - From the Web interface, select **Diagnostics > View System Logs > Watchdog Logs**
   - From the Linux command line, enter **`logv -w`** or by examining the `/var/log/ecs/wdlog` log file.
2. Check if the file named in the log exists and is executable.

   To locate the executable file of the application, 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 the file is present:
   a. Enter **`ls -l`** on the symbolic link's address.
   b. Check if the file has execute permissions. If the file does not have execute permissions, enter **`chmod +x`** to enable execution of the application.

   If the file is not present, Linux has returned a "null link."
   - Acquire the executable from the distribution.
4. Check if the string in `watchd.conf` is correct.
5. Enter **`start -s application`** to start the application.
6. Manually clear the alarm:
   - From the Web interface, select **Alarms and Notification** and the appropriate alarm, and click **Clear**
   - From the Linux command line, enter **`almclear -n #id`**

WD Event ID 13 (Except S8500)

Alarm level

MIN

Alarm text

ERROR: could not dup socket fd in reqsvr.c, heartbeat thread not created, errno=<x>

Cause

Booting application initiates

Restarting application re-initiates heartbeating 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 canot create the socket. Meanwhile, if the other server is started, it becomes the active

server.

If the server hangs when this alarm occurs, the external symptoms of this alarm resemble those of two other _WD alarms, #5 and #14 (Except S8500). Therefore, carefully discriminate between these three events.

Resolution

1. To determine the cause of this:
   a. Check if Linux OS and the Web interface are running, including the commands: **telnet**, **statapp**, **server**, **logv**, **cat**, **grep**, **tail**, **vi**, etc.
   b. Check if the Watchdog application and *some* other Communication Manager processes are up:
      — From the Web interface, select **View Process Status**
      — From the Linux command line, enter **statapp**
   c. If the GMM process is active, the **almdisplay -v** command shows the message string of Event #13.

      If the GMM process is not active, check if the Watchdog log shows the message string:
      — From the Web interface, select **Diagnostics > View System Logs > Watchdog Logs**
      — From the Linux command line, enter **logv -w** or directly examine the `/var/log/ecs/wdlog` log file.

   CAUTION:
   The following procedure causes a brief service outage and must executed only at the convenience of the customer.
2. Go to the Avaya Support website at http://support.avaya.com to open a service request.

3. Enter **server** to check if the suspected server is the standby.

   If necessary and at the convenience of the customer, enter **server -if** to force a server interchange.

4. Reboot the standby server:
   - From the Web interface, select **Shutdown This Server**
   - From the Linux command line, enter **/sbin/shutdown -r now**
5. If rebooting the server does not help *or* if the problem persists, go to the Avaya Support website at http://support.avaya.com to open a service request.

WD Event ID 14 (Except S8500)

Alarm level

MIN

Alarm text

ERROR in req2svr.p trying to create heartbeat thread, errno=<x>

Cause

After the “reqsvr” (request server) creates a duplicate socket (see Event ID #13 (Except S8500), it tries to create a heartbeating thread. This alarm indicates that reqsvr cannot create the thread. Meanwhile, if the other server is started, it becomes the active server.

If the server hangs when this alarm occurs, the external symptoms of this alarm resemble those of two other _WD alarms, #5 and #13 (Except S8500). Therefore, carefully discriminate between these three events.

Resolution

1. To determine the cause of this problem:
   a. Check if Linux OS and the Web interface are active including the commands: **telnet**, **statapp**, **server**, **logv**, **cat**, **grep**, **tail**, **vi**, etc.
   b. Check if the Watchdog application is partially active and other Communication Manager processes are active:s
      - From the Web interface, select **View Process Status**
      - From the Linux command line, enter **statapp**
   c. The **almdisplay -v** command shows the message string of Event #14

   CAUTION:
   The following procedure causes a brief service outage and must executed only at the convenience of the customer.
2. Go to the Avaya Support website at http://support.avaya.com to open a service request.

3. Enter **server** to check if the suspected server is the standby.

   If necessary and at the convenience of the customer, enter **server -if** to force a server interchange.

4. Reboot the standby server:
   - From the Web interface, select **Shutdown This Server**
5. If rebooting the server does not help *or* if the problem persists, go to the Avaya Support website at http://support.avaya.com to open a service request.

WD Event ID 15 S8300D

Alarm level

MAJ

Alarm text

Detected a rolling reboot

Cause

Watchdog has detected “x” number of Linux reboots within “y” minutes. The x and y parameters configurable in /etc/opt/ecs/watchd.conf. Rolling reboots have a many possible causes.

Resolution

1. To verify the alarm, locate the message, “WARNING: Rolling reboot detected!!“:
   - From the Web interface, select **Diagnostics > View System Logs > Watchdog Logs.**
   - From the Linux command line, enter **logv -w** or directly examine the `/var/log/ecs/wdlog` log file.
2. Go to the Avaya Support website at http://support.avaya.com to open a service request.
3. Giving priority to Communication Manager errors, examine the Watchdog log from Step 1, and determine which application failed.
4. Check if all the files listed in `watchd.conf` exists and are executable. Rolling reboots are often caused by executables in unexpected locations.
5. If the files and their locations are valid, examine the trace log to determine the cause:
   - From the Web interface:
     a. Select the **View System Logs** diagnostic and **Logmanager Debug** trace
     b. Specify the **Event Range** for the appropriate time frame
     c. Match the “rolling reboot” pattern
   - From the Linux command line, enter **logv -t ts.**

WD Event ID 18 S8300D

Alarm level

WRN

Alarm text

`Application <name> restarted. Retry <retry count>, New Pid: <pid>`

Cause

An application has failed, and Watchdog successfully restarted it.

Resolution

1. To verify the alarm, locate the application name or process ID (PID):
   - From the Web interface, by select **Diagnostics > View System Logs > Watchdog Logs.**
   - From the Linux command line, enter **`logv -w`** or directly examine the `/var/log/ecs/wdlog`.
2. No corrective action necessary. Manually clear the alarm:
   - From the Web interface, select **Alarms and Notification** and the appropriate alarm, and click **Clear.**
   - From the Linux command line, enter **`almclear -n #id.`**

WD Event ID 19 S8300D

Alarm level

MIN

Alarm text

`Application failed unintentionally`

Cause

Watchdog is shutting down the system down because an application failed to start correctly. The application failed to start because of the following:

The file did not exist, similar to Event ID #7.

Required application parameters were missing or invalid in **`watchd.conf`**.

Resolution

1. To verify the alarm, locate the message, “Application num <#> (<application path>) not started. Watchdog exiting NOW”:
   - From the Web interface, select **Diagnostics > View System Logs > Watchdog .**

- From the Linux command line, enter **logv -w** or directly examine the /var/log/ecs/wdlog log file.

2. Check if the file named in the log exists and is executable.
3. Check if 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:
   - From the Web interface:
     a. Select the **View System Logs** diagnostic and **Logmanager Debug** trace
     b. Specify the **Event Range** for the appropriate time frame
     c. Match the application number as the pattern
   - From the Linux command line, enter **logv -t ts**
5. Once resolved, manually clear the alarm:
   - From the Web interface, select **Alarms and Notification** and the appropriate alarm, and click **Clear**
   - From the Linux command line, enter **almclear -n *#id***

WD Event ID 20 S8300D

Alarm level

MAJ

Alarm text

Application <name> (pid) TOTALLY FAILED

Cause

Application failed the maximum allowed number of times. This alarm usually occurs with Event ID #4.

Resolution

1. To verify the alarm, locate the application name or process ID (PID):
   - From the Web interface, select **Diagnostics > View System Logs > Watchdog Logs.**
   - From the Linux command line, enter **logv -w** or directly examine the /var/log/ecs/wdlog log file.
   - Check if the application is running:
     - From the Web interface, select **View Process Status.**
     - From the Linux command line, enter **statapp.**
2. If the application is not running down, enter **start -s *application*** to start the application.

3. If the application starts, continue with Step 7.

   If the application does not start, check the trace log to determine why the application failed to start:

   — From the Web interface:

      a. Select the **View System Logs** diagnostic and **Logmanager Debug** trace

      b. Specify the **Event Range** for the appropriate time frame

      c. Match the application's PID as the pattern

   — From the Linux command line, enter `logv -t ts`

4. To locate the executable file of the application, enter the command:

   `ls -l /opt/ecs/sbin/appl`

   If the executable is present, Linux returns a symbolic link to its location.

5. If the file is present:

   a. Enter `ls -l` on the symbolic link's address.

   b. Verify that the file has execute permissions. If not, enter `chmod +x` to enable execution of the application.

   If the file is not present, Linux has returned a "null link":

   — Acquire the executable from the CD

6. Enter `start -s application` to start the application.

7. Manually clear the alarm:

   — From the Web interface, select **Alarms and Notification** *and* the appropriate alarm, and click **Clear.**

   — From the Linux command line, enter `almclear -n #id.`

8. If the problem persists, go to the Avaya Support website at http://support.avaya.com to open a service request.

WD Event ID 22 S8300D

Alarm level

MIN

Alarm text

`Application <name> (<pid>) terminated`

Cause

Watchdog successfully shut down the named application, and if necessary, watchdog will restart the application.

Resolution

1. To verify the alarm, locate the application name or process ID (PID):
   - From the Web interface, select **Diagnostics > View System Logs > Watchdog Logs.**
   - From the Linux command line, enter `logv -w`.
2. On the standby server, look for occurrences of the `stop` command:
   - From the Web interface:
     a. Select **View System Logs**
     b. Select **Platform command history log**
     c. Specify the **Event Range** for the appropriate time frame
     d. Match the “Stop” pattern
   - From the Linux command line, enter `listhistory.`
3. If a `stop` command was inappropriately 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 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, Watchdog responded to abnormal internal processes by shutting down the application.

   Check the trace log for information about this application:
   - From the Web interface:
     a. Select the **View System Logs** diagnostic and **Logmanager Debug** trace
     b. Specify the **Event Range** for the appropriate time frame
     c. Match the application PID as the pattern
   - From the Linux command line, enter `logv -t ts`
5. Manually clear the alarm:
   - From the Web interface, select **Alarms and Notification** and the appropriate alarm, and click **Clear.**
   - From the Linux command line, enter `almclear -n #id.`
6. Check if the alarm persists. If the alarm persists, go to the Avaya Support website at http://support.avaya.com to open a service request.

WD Event ID 23 S8300D

Alarm level

MAJ

Alarm text

`Watchd high-monitor thread is rebooting the system`

Cause

The Lo-monitor thread is missing heartbeats (cannot get CPU time). The Hi-monitor thread has tried 3 times to recover the system by killing any infinitely looping processes. If the lo-monitor thread does not heartbeat even after three CPU-occupancy profiles and recoveries, the Watchd reboots the server.

Resolution

1. To verify the alarm, look for messages containing the CPU profiling results and attempted recoveries and messages stating that Watchd is rebooting the server:
   - From the Web interface, select **Diagnostics > View System Logs > Watchdog Logs.**
   - From the Linux command line, enter **`logv -w`** or directly examine the `/var/log/ecs/wdlog` log file.

   No corrective action is necessary. The server restarts by the time a technician analyzes the system. A reboot clears the alarm and fixes problems with unresponsive software.
2. Check if the alarm persists. If the alarm persists, go to the Avaya Support website at http://support.avaya.com to open a service request.

WD Event ID 24 S8300D

Alarm level

MAJ

Alarm text

`Watchd's high-monitor thread is stopping tickling of hw`

Cause

Event ID #23's call to reboot the server was unsuccessfully invoked. A semaphore of the Linux kernel is stuck. Once this alarm is raised, Watchd stops the HW sanity timer prompting HW sanity watchdog to execute a hard reboot of the processor.

Resolution

1. To check if the alarm occurred, look for messages that indicate stopping stopping the tickling of the HW sanity timer and CPU occupancy profiling:
   - From the Web interface, select **Diagnostics > View System Logs > Watchdog Logs.**

- From the Linux command line, enter **logv -w** or directly examine the /var/log/ecs/wdlog log file.
  - If the HW sanity watchdog successfully executes a hard reboot, the alarm clears. This reboot fixes problems caused by unresponsive software.

    If the HW sanity watchdog fails to execute a hard reboot, disengage and reengage the power source of the server to release it from this condition and to clear the alarm.

2. Check if the alarm persists. If the alarm persists, go to the Avaya Support website at http://support.avaya.com to open a service request.

WD Event ID 26

Alarm level

MIN

Alarm text

Watchd handshake error

Cause

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.

Resolving WD Event # 26

1. Refer to the SAMP User Guide for troubleshooting procedures (03-300322).
2. Go to the Avaya Support website at http://support.avaya.com to open a service request.

WD Event ID 27

Alarm level

MAJ

Alarm text

Free memory on the system is low

Resolution

1. To check if the alarm occurred, look for messages that indicate stopping the tickling of the HW sanity timer and messages that indicate CPU occupancy profiling:
   - From the Web interface, select **Diagnostics > View System Logs > Watchdog Logs.**
   - From the Linux command line, enter **`logv -w`** or directly examine the `/var/log/ecs/wdlog` log file.

Appendix A: PCN and PSN

A product-change notice (PCN) is issued in case of any software update. For example, a PCN must accompany a service pack or a patch that needs to be applied universally. A product-support notice (PSN) is issued when there is no patch, service pack, or release fix, but the business unit or services need to alert Avaya Direct, Business Partners, and customers of a problem or a change in a product. A PSN can also be used to provide a workaround for a known problem, steps to recover logs, or steps to recover software. Both these notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

About this task

To view PCNs and PSNs, perform the following steps.

Procedure

1. Go to the Avaya Support website: http://support.avaya.com

   Note:
   If the Avaya Support website displays the login page, enter your SSO login credentials.

2. On the top of the page, select **DOCUMENTS**.
3. On the Documents page, in the **Enter Your Product Here** field, enter the name of the product.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. Select **Documents** as the content type.
6. Select the appropriate filters as per your search requirement. For example, if you select Product Support Notices, the system displays only PSNs in the documents list.

   Note:
   You can apply multiple filters to search for the required documents.

Signing up for notifications alerts

Manually viewing PCNs and PSNs is helpful, but you can also sign up for receiving notifications of new PCNs and PSNs. Signing up for notifications alerts you to specific issues you must be aware of. These notifications also alert you when new product documentation, new product patches, or new services packs are available. This proactive notification system is performed by the Avaya E-Notifications process.

To sign up for notifications:

1. Go to the Avaya Support Web Tips and Troubleshooting: eNotifications Management page at https://support.avaya.com/ext/index?page=content&id=PRCS100274#,
2. Set up e-notifications as per the steps indicated in the the **How to set up your E-Notifications** procedure.