Maintaining and Troubleshooting Avaya Aura® Conferencing

Release 8.0.6
April 2016

Notice

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

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of 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 or on the express behalf of 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 Avaya hardware and software. 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: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; 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. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “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. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance 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, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of 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.

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 is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage

Nortel Products" or such successor site as designated by Avaya. 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 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, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, 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

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products 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 products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, 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, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Java is a registered trademark of Oracle and/or its affiliates.

Contents

Chapter 1: An Introduction to Avaya Aura® Conferencing

About this document

This document describes how to manage your deployment of Avaya Aura® Conferencing on an ongoing basis. It describes how to perform routine maintenance tasks and it also addresses the most commonly observed usage issues that may arise.

Related resources

Documentation

The following table lists the related documents for Avaya Aura® Conferencing. Download the documents from the Avaya Support website at http://support.avaya.com.

The Avaya Support website also includes the latest information about product compatibility, ports, and Avaya Aura® Conferencing releases.

Related links

Overview on page 11
Implementation on page 12
Administration on page 13
Reference on page 13

Overview

Document number	Title	Use this document to:	Audience
04-604343	*Avaya Aura® Conferencing Overview and Specification for Avaya Aura®*	Understand the high-level features and functionality of the product.	Customers, business partners, and

Table continues…

Document number	Title	Use this document to:	Audience
			services and support personnel
04-604344	*Avaya Aura® Conferencing Overview and Specification for Turnkey*	Understand the high-level features and functionality of the product.	Customers, business partners, and services and support personnel
04-604323	*Avaya Aura® Conferencing Solution Description for Small and Medium Enterprises*	Understand the high-level features and functionality of the solution.	Customers, business partners, and services and support personnel
04-604328	*Avaya Aura® Conferencing Solution Description for Medium Enterprises*	Understand the high-level features and functionality of the solution.	Customers, business partners, and services and support personnel
04-604333	*Avaya Aura® Conferencing Solution Description for Large Enterprises*	Understand the high-level features and functionality of the solution.	Customers, business partners, and services and support personnel

Related links

Documentation on page 11

Implementation

Document number	Title	Use this document to:	Audience
04-604418	*Deploying Avaya Aura® Conferencing: Basic Installation*	Perform installation and configuration tasks.	Partners, Services, and Support personnel
04-604363	*Deploying Avaya Aura® Conferencing: Advanced Installation and Configuration*	Perform installation and configuration tasks.	Partners, Services, and Support personnel
04-604353	*Upgrading Avaya Aura® Conferencing*	Perform upgrading and configuration tasks.	Partners, Services, and Support personnel

Table continues…

Document number	Title	Use this document to:	Audience
04-604403	*Migrating Avaya Aura® Conferencing*	Perform migration and configuration tasks.	Partners, Services, and Support personnel

Related links

Documentation on page 11

Administration

Document number	Title	Use this document to:	Audience
04-604378	*Administering Avaya Aura® Conferencing*	Perform system-wide administration tasks.	System administrators
04-604403	*Migrating Avaya Aura® Conferencing*	Perform system-wide security administration and backup/restore tasks.	System administrators
04-604398	*Maintaining and Troubleshooting Avaya Aura® Conferencing*	Perform maintenance and troubleshooting tasks. Understand logs and fault tracking.	System administrators Partners, Services, and Support personnel
—	*Avaya Aura® Conferencing Security*	Perform system-wide security-related administration tasks.	System administrators

Related links

Documentation on page 11

Reference

Document number	Title	Use this document to:	Audience
04–604423	*Avaya Aura® Conferencing Accounting Records Reference*	Collect information about accounting records	System administrators Customers, Partners, Services, and Support personnel

Table continues…

Document number	Title	Use this document to:	Audience
04-604443	*Avaya Aura® Conferencing Alarms and Logs Reference*	Collect information about alarms and logs, including the alarms and logs families	System administrators Customers, Partners, Services, and Support personnel
04-604444	*Avaya Aura® Conferencing Operational Measurements Reference*	Collect information about operational measurements	System administrators Customers, Partners, Services, and Support personnel

Related links

Documentation on page 11

Training

The following courses are available at http://www.avaya-learning.com. In the **Search** field, type the course code, and click **Go** to search for the course.

Course code	Course title
2U00110O	Selling Avaya Aura® Conferencing Solution Learning Bytes
2U00325O	Avaya Aura® Conferencing 7 L1 Customer Scenario
3U00260W	Designing Avaya Aura® Conferencing
5U00120E	Avaya Aura® Conferencing
3204	Avaya Aura® Conferencing Implementation and Maintenance Exam

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 and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to 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 website.

Note:

Videos are not available for all products.

Deploying online help

Avaya Aura® Conferencing contains a number of online help files and online manuals to guide you through the process of installing, configuring, and maintaining your conferencing system. These online help files include:

- Online help for Element Manager
- Online help for the Provisioning Client
- Online help for Reports
- Online help for users of Collaboration Agent

By default, each of these online help packages is fully integrated with the component which it describes. So, for example, if you view help on Element Manager, you can access the Element Manager online help. The Element Manager online help file describes each of the Element Manager fields and describes many of the common procedures that you can perform using the Element Manager interface.

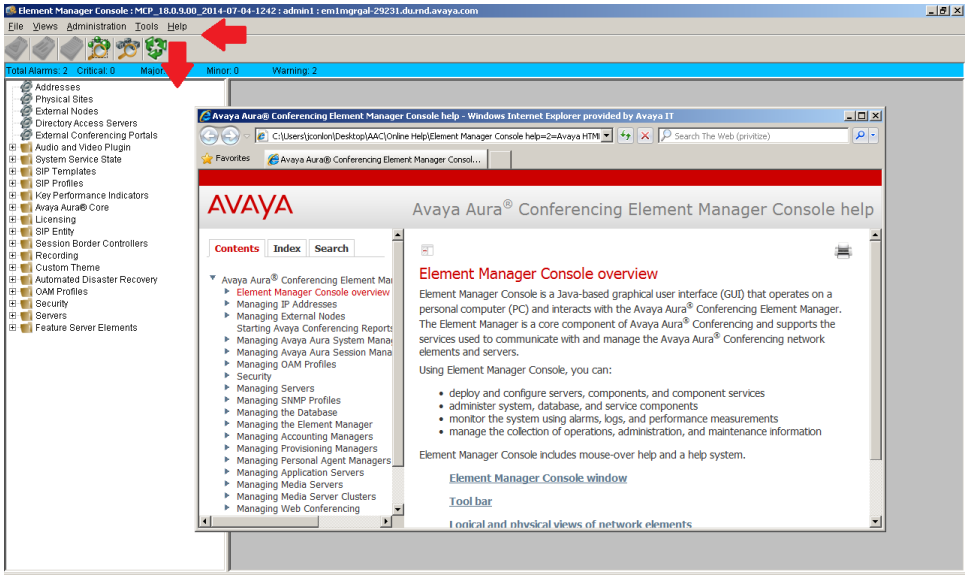


Figure 1: Online Help for Element Manager

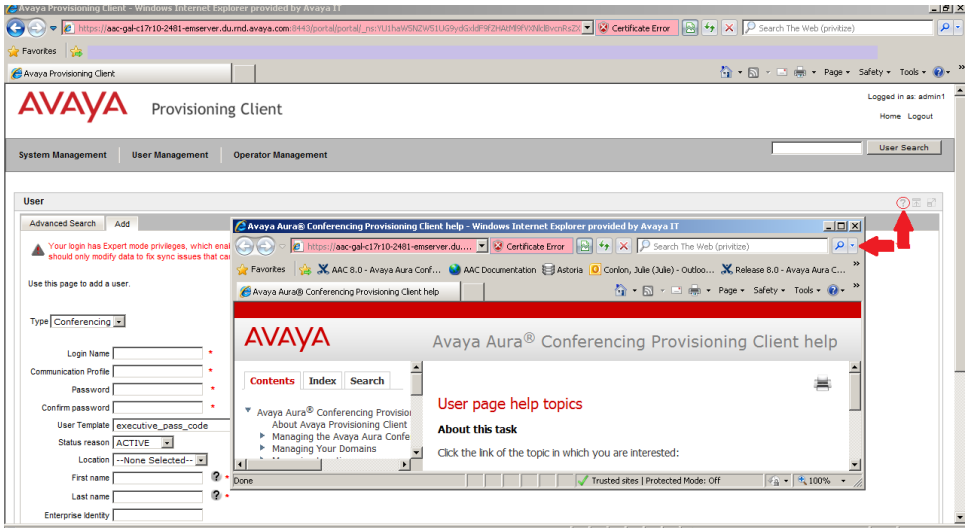


Figure 2: Online Help for the Provisioning Client

In the case of the online help for users of Collaboration Agent, Avaya has translated the online help into several languages. The list of available languages conforms with the i18n and L10n (internationalization and localization standards). When users install the Collaboration Agent application, it chooses which language to display based on the computer's locale.

The online help files are packaged within the Avaya Aura® Conferencing software application bundle.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Audience

The intended audience for this document is:

- Tier 1 Avaya technical support
- Avaya Professional Services
- Authorized Business Partners

You must have the following core competencies:

- The ability to access servers using:
  - a locally attached keyboard and monitor or KVM (Keyboard, Video, Mouse) switch
  - the ssh remote access protocol
- Basic Linux operations:
  - navigating the file system (changing directories)
  - managing the implications of uninformed or careless use of system commands while logged in as the root user
- Basic server tasks:
  - powering servers up
  - powering servers down
  - resetting servers
  - inserting and removing CD-ROM and DVD-ROM disks
- Basic Microsoft knowledge:

  Windows:
  - editing text files
  - creating folders
  - Microsoft Excel:
    - transitioning between worksheets of a workbook
    - entering data into cells

    - copying/pasting between cells and commands, such as Control+c, Control+v, and Edit > Paste Special menu
- The ability to operate a supported Web browser (such as Firefox or Internet Explorer):
  - Interacting with pop-up windows
  - Inspecting and accepting x.509 certificates and installing CA certificates that are presented by the browser
  - Downloading and installing software through the browser
- Basic Public Key Infrastructure (PKI) tasks:
  - Creating Certificate Signing Requests (CSR)
  - Inspecting the details of a certificate
  - Installing Certificate Authority certificates on Windows Certificate Store
  - Installing Personal certificates on Windows Certificate Store
  - Installing Certificate Authority certificates on Firefox Certificate Manager
  - Installing Your Certificates on Firefox Certificate Manager

How to use this document

You must complete a given task successfully before beginning the next one. If you encounter issues while performing a step, contact the Avaya Support Web site at http://support.avaya.com to open a service request.

Use the Avaya Aura® Conferencing Intelligent Workbook together with this document to guide you through the preparatory requirements and installation and configuration steps for Avaya Aura® Conferencing. The Intelligent Workbook can be found on the Avaya Web site at http://support.avaya.com/.

Related links

Preparing your data using the Avaya Aura Conferencing Intelligent Workbook on page 18

Preparing your data using the Avaya Aura® Conferencing Intelligent Workbook

The Avaya Aura® Conferencing Intelligent Workbook is a data collection tool. It is in the Microsoft Excel format. The important tabs are **Checklist**, **Design**, and **Configuration Data** tabs. The other steps and tabs of the workbook are dynamic and depend on the layout selected in the **Design** tab, so they might not be listed as they are listed below. This is an example of typical tabs that might be visible:

- Instructions

- 0-Configuration Data
- 1-OS Linux Install
- 2-OS Patches Install
- 3-ACC Apps Install
- 4-Licensing
- 5-Single sign-on
- 6-Config AAC Services
- 7-Config Avaya Aura
- 8-Provisioning
- 9-Web Conferencing: Enabling Web conferencing
- 10-Video
- A-Flare for Windows and iPad
- B-Update AAC
- C-Apply patches
- FAQ
- Troubleshooting
- Values

Related links

How to use this document on page 18

Administrative user roles and preconfigured accounts

Roles define operational boundaries (access permissions) for administrators. Administrators can have more than one role, depending on their duties. You assign roles to new administrators when you create their accounts. During server installation, the installation software creates the following user accounts:

Preconfigured/ Admin accounts	Default password	Preassigned role	Description
ntsysadm	password	System Security Administrator (SSA) role.	The SSA can perform system configuration and specify security attributes such as: • Password configuration • User management • Certificate management

Table continues…

Preconfigured/ Admin accounts	Default password	Preassigned role	Description
			• Access control • Antivirus • File System Integrity tools • Network configuration • System backup and restore
ntappadm	password	Application Administrator (AA) role	The AA can install the Avaya Aura® Conferencing application software and manage components related to the application. The AA is responsible for installing, maintaining, patching, and upgrading Avaya Aura® Conferencing software only.
ntsecadm	password	Security Auditor (SA) role	The SA can collect and view security audit logs and syslogs at the platform level. The SA can also transfer the security logs off the server.
ntbackup	password	Backup Administrator (BA) role	The BA can perform only system backups. A BA cannot perform: • any operation on the server except backups. • a system restore—only the SSA or root user can perform a system restore.
ntdbadm	password	Database Administrator (DBA) role	The DBA can manage the database schemas and database tools on servers where the database resides. The server must host the database for this role to be relevant.
ntossadm	password	Operational Support System Administrator (OSS) role	Downstream processors can use the ntossadm account with this role to connect to the server and collect OSS logs.
admin admin1 admin2 admin3 admin4 admin5	admin admin1 admin2 admin3 admin4 admin5	Unlimited privileges	For expert mode login to Avaya Aura® Conferencing, Element Manager, and Provisioning Manager.

Table continues…

Preconfigured/ Admin accounts	Default password	Preassigned role	Description
init	Not applicable	System Security Administrator (SSA) role and Database Administrator (DBA) role	SSA and DBA account for Avaya Services access.
craft	Not applicable	Application Administrator (AA) role	AA account for Avaya Services access

Supported Web browsers

Avaya Aura® Conferencing supports the following browsers for Collaboration Agent users and Avaya Aura® Conferencing administrators. Administrators use the following applications to administer and maintain Avaya Aura® Conferencing:

- Element Manager Console
- Provisioning Client
- Avaya Conferencing Reports & Monitors

These administration applications run on the Windows operating system and are not compatible with the Apple OS X operating system.

Web browser	Operating system
Microsoft Internet Explorer 8 and later	Windows 7 and 8
Microsoft Edge	Windows 10
Mozilla Firefox version 10 and later	Windows 7 and 8 Apple OS X
Google Chrome latest version	Windows 7 and 8 Apple OS X
Apple Safari latest version	Apple OS X

Enable pop-ups in your web browser for Collaboration Agent to function properly.

Possible limitations in relation to the Audio/Video in Collaboration Agent feature

When running the Audio/Video in Collaboration Agent feature, Google Chrome may demonstrate poor lip synchronization. When Collaboration Agent detects when a user wishes to use the Audio/Video in Collaboration Agent feature in Google Chrome, it displays an information message to inform them of this possible limitation.

In addition, users running Google Chrome for the Mac operating system may experience issues when sharing their desktop. Avaya recommends using Apple Safari or Mozilla Firefox for desktop sharing instead.

Related links

Avaya Web Collaboration audio and video plug-in on page 22

Avaya Web Collaboration audio and video plug-in

In this release of Avaya Aura® Conferencing, there is a new Web-based audio and video client. This client is a browser plug-in which executes within the Web Collaboration Agent client. It enables users to receive their audio and video through the Web. This functionality means that users do not have to dial into the conference using a phone connection. The client is available for all deployment types and can operate seamlessly with other supported clients. Avaya are delivering this feature as a browser plug-in. In previous releases, Avaya delivered a similar but inferior feature using a Flash-based client. The newly enhanced browser plug-in offers an improved audio and video experience and a more intuitive user interface. The older client is still available as part of the software bundle and existing installations can still continue to use the older client. However, Avaya recommends upgrading to the new client for a superior user experience.

For Avaya Aura® Conferencing turnkey deployments, it is likely that most users will receive their audio and video using the new client.

You can control access to the plug-in at a system level. Using this system parameter, you can enable or disable access for all users in your deployment. In addition to this system-wide setting, you can also control access to the Avaya Web Collaboration audio and video plug-in at a user level, by configuring a class of service. For example, you may want to offer the plug-in to some users but not to others. If you enable access to the Avaya Web Collaboration audio and video plug-in, you can choose to inform users of its availability immediately after they join the conference or you can choose not to inform them. If you choose to inform them, Avaya Aura® Conferencing displays a menu and if you choose not inform them, Avaya Aura® Conferencing hides this menu.

If you wish to offer this form of integrated audio and video to external users who reside outside of the enterprise, you must install and configure a Session Border Controller (SBC).

Related links

Supported Web browsers on page 21
Web browsers and operating systems that the audio and video conferencing plug-in supports on page 22

Web browsers and operating systems that the audio and video conferencing plug-in supports

Web browsers

Web browsers supported	Web browsers not supported
• Mozilla Firefox version 10 and later • Microsoft Internet Explorer 8 and later • Apple Safari latest version for Apple OS X	• Microsoft Internet Explorer for Microsoft Metro • Microsoft Edge • Google Chrome • Opera

Web browsers supported	Web browsers not supported
	• Any 64–bit version of browsers • All other mobile browsers

Operating systems

Operating systems supported	Operating systems not supported
• Windows 7, 32–bit and 64–bit • Windows 8, 32–bit and 64–bit • Windows 10, 32–bit and 64–bit • Apple OS X 10.7 and later	• Older versions of Windows, such as Windows XP • Android • iOS • Google Chrome • Linux • Windows Mobile

Limitations of the audio and video conferencing plug-in

- Avaya Aura® Conferencing does not support the audio and video conferencing and web collaboration plug-ins for Google Chrome and Microsoft Edge. You can only view the shared content in these web browsers. Use another web browser for audio and video conferencing and sharing content in Collaboration Agent.
- The audio and video conferencing plug-in supports only the 32–bit version of web browsers.
- The enterprise network must have a session border controller deployed to support participants who log in to an integrated audio and video conference from outside the network.

Related links

Avaya Web Collaboration audio and video plug-in on page 22

Supported hardware

In this release, Avaya Aura® Conferencing supports the HP ProLiant DL360 G9 for all deployment configurations. Alternatively, if you have an existing HP ProLiant DL360p G8 or HP ProLiant DL360 G7, you can reuse it. If you have existing Dell 610 or IBM S8800 servers, you may be able to reuse them as cascading Avaya Aura® Media Server (MS)'s. However, you cannot reuse the Dell 610 or IBM S8800 servers as Avaya Aura® Conferencing core servers.

The hardware requirements for Avaya Aura® Conferencing are the same whether you are installing the product in an Avaya Aura® deployment or a Turnkey deployment. In both cases, it is the HP ProLiant DL360 G9 server.

Server type	Supported use
HP ProLiant DL360 G9	Used for new installations of Avaya Aura® Conferencing.

Table continues…

Server type	Supported use
HP ProLiant DL360p G8 or HP ProLiant DL360 G7	Can be reused when upgrading existing Avaya Aura® Conferencing 7.2 deployments to the new release. **Note:** For Large deployments (previously known as Standalone in previous Avaya Aura® Conferencing releases) the server hosting the Element Manager and Database must have more than 12GB of RAM. If your server only has 12GB of RAM, please contact Avaya for a memory expansion kit and apply this kit prior to the upgrade to the new release. For more information on installing and configuring the memory expansion kit, see *Deploying Avaya Aura® Conferencing 7.2.2*, which is available from https://support.avaya.com/.
Dell 610	Can only be used as cascading media servers.
IBM S8800	Can only be used as cascading media servers.

Chapter 2: Guidelines for administrators

This document provides the tasks required to maintain, troubleshoot, and manage faults for an Avaya Aura® Conferencing system.

Prerequisites

- Ensure the installation is complete.
- Be familiar with the Element Manager Console.
- Be familiar with RedHat Linux Enterprise edition.
- Be familiar with HP ProLiant DL360 G9.

Administrator responsibilities

As the administrator for Avaya Aura® Conferencing, you are responsible for:

- Managing Avaya Aura® Conferencing users. For example, administrators can control access to features such as the ability to record, the ability to dial out, the ability to use video, the ability to use Presentation Mode, the ability to use Fast Start, and so on.
- Managing software loads and patches
- Managing Avaya Aura® Conferencing network elements, such as, media servers, media server clusters, and web conferencing resources
- Monitoring system alarms and logs
- Monitoring system performance
- Backing up the Avaya Aura® Conferencing system periodically
- Restoring the Avaya Aura® Conferencing system in the event of data loss
- Managing system security

Toll fraud

It is important to note that there is a risk of toll fraud on all telephony systems. It is difficult to eliminate the risk entirely but it is possible to optimize Avaya Aura® Conferencing security features to minimize the risk.

A popular feature on Avaya Aura® Conferencing enables conference moderators to dial out from the conference to other telephone numbers. This feature is useful, for example, to contact an individual who is not currently in the conference and to bring them into the conference. To dial out, moderators can use the **Add Participants** menu option on the Collaboration Agent interface or they can hit ***1** to

dial out to an external line and when the call is answered, they can hit ***1** to return themselves and the called party to the conference.

If this feature is enabled, it is important to ensure that moderators are aware that they must keep their moderator codes private and not allow them to be widely distributed. If a moderator code falls into the hands of an individual with malicious intent, they may be able to commit toll fraud by dialling out to international or premium telephone lines.

To minimize the risk of toll fraud, you can disable the dial out feature entirely or disable it for certain users, using the conference class of service menu in the Provisioning Client. After you have created a conference class of service template with dial out disabled, you can assign users to it. Additionally, you can configure other features, such as mandatory passcode entry for conferences using the conference class of service template.

If you wish to offer Avaya Aura® Conferencing to smartphone users, who are outside of the enterprise firewall and if the Avaya Aura® Media Server (MS) resides within the enterprise firewall, you must configure a Session Border Controller (SBC). You also require an SBC if you wish to offer integrated audio and video to external users who reside outside of the enterprise. To reduce your exposure to the threat of toll fraud, you can configure a restrictive end point policy for the subscriber flow on the SBC. For an even higher level of security, you can confine access to enterprise users by not configuring an SBC. As a general rule, you should always configure the TLS method of secure transmission, rather than the regular TCP method.

The Conferencing Reports & Monitors application enables you to monitor usage patterns in your system. You can use Key Performance Indicators (KPIs) to provide insight into what is currently occurring on the system now or what has occurred on the system at some point in the past. You can set alert thresholds to inform you of excessive bandwidth usage or irregular call patterns. These investigative tools provide a valuable source of information.

Outside of Avaya Aura® Conferencing, you can configure the security of your telephony gateway to prevent international dial out or to restrict dial out to premium telephone numbers. It is your responsibility to ensure that your system is secure.

Fault management fundamentals

This section describes the fundamentals for identifying faults in your Avaya Aura® Conferencing system, how to perform general operational measurements, and general strategies for managing faults.

Methods for identifying a fault

Avaya Aura® Conferencing provides logs, alarms, and hardware and software faults that can be used to help identify problems with the system.

Event logs

The system uses logs to record information related to an event so the information can be analyzed at a later time. Every log event is captured and archived to disk by the Fault Performance Manager assigned to the network element or server. At the same time, the log stream is available to the

Element Manager for display at the Element Manager Console. Use the Element Manager Console log browser to view events.

Event logs should be reviewed periodically so you can identify any potential problems.

Alarms

The system can generate an alarm, notifying you of a problem. Once activated, the alarm remains on a list of active alarms until the alarm has been resolved. Use the Element Manager Console alarm browser to view alarms.

Hardware faults

The hardware associated with Avaya Aura® Conferencing uses a combination of alarms, light emitting devices (LED), and Light Path Diagnostics to help you identify and correct hardware faults.

Software faults

Software faults are usually related to network element instance failures, configuration errors, patching errors, post-installation problems or other problems identified by the Element Manager Console.

Operational measurements

Operational measurements (OMs) provide statistical information about the server and network element operations and performances. OMs are represented by groups, which contain registers (counters and gauges) that provide performance-related data.

Strategies

Avaya Aura® Conferencing provides several features to help manage faults and serious problems that may affect your system.

Denial of service

Denial of service (DoS) attacks cause high levels of SIP messaging or HTTP messaging, which can degrade system performance. The SIP DoS mitigation and HTTP DoS mitigation features protect the call server from DoS attacks.

Administrators can enable the SIP or/and HTTP DoS mitigation feature on each Network Element Instance (NEI). The SIP DoS mitigation feature and HTTP DoS mitigation feature applies to Avaya Aura® Conferencing Provisioning Client and Avaya Aura® Conferencing Personal Agent.

Patching

Problems upgrading the software can occur either during the command line patch, or during upgrades of the database schema, Element Manager, network elements, or any other components upgraded through the Element Manager Console. If an error occurs during an upgrade or patch, the system attempts to rollback to the previous maintenance release or patch load.

Manual failover

Element Manager supports Hot Standby. If the active Element Manager process fails or if there is a network isolation, the secondary Element Manager takes over activity. You can perform a manual failover to restore the active Element Manager.

Disaster recovery

Disaster recovery includes cases of unscheduled power outages and drive replacements.

Chapter 3: Management Tools

To maintain and troubleshoot Avaya Aura® Conferencing, you will use the following applications:

- Element Manager Console
- Conferencing Reports & Monitors

Related links

Element Manager Console overview on page 29
Conferencing Reports & Monitors Overview on page 37

Element Manager Console overview

Element Manager Console is a Java-based graphical user interface (GUI) that operates on a personal computer (PC) and interacts with the Avaya Aura® Conferencing Element Manager. The Element Manager is a core component of Avaya Aura® Conferencing and supports the services used to communicate with and manage the Avaya Aura® Conferencing network elements and servers.

Using Element Manager Console, you can:

- deploy and configure servers, components, and component services
- administer system, database, and service components
- monitor the system using alarms, logs, and performance measurements
- manage the collection of operations, administration, and maintenance information

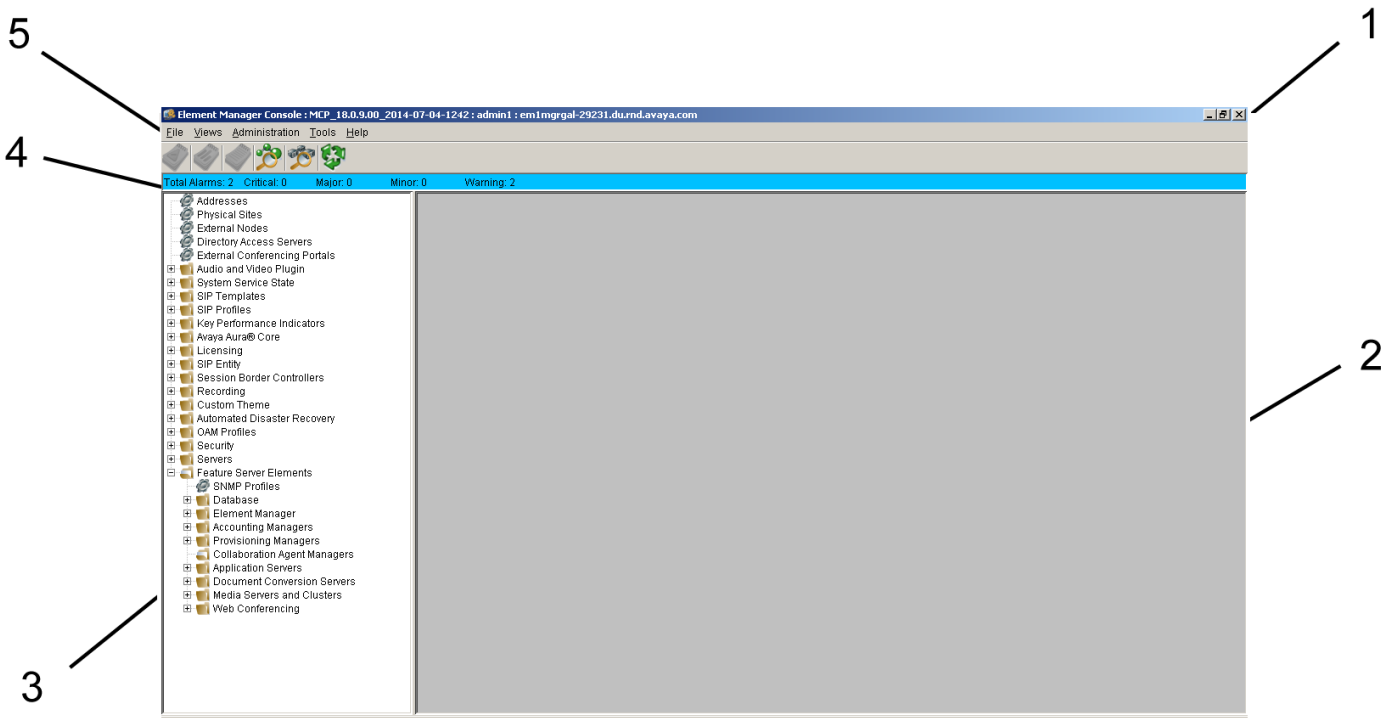
Element Manager Console includes mouse-over help and a help system.

Related links

Management Tools on page 29
Element Manager Console window on page 30
Tool bar on page 31
Logical and physical views of network elements on page 32
Recommended PC hardware and software requirements for running Element Manager Console on page 33
Logging on to Element Manager Console on page 34
Logging off from Element Manager Console on page 37

Element Manager Console window

The following figure shows a sample Element Manager Console window.



No.	Name	Description
1	Title bar	Displays the following information: • name of the application • software version • user ID of the person logged in • IP address/name of the Avaya Aura® Conferencing Element Manager .
2	Work area	Displays the window or dialog box for the node selected in the navigation pane (3).
3	Navigation pane	Displays the nodes for the Avaya Aura® Conferencing Element Manager components.
4	Alarm Summary bar	Provides a concise, system-wide summary of alarms for managed and monitored network elements. The background color of the alarm

Table continues…

No.	Name	Description
		bar indicates the most severe alarm for the system. The alarm color codes are: • Blue - warning • Green - no alarms • Yellow - minor • Orange - major • Red - critical The total number of alarms for the system, as well as the number of alarms of reach severity level appears on the alarm summary bar. The summary bar also includes a section called ACK Critical, which shows the number of previously acknowledged, but not yet cleared alarms.
5	Tool bar	Provides button shortcuts for commonly used menu commands.

Related links

Element Manager Console overview on page 29

Tool bar

The icons on the tool bar are button shortcuts. Not all tool bar options are available for every component or server. Icons that appear disabled are unavailable for the element selected in the navigation pane.

The following figure shows the tool bar.

Button	Name
	Alarm Browser. This button displays the Alarm Browser window, which displays information about current alarms on the selected network element. The Alarm Browser button is disabled until you select a network element.
	OM Browser. This button displays the OM Browser window, which displays OM details about the selected network element. The OM Browser button is disabled until you select a network element.
	Log Browser. This button displays the Logs window, which displays the logs for the selected network element. The Log Browser button is disabled until you select a network element.
	Logical View button. This button opens the Logical View window. For more information, see Logical View window on page 32.

Table continues…

Button	Name
	Physical View button. This button opens the Physical View window. For more information, see Physical View window on page 32.
	Refresh button. This button refreshes the current view.

Related links

Element Manager Console overview on page 29

Logical and physical views of network elements

Element Manager Console provides two graphical views to help you to quickly identify and diagnose alarm and fault conditions for all Avaya Aura® Conferencing network elements:

- the Logical View window, which organizes and displays network elements by element type.
- the Physical View window, which organizes and displays network elements by server.

You open these windows from the tool bar or the Views menu.

Related links

Element Manager Console overview on page 29

Logical View window on page 32

Physical View window on page 32

Logical View window

The Logical View window provides a graphical view of network elements, servers, and logical databases. The network element instances are organized by type. In this view, you cannot determine which network elements are deployed on which servers.

Use this view to see the alarm conditions for all equipment for each network element type. The Alarm Browser button, Log Browser button, and OM Browser button are disabled until you select an network element instance, server, or Avaya media server.

Related links

Logical and physical views of network elements on page 32

Physical View window

The Physical View window provides a graphical view of the system. The network elements are organized by server. Under each server, the network element applications deployed on the server are displayed.

Use this view to see alarm conditions for all monitored equipment. The Alarm Browser button, Log Browser button, and OM Browser button are disabled until you select an network element instance, server, or Avaya media server.

Related links

Logical and physical views of network elements on page 32

Recommended PC hardware and software requirements for running Element Manager Console

Avaya recommends that the management PC (the PC that you use to run Avaya Aura® Conferencing Element Manager Console) meets the requirements described in the following table.

Category	Minimum requirement	Recommended requirement
Processor	600 MHz Pentium-class or equivalent processor	1.0 GHz (or higher) Pentium-class or equivalent processor
Available RAM	64 MB of RAM This requirement is in addition to the memory requirements of the operating system and other concurrent applications.	64 MB of RAM This requirement is in addition to the memory requirements of the operating system and other concurrent applications.
Available hard disk space	50 MB	50 MB
Mouse	Required	Required
Video graphics card	800 x 600 @16bpp [65,536 colors] VGA	1024x768 @16bpp [65,536 colors] VGA or better
Sound card	Not applicable	Not applicable
Operating system	Microsoft Windows 7, 8, 10, or Microsoft Server 2003.	Microsoft Windows 7, 8, 10, or Microsoft Server 2003
Network connectivity	56 Kbps modem	10Base-T or other fast network connection (such as DSL, Cable, or LAN)
Internet browser	Microsoft Internet Explorer 7.0, 8.0, 9.0, 10.0, 11.0 Mozilla Firefox 10 Google Chrome 35	Microsoft Internet Explorer 7.0, 8.0, 9.0, 10.0, 11.0 Mozilla Firefox 10 or later Google Chrome 35
Java	Latest Oracle JRE Version 1.7	Latest Oracle JRE Version 1.7
Cookies	Enabled	Enabled
Javascript	Enabled	Enabled

Important:

If you use a Proxy server in the Java network configuration, the Proxy server must allow access to the IP address and port. If there is no access to the IP address and port, use the Direct Connection option in the Java network configuration.

Related links

Element Manager Console overview on page 29

Logging on to Element Manager Console

There are two ways to log on to Element Manager Console:

- single sign-on access through Avaya Aura® System Manager (This applies to Avaya Aura® deployments only.)
- locally (This applies to both Avaya Aura® and Turnkey deployments.)

Single sign-on access through Avaya Aura® System Manager

For single sign-on access through Avaya Aura® System Manager, you must use the Avaya Aura® System Manager default administrative account or an account that is configured for accessing Avaya Aura® Conferencing. To log on to Element Manager Console using single sign-on access, you must log into the central login page for Single Sign-On for System Manager. Once you log into System Manager successfully, you can access Element Manager Console from the Conferencing Dashboard in System Manager.

When you log on to Element Manager Console using single sign-on access through Avaya Aura® System Manager, System Manager controls password administration, session time limits, and the administrative tasks you can perform in Element Manager Console.

Note:

Unless instructed by Avaya Support, you should always log on to Element Manager Console using single sign-on access through Avaya Aura® System Manager.

Local logon access

For local logon access to Element Manager Console, you must have a local logon user ID. Element Manager Console provides the following local logon user IDs:

- admin
- admin1
- admin2
- admin3
- admin4
- admin5

Local logon user IDs have “expert privileges,” which enables a local logon user to have unrestricted administrative capabilities in Element Manager Console. When you log on to Element Manager Console with a local logon user ID, Element Manager Console controls password administration and login rules. Using a local logon user ID, you can access the Administration menu in Element Manager Console, which enables you:

- change the password for the local logon user IDs
- configure the password rules for the local logon user IDs
- configure the login rules for the local logon user IDs
- view the users currently logged on to Element Manager Console
- log out (force off) a user from Element Manager Console

Note:

The Administration menu is only available when you log on to Element Manager Console locally.

Warning:

Unless instructed by Avaya Support, you should always log on to Element Manager Console using single sign-on access through Avaya Aura® System Manager.

Related links

Element Manager Console overview on page 29
Logging on to Element Manager Console via System Manager on page 35
Logging on to Element Manager Console Locally on page 36

Logging on to Element Manager Console via System Manager

Note:

This method of logging on to Element Manager only applies to Avaya Aura® deployments.

Before you begin

You must use the Avaya Aura® System Manager default administrator account or an alternative administrative account that is configured for accessing Avaya Aura® Conferencing.

Procedure

1. On the management PC, open the browser.
2. Go to the central login page for Single Sign-On for System Manager.
3. In the User ID box on the System Manager Log On page, enter your user name.
4. In the Password box, enter your password.
5. Click **Log On**.
6. In the Elements area on the System Manager console, click **Conferencing**.
7. In the Name column on the Conferencing Dashboard, click on the name of Element Manager Console.

   A new browser window appears and displays the Element Manager Console window.
8. If you want to configure initial Differentiated Services Code Point (DSCP) values for outgoing network packets (High Throughput Data Network packets and Low Latency Data Network packets) before you log on, perform the following steps:
   a. On the Element Manager Console window, click **Advanced**.
   b. Click the right arrow button next to the tabs to scroll to the **DSCP Marking** tab.
   c. Click the **DSCP Marking** tab.
   d. On the DSCP Marking tab, configure the settings.
   e. When finished, click the **Ok** button.
9. From the IPv4 Service Address box on the Element Manager Console window, select the IP address of the server running Element Management Console.

10. Click **Connect**.
11. On the Element Manager Authentication window, click **Accept the certificate for this session only**.
12. Click **Apply**.

    The Element Manager Console window appears.

Related links

Logging on to Element Manager Console on page 34

Logging on to Element Manager Console Locally

About this task

Use this procedure to log on to Element Manager Console using a local logon user ID (for example, admin).

If your system supports security mode, you can use secure mode to connect to the Element Manager Console.

You can configure initial Differentiated Services Code Point (DSCP) values for outgoing network packets (High Throughput Data Network packets and Low Latency Data Network packets) before you log on.

Note:

If you have an Avaya Aura® deployment, you should only perform this procedure if you are unable to log onto Element Manager Console from Avaya Aura® System Manager. See Logging on to Element Manager Console via System Manager on page 35.

Procedure

1. On the management PC, open the browser.
2. In the Address box, enter the following address:
   - For normal access: `http://<IP address>:12120`

     where <*IP address*> is the EM Internal OAM Service IP address. (This is the logical IP address of the server running Element Manager Console.)
   - For secure access: `https://<IP address>:12121`

     where <*IP address*> is the EM Internal OAM Service IP address. (This is the logical IP address of the server running Element Manager Console.)
3. Press **ENTER** on your keyboard.
4. On the <IP address> page, click **Launch Element Manager Console**.

   The Element Manager Console window appears.

5. If you want to configure initial Differentiated Services Code Point (DSCP) values for outgoing network packets (High Throughput Data Network packets and Low Latency Data Network packets) before you log on, perform the following steps:
   a. On the Element Manager Console window, click **Advanced**.
   b. Click the right arrow button next to the tabs to scroll to the **DSCP Marking** tab.
   c. Click the **DSCP Marking** tab.
   d. On the DSCP Marking tab, configure the settings.
   e. When finished, click the **Ok** button.
6. From the IPv4 Service Address box on the Element Manager Console window, select the IP address of the server running Element Manager Console.
7. Click **Connect**.
8. On the Element Manager Authentication window, click **Accept the certificate for this session only**.
9. Click **Apply**.
10. In the UserID box on the Element Manager Console window, enter the local login name.
11. In the Current Password box, enter the password for the local login name.
12. (Optional) If you must end a previous session to log on, select the **ForceOut** check box.
13. Click **Ok**.

    The Element Manager Console window appears.

Related links

Logging on to Element Manager Console on page 34

Logging off from Element Manager Console

Procedure

From the Element Manager Console menu bar, select **File > Exit**.

Related links

Element Manager Console overview on page 29

Conferencing Reports & Monitors Overview

The Avaya Conferencing Reports & Monitors application enables you to monitor key performance indicators (KPIs) in the Avaya Aura® Conferencing system. Key performance indicators such as the number of active conferences or sessions, the amount of bandwidth in use at a location, and the number of Avaya Aura® Conferencing licenses in use can help you understand how the system is operating currently and how the system has been operating in the past. Some key performance

indicators will display an alert when they exceed specific thresholds. With these key performance indicators, you can identify and troubleshoot problems or plan for system expansion.

Monitoring bandwidth usage is extremely important because much of the day-to-day cost of conferencing is related to how much bandwidth is being used. The key performance indicators you can monitor with Avaya Conferencing Reports & Monitors will provide insight into how much bandwidth Avaya Aura® Conferencing is using (and not using).

Avaya Conferencing Reports & Monitors uses charts and graphs to display current and historical data for:

- the Avaya Aura® Conferencing system
- each location
- each media server
- each web conference server
- an individual conference
- an individual session

From Avaya Conferencing Reports & Monitors, you can export this data to a .CSV file.

Avaya Conferencing Reports & Monitors obtains the Avaya Aura® Conferencing data from the following sources:

- current operational measurements (OMs). Avaya Conferencing Reports & Monitors queries the Avaya Aura® Conferencing element manager for the current values of the OMs and converts them into the appropriate chart, graph, or table column.
- persisted OMs. Avaya Aura® Conferencing stores the OM values in its database at 15-minutes intervals. (Each 15-minute interval is referred to as an office transfer period.) These values are saved in the database for up to 30 days. Avaya Conferencing Reports & Monitors can retrieve this persisted OM data and present it in historical reports.
- live data. Avaya Conferencing Reports & Monitors can query an Avaya Aura® Conferencing element for some other type of data or report.

Related links

Management Tools on page 29
KPI alerts on page 38
Alert indication on page 39
Conference live monitoring on page 39
Session live monitoring on page 41
Starting Avaya Conferencing Reports & Monitors on page 42

KPI alerts

The KPI alerts feature adds indication of the data that requires administrator attention in the Avaya Conferencing Reports & Monitors application. The main purpose of this feature is to bring

administrator attention to the values which require the administrator to perform some actions (such as values which exceed thresholds or high severity events). KPI alerts are different than alarms. Alarms are generated on the server side and are displayed in the Element Manager Console and possibly sent to the external device using SNMP traps. KPI alerts are raised on the client to indicate system performance and system resources. KPI alerts are not logged anywhere. When system performance becomes better, the KPI alert is automatically removed.

Administrators can disable KPI alerts using threshold configuration, but they are not able to clear KPI alerts. When the data is above the threshold, a color-coded icon appears and tooltips are added, describing why alert has been raised. Thresholds configuration is performed from the Element Manager Console. There are minor, major, and critical threshold levels for each type of data.

Some KPI alerts, such as license usage alerts, may have an associated alarm on the Element Manager Console because they use the same thresholds.

Related links

Conferencing Reports & Monitors Overview on page 37

Alert indication

The alert icon (indicated by an exclamation point inside of a circle) indicates a minor, major, or critical alert, as follows:

- A yellow icon indicates a minor alert.
- An orange icon indicates a major alert.
- A red icon indicates a critical alert.

For a chart, the alert icon is centered above the column that shows the associated data. A column tooltip shows alert information.

For a table, the row that contains an alert is shaded with the color of the maximum severity alert in the row. For example, if the row contains both a minor and major alert, the row appears orange (for a major alert). A tooltip on the cell shows alarm information.

For an area chart, only the most severe threshold that is crossed is displayed. Not all thresholds are shown at the same time.

Related links

Conferencing Reports & Monitors Overview on page 37

Conference live monitoring

Conference live monitoring displays information about started/ended sessions, bandwidth changes, and other in-conference events. Every event is assigned one of the following severity levels:

- minor

- major
- critical

The activity log records every event and the severity of the event. Major events are highlighted in the activity log. The system generates an alert for every major event and critical event.

For some events, one of the following reasons may be provided:

- Conference full.
- Reason – proactive thinning.
- No audio bandwidth available.
- No video bandwidth available.
- No audio license available.
- Bandwidth optimization applied.

Minor events

The system supports the following “minor” events:

- Conference started.
- Conference ended.
- The chair person has left the conference. The conference will end in a few minutes.
- The chair person has joined the conference. The conference is now starting.
- Presentation mode is enabled.
- Presentation mode is disabled.
- Conference locked.
- Conference unlocked.
- Continuation enabled.
- Continuation disabled.
- Entry and exit notification enabled.
- Entry and exit notification disabled.
- Conference muted.
- Conference unmuted.
- Conference audio muted.
- Conference audio unmuted.
- Conference video muted.
- Conference video unmuted.
- Conference recording started
- Conference recording stopped
- Video enabled.

- Video disabled.
- Web conference started.
- Web conference ended.
- <Priority> priority session <session name> closed.
- <Priority> priority session added.
- <Priority> priority session video downgraded.
- Session <session name> joined web collaboration.
- Session <session name> left web collaboration.
- Session <session name> promoted to presenter.
- Session <session name> demoted from presenter.
- Video downgrade by proactive thinning.

Major events

The system supports the following “major” events:

- <Priority> priority session rejected <reason>.
- <Priority> priority session downgraded to audio only.
- Video downgrade by reactive thinning.
- Downgrade to audio-only by proactive thinning.

Critical events

The system supports the following “critical” events:

- Downgrade to audio-only by reactive thinning.

Related links

Conferencing Reports & Monitors Overview on page 37

Session live monitoring

Session live monitoring displays information about session bandwidth changes and other in-session events. Every event is assigned one of the following severity levels:

- minor
- major
- critical

The activity log records every event and the severity of the event. Major events are highlighted in the activity log. The system generates an alert for every major event and critical event.

For some events, the following reason may be provided:

- Bandwidth optimization applied.

Minor events

The system supports the following “minor” events:

- Audio muted.
- Audio unmuted.
- Video muted.
- Video unmuted.
- User promoted to moderator.
- User promoted to presenter.
- User demoted from presenter.
- On hold.
- Off hold.
- Video downgraded. <reason>.
- Session joined web collaboration.
- Session left web collaboration.
- User promoted to presenter.
- User demoted from presenter.
- User joined audio/video conference.
- User left audio/video conference.
- Video downgrade by proactive thinning.

Major events

The system supports the following “major” events:

- Video downgrade by reactive thinning.
- Downgrade to audio-only by proactive thinning.
- Downgrade to audio only. <reason>.

Critical events

The system supports the following “critical” events:

- Downgrade to audio-only by reactive thinning.

Related links

Conferencing Reports & Monitors Overview on page 37

Starting Avaya Conferencing Reports & Monitors

About this task

Use this procedure to start the Avaya Conferencing Reports & Monitors application. From Avaya Conferencing Reports & Monitors, you can monitor and generate reports on key performance indicators.

Procedure

In the navigation pane of Element Manager Console, click **Key Performance Indicators > Monitoring and Reporting**.

Related links

Conferencing Reports & Monitors Overview on page 37

Chapter 4: Monitoring alarms

The Alarm Summary bar at the top of the Element Manager Console window provides a concise, system-wide summary of alarms for managed and monitored network elements. The background color of the alarm bar indicates the most severe alarm for the system. The alarm color codes are:

- Blue - warning
- Green - no alarms
- Yellow - minor
- Orange - major
- Red - critical

The total number of alarms for the system, as well as the number of alarms of reach severity level appears on the alarm summary bar. The summary bar also includes a section called ACK Critical, which shows the number of previously acknowledged, but not yet cleared alarms.

The Alarm Browser window enables you to view the details for alarms that originate from the selected service or server.

Viewing alarms

The Alarm Browser window enables you to view details about any alarms on your system. You can access the Alarm Browser window using the following methods:

- from the navigation pane in Element Manager Console
- from Logical View window in Element Manager Console
- from Physical View window in Element Manager Console

Viewing alarms from the navigation pane of Element Manager Console

Before you begin

The server monitor must be running.

About this task

Use this procedure to view the alarms of a server or feature server element by selecting the server or feature server element from the navigation panel of Element Manager Console.

Note:

You cannot view the alarms for the logical databases using this procedure.

Procedure

1. In the navigation panel of Element Manager Console select the server or feature server element in which you are interested.

   The Alarm Browser, OM Browser, and Log Browser buttons on the tool bar at the top of the Element Manager Console window become enabled.

2. On the tool bar, click **Alarm Browser**.

   The Alarm Browser window appears and displays the alarms associated with the selected network element.

3. To view the details for an alarm, select the alarm in the top of the Alarm Browser window.

   The detailed information for the selected alarm appears in the Alarm Details area.

4. To refresh the list of active alarms displayed, click **Refresh**.

Related links

Starting the monitor service for a server on page 119
Viewing alarms from the Logical View window of Element Manager Console on page 45
Viewing alarms from the Physical View window of Element Manager Console on page 46

Viewing alarms from the Logical View window of Element Manager Console

Before you begin

The server monitor must be running.

Procedure

1. Perform one of the following steps:
   - Click the Alarm bar at the top of the Element Manager Console window, and select **Logical View**.
   - On the tool bar in Element Manager Console, click **Logical View**.
2. In the Logical View window, select the server or feature server element in which you are interested.

   The Alarm Browser, OM Browser, and Log Browser buttons at the bottom of the Logical View window become enabled.

3. In the Logical View window, click **Alarm Browser**.

   The Alarm Browser window appears and displays all alarms associated with the selected network element.

4. To view the details for an alarm, select the alarm in the top of the Alarm Browser window.

   The detailed information for the selected alarm appears in the Alarm Details area.

5. To refresh the list of active alarms displayed, click **Refresh**.

Related links

Starting the monitor service for a server on page 119
Viewing alarms from the navigation pane of Element Manager Console on page 44
Viewing alarms from the Physical View window of Element Manager Console on page 46

Viewing alarms from the Physical View window of Element Manager Console

Before you begin

The server monitor must be running.

Procedure

1. Perform one of the following steps:
   - Click the Alarm bar at the top of the Element Manager Console window, and select **Physical View**.
   - On the tool bar in Element Manager Console, click **Physical View**.
2. In the Physical View window, select the server or feature server element in which you are interested.

   The Alarm Browser, OM Browser, and Log Browser buttons at the bottom of the Physical View window become enabled.

3. In the Physical View window, click **Alarm Browser**.

   The Alarm Browser window appears and displays all alarms associated with the selected network element.

4. To view the details for an alarm, select the alarm in the top of the Alarm Browser window.

   The detailed information for the selected alarm appears in the Alarm Details area.

5. To refresh the list of active alarms displayed, click **Refresh**.

Related links

Starting the monitor service for a server on page 119
Viewing alarms from the Logical View window of Element Manager Console on page 45
Viewing alarms from the navigation pane of Element Manager Console on page 44

Sorting alarms

About this task

Use this task to change the order in which alarms are displayed in the Alarm Browser window. You can sort alarms according to the following attributes:

- Alarm name
- Time stamp
- Severity
- Short family name
- Fault number
- Acknowledged

By default, alarms appear in order of severity, with the most severe alarm listed at the top.

Procedure

1. In the Alarm Browser window, click the column heading of the attribute by which you want to sort the alarms.

   The alarms appear either in alphabetical or numerical order, depending on the alarm attribute.

2. Click the column heading a second time to reverse the order.

Clearing and acknowledging alarms

About this task

Some alarms can be cleared manually. Use this task to clear and acknowledge alarms manually. For alarms that can be cleared manually, the **Clear** and **Acknowledge** buttons are enabled.

Procedure

1. In the Alarm Browser window, select the alarm to want to clear or acknowledge.

   If the **Clear** button or **Acknowledge** button is inactive, the alarm is not manually clearable.

2. Note the corrective action displayed in the Alarms Details area for the selected alarm.
3. Do one of the following:
   - To clear an alarm, click **Clear**.
   - To acknowledge an alarm, click **Acknowledge**.
4. Click **Refresh** to refresh the list of active alarms displayed in the Alarm Browser window, .

   If you acknowledge an alarm, that alarm remains in the Alarm Browser window, and the acknowledged status field changes from **False** to **True**. After you clear or acknowledge all

alarms, the Alarm Summary bar at the top of the Element Manager Console color turns green.

You can configure Avaya Aura® Conferencing to forward alarms to the SAL gateway, to Avaya Aura® System Manager, or to an external Simple Network Management Protocol (SNMP) manager.

If you choose to forward alarms to an external SNMP manager, you require the SNMP Management Information Base (MIB) file. The MIB file for Avaya Aura® Conferencing is called AVCONFERENCING-MIB.mib and is stored on the Avaya Aura® Conferencing DVD in the following location:

```
dvd_AAC_MCP_X.X.X.XX_XXXX-XX-XX-XXXX_coreApps.iso
        MCP_XX.X.X.XX_XXXX-XX-XX-XXXX.zip
                clientAPIs
                        mibs
                                AVCONFERENCING-MIB.mib
```

In terms of Simple Network Management Protocol (SNMP) support, Avaya Aura® Conferencing supports the SNMP v1 and SNMP v2c protocols.

Best practice

The AVCONFERENCING-MIB.mib file contains over 1800 traps (alarms). There are a large number of traps because some alarms can be raised with different severity levels and there is a unique trap to clear each level of alarm severity. As a result, there are actually only about 400 alarms that Avaya Aura® Conferencing can theoretically raise.

Avaya Aura® Conferencing administrators should always monitor the external SNMP manager for traps. However, alarms that are not classed as “Clear” or “Warning” are of particular importance. They indicate an issue with the system.

“Clear” alarms end with the letter “C” and “Warning” alarms end with the pattern ‘WARNING*dd*r where *dd* is any two digits

Chapter 5: Monitoring event logs

The Logs window enables you to view the event logs for network elements. You can access the Logs window using the following methods:

- from the navigation pane in Element Manager Console
- from Logical View window in Element Manager Console
- from Physical View window in Element Manager Console

You should review event logs periodically so you can identify any potential problems.

Viewing logs from the navigation pane of Element Manager Console

Before you begin

The server monitor must be running.

About this task

Use this procedure to view the log of a server or feature server element by selecting the server or feature server element from the navigation panel of Element Manager Console.

Note:

You cannot view the logs for the logical databases using this procedure.

Procedure

1. In the navigation panel of Element Manager Console, select the server or feature server element in which you are interested.

   The Alarm Browser, OM Browser, and Log Browser buttons on the tool bar at the top of the Element Manager Console window become enabled.

2. On the tool bar, click **Log Browser**.

   The Logs window appears and displays the logs for the selected network element. If the selected network element type is redundant, a Logs window appears for each instance of the network element.

Related links

Starting the monitor service for a server on page 119

Viewing logs from the Logical View window of Element Manager Console on page 50
Viewing logs from the Physical View window of Element Manager Console on page 50

Viewing logs from the Logical View window of Element Manager Console

Before you begin

The server monitor must be running.

About this task

Use this procedure to view the log of a server, feature server element, or logical database from the Logical View window of Element Manager Console.

Procedure

1. Perform one of the following steps:
   - Click the Alarm bar at the top of the Element Manager Console window, and select **Logical View**.
   - On the tool bar in Element Manager Console, click **Logical View**.
2. In the Logical View window, select the server or feature server element in which you are interested.

   The Alarm Browser, OM Browser, and Log Browser buttons at the bottom of the Logical View window become enabled.
3. In the Logical View window, click **Log Browser**.

   The Logs window appears and displays the logs for the selected network element. If the selected network element type is redundant, a Logs window appears for each instance of the network element.

Related links

Starting the monitor service for a server on page 119
Viewing logs from the navigation pane of Element Manager Console on page 49
Viewing logs from the Physical View window of Element Manager Console on page 50

Viewing logs from the Physical View window of Element Manager Console

Before you begin

The server monitor must be running.

About this task

Use this procedure to view the log of a server, feature server element, or logical database from the Physical View window of Element Manager Console.

Procedure

1. Perform one of the following steps:
   - Click the Alarm bar at the top of the Element Manager Console window, and select **Physical View**.
   - On the tool bar in Element Manager Console, click **Physical View**.
2. In the Physical View window, select the server or feature server element in which you are interested.

   The Alarm Browser, OM Browser, and Log Browser buttons at the bottom of the Physical View window become enabled.
3. In the Physical View window, click **Log Browser**.

   The Logs window appears and displays the logs for the selected network element. If the selected network element type is redundant, a Logs window appears for each instance of the network element.

Related links

Starting the monitor service for a server on page 119
Viewing logs from the Logical View window of Element Manager Console on page 50
Viewing logs from the navigation pane of Element Manager Console on page 49

Monitoring syslog

Syslog server

You must configure the syslog according to the instructions in *Deploying Avaya Aura® Conferencing*, which is available on https://support.avaya.com/. You can use the script `reconfigure.pl` to configure the Syslog server on a live system. You must restart the system once the reconfiguration is complete. Once the Syslog server is configured, Avaya Aura® Conferencing sends all the information from `/var/mcp/oss/logs` to the Syslog server. This information is stored in `/var/log/`.

Configuring log level

Log level refers to the verbosity level of the logging output. There are four log levels:

- OFF
- NORMAL
- TERSE
- VERBOSE

By default, most of the families are set to OFF.

About this task

Use this task to configure the log level.

Procedure

1. Log on to the network element through SSH and enter the required password information.
2. At the prompt, type `telnet localhost <NE debug port>`. E.g for PROV default port is 24000. It is configured in EM console.

   For example, the Provisioning Client default port is 24000.

   You can configure the ports for the network elements using the Element Manager console.
3. Type `debuglevel get all`.
4. Type `debuglevel set <FAMILY> <level>`.

   For example:

   ```
   debuglevel set OPIS terse
   ```

Result

Bear in mind that increasing the log level for any log family may cause excessive log output. Some of them are used only for a short term debug session. Avaya recommends increasing the level for a certain family only if the system has a potential problem in this area.

Chapter 6: Monitoring operational measurements

Operational measurements (OMs) provide statistical information about the server and network element operations and performances. OMs are represented by groups, which contain registers (counters and gauges) that provide performance-related data.

Viewing OM details from the navigation pane of Element Manager Console

Before you begin

The server monitor must be running. See Starting the monitor service for a server on page 119.

About this task

Use this procedure to view the OM details of a server or feature server element by selecting the server or feature server element from the navigation panel of Element Manager Console.

Note:

You cannot view the OM details for the logical databases using this procedure.

Procedure

1. In the navigation panel of Element Manager Console, select the server or feature server element in which you are interested.

   The Alarm Browser, OM Browser, and Log Browser buttons on the tool bar at the top of the Element Manager Console window become enabled.

2. On the tool bar, click **OM Browser**.

   The OM Browser window appears and displays the OM details for the selected network element. By default, the browser queries active OMs.

3. To view register information of a specific OM group, select the group in which you are interested from the OM Group box.

   The registers and statistics for the selected OM group appear in the OM Details area.

Viewing OM details from the Logical View window of Element Manager Console

Before you begin

The server monitor must be running. See Starting the monitor service for a server on page 119.

Procedure

1. Perform one of the following steps:
   - Click the Alarm bar at the top of the Element Manager Console window, and select **Logical View**.
   - On the tool bar in Element Manager Console, click **Logical View**.
2. In the Logical View window, select the server or feature server element in which you are interested.

   The Alarm Browser, OM Browser, and Log Browser buttons at the bottom of the Logical View window become enabled.
3. In the Logical View window, click **OM Browser**.

   The OM Browser window appears and displays the OM details for the selected network element. By default, the browser queries active OMs.
4. To view register information of a specific OM group, select the group in which you are interested from the OM Group box.

   The registers and statistics for the selected OM group appear in the OM Details area.

Viewing OM details from the Physical View window of Element Manager Console

Before you begin

The server monitor must be running. See Starting the monitor service for a server on page 119.

Procedure

1. Perform one of the following steps:
   - Click the Alarm bar at the top of the Element Manager Console window, and select **Physical View**.
   - On the tool bar in Element Manager Console, click **Physical View**.
2. In the Physical View window, select the server or feature server element in which you are interested.

   The Alarm Browser, OM Browser, and Log Browser buttons at the bottom of the Physical View window become enabled.

3. In the Physical View window, click **OM Browser**.

   The OM Browser window appears and displays the OM details for the selected network element. By default, the browser queries active OMs.

4. To view register information of a specific OM group, select the group in which you are interested from the OM Group box.

   The registers and statistics for the selected OM group appear in the OM Details area.

Refreshing data in the OM Browser window

About this task

The system updates the OM data according to the interval configured for the OfficeTransferPeriod configuration parameter. After the OM Browser window is open for an extended period, you can query the latest OM data.

Procedure

1. In the OM Browser window, select **Active** or **Holding** from the Type box.
2. Click **Refresh**.

Chapter 7: Monitoring key performance indicators

Using the Avaya Conferencing Reports & Monitors application, administrators can monitor key performance indicators (KPIs) in order to understand how the system is operating at any point in time. Examples of KPIs include the number of active conferences or sessions, bandwidth in use at a location, and the number of licenses in use. KPIs provide insight into what is currently occurring on the system now or what has occurred on the system at some point in the past. An administrator can use these measurements to find problems or to plan for system expansion.

Related links

Modifying the alert thresholds for key performance indicators on page 56
Generating a report for a server on page 110

Modifying the alert thresholds for key performance indicators

About this task

Use this procedure to modify the alert thresholds for key performance indicators.

Once you modify the value for an alert threshold, that change is not applied immediately to the Avaya Conferencing Reports & Monitoring application (that is, the value persists in the database). The new alert threshold value is applied with the network configuration data (in a maximum of five minutes). If you want this value to be applied immediately, you must restart the Avaya Conferencing Reports & Monitoring application.

Procedure

1. In the navigation pane of Element Manager Console, click **Key Performance Indicators > Alert Thresholds**.
2. In the KPI Alert Thresholds window, select the parameter you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit dialog box, make your changes. See Configurable thresholds and default values on page 57.

If you want to disable an alert threshold, select the minimum value for that threshold (typically 0).

Note:

When you disable an alert threshold, that threshold is not displayed in the Avaya Conferencing Reports & Monitoring application. If the major threshold for an alert is disabled, and the minor threshold for that alert is enabled, only the minor and critical thresholds for the alert are displayed in the Avaya Conferencing Reports & Monitoring application.

5. When finished, click **Apply**.

Related links

Monitoring key performance indicators on page 56
Configurable thresholds and default values on page 57

Configurable thresholds and default values

Name	Minor	Major	Critical	Minimum	Maximum
Audio packet loss	5	10	15	0 (off)	100
Delay (ms)	250 ms	350 ms	500 ms	0 (off)	2500 ms
Failed meeting requests	2	5	10	0 (off)	100
Failed sessions	2	5	10	0 (off)	100
Jitter (ms)	3 ms	5 ms	10 ms	0 (off)	50 ms
Multimedia bandwidth usage	50	80	90	0 (off)	100
R-factor	90	85	70	0 (off)	100
Session completion ratio	95	90	80	0 (off)	100
Sessions with R-factor < 70	5	10	20	0 (off)	100
Sessions with packet loss	5	10	20	0 (off)	100
Total bandwidth usage	50	80	90	0 (off)	100
Video packet loss	5	10	15	0 (off)	100
Session licenses usage	50	80	90	0 (off)	100
User licenses usage	50	80	90	0 (off)	100

Related links

Modifying the alert thresholds for key performance indicators on page 56

Viewing general performance data

Viewing the current data for Avaya Aura® Conferencing

About this task

The Conferencing Reports & Monitors application will display the following current data for the application server in a bar graph format:

- number of active conferences (active, cascaded, and recording)
- number of active sessions (and type)
- theoretical requested, connection requested, negotiated, and actual bandwidth for the entire Avaya Aura Conferencing system
- theoretical requested, connection requested, negotiated, and actual bandwidth for each location
- total bandwidth savings, cascaded savings, gap savings, and thinning savings for the entire Avaya Aura Conferencing system
- total bandwidth savings, cascaded savings, gap savings, and thinning savings for each location
- number of available and consumed licenses

If you place your mouse over a bar in a graph, details for the associated bar are displayed. This data is constantly updated at the time interval you specify.

Procedure

1. In the Conferencing Reports & Monitors window, click the **General** tab.
2. On the Dashboard page, click the **Performance** tab. For more information, see General page - Performance tab field descriptions on page 59.
3. From the Update period box, enter the number of seconds at which you want the updated data to be displayed.
4. To view the bandwidth usage for the entire Avaya Aura Conferencing system, click **Click here for details** below the Total Usage graph. See General page - Performance tab field descriptions on page 59 (**Total Savings** row).
5. To view the bandwidth usage for a specific location, click the name of the appropriate location below the Bandwidth Usage per Location graph. See Location page - Bandwidth tab field descriptions on page 70.
6. To view the bandwidth savings for a specific location, click the name of the appropriate location below the Bandwidth Savings per Location graph. See Location page - Bandwidth tab field descriptions on page 70
7. To view the license information, click the **Resources** tab.

Related links

Monitoring key performance indicators on page 56

General tab on page 59

General page - Performance tab field descriptions on page 59

General tab

The General tab provides a “dashboard” that provides charts and graphs of high-level performance information for the Avaya Aura® Conferencing system. From this tab, you can view current performance information, current resource information, and historical performance information, and historical bandwidth information.

To view the current performance information for the Avaya Aura® Conferencing system, click the **Performance** tab. See General page - Current tab field descriptions on page 59.

To view the current resource information for the Avaya Aura® Conferencing system, click the **Resource** tab. See General page - Current tab field descriptions on page 59.

To view historical performance information for the Avaya Aura® Conferencing system, click the **Performance History** tab. See General page - History tab field descriptions on page 62.

To view historical bandwidth information for the Avaya Aura® Conferencing system, click the **Bandwidth History** tab. See General page - History tab field descriptions on page 62.

See also:

- Viewing the current data for Conferencing on page 58
- Viewing the historical data for Conferencing on page 61

Related links

Viewing the current data for Avaya Aura Conferencing on page 58

General page - Performance tab field descriptions

Use this page to view information about the current state of the Avaya Aura® Conferencing system.

Place the mouse over any bar in a chart to view more detailed information.

The system provides alerts for the following data:

- Percentage of failed sessions compared to the overall session attempts
- Percentage of sessions with R-factor < 70 compared to the number of active sessions
- Percentage of sessions with packet loss compared to the number of active sessions
- Number of consumed licenses < Number of available licenses (for server, audio, and audio/video)
- Percentage of negotiated send/receive bandwidth for location comparing to the total bandwidth configured
- Location name that has total bandwidth usage percentage above threshold
- Location name that has multimedia bandwidth usage percentage above threshold
- Session completion ratio

Name	Description
Update period	Enter the number of seconds at which you want updated data to be displayed.
Conferences	The **Active** chart shows the current number of active conferences, the current number of active conferences that are cascaded, and the current number of active conferences that are recording. The **Last x minutes** chart shows the number of started conferences for the displayed time period. This data is cleared every 15 minutes.
Sessions	The **Active** chart shows the current number of active audio sessions, video sessions, and web sessions. This chart also shows the current number of active sessions with an R-factor of less than 70 and packet loss. The **Last x minutes** chart shows the number of successful, failed, dropped, and downgraded sessions for the displayed time period. This data is cleared every 15 minutes.
Total Usage	Shows the total WAN bandwidth usage for the entire Avaya Aura® Conferencing system. The transmitted and received values are displayed for theoretical bandwidth, connection requested bandwidth, negotiated bandwidth, and actual bandwidth. If you place the mouse over the actual bar, you can see the total usage for the selected category. To enlarge this chart, click on it. To view more information about the total bandwidth usage for the system, click **Click here for details** below the chart.
Bandwidth Usage per Location	Shows the WAN bandwidth usage for each location. The transmitted and received values are displayed for theoretical bandwidth, connection requested bandwidth, negotiated bandwidth, and actual bandwidth. If you place the mouse over the actual bar, you can see the total usage for the selected category. To enlarge this chart, click on it. To view more information about bandwidth usage for a location, click on the name of the location below the chart.
Total Savings	Shows the total WAN bandwidth savings for the entire Avaya Aura® Conferencing system. The

Table continues…

Name	Description
	transmitted and received values are displayed for total bandwidth savings, cascaded bandwidth savings, gap bandwidth savings, and thinning bandwidth savings. If you place the mouse over the actual bar, you can see the total savings for the selected category. To enlarge this chart, click on it. To view more information about the total bandwidth savings for the system, click **Click here for details** below the chart.
Bandwidth Savings per Location	Shows the WAN bandwidth savings for each location. The transmitted and received values are displayed for theoretical total bandwidth savings, cascaded bandwidth savings, gap bandwidth savings, and thinning bandwidth savings. If you place the mouse over the actual bar, you can see the total savings for the selected category. To enlarge this chart, click on it. To view more information about bandwidth usage for a location, click on the name of the location below the chart.

See also:

- General tab on page 59
- Viewing the current data for Conferencing on page 58

Related links

Viewing the current data for Avaya Aura Conferencing on page 58

Viewing the historical performance data for Avaya Aura® Conferencing

About this task

The Conferencing Reports & Monitors application will display the following historical performance data for the application server in a bar graph format:

- duration of all audio calls, video calls, web collaboration sessions, and recordings
- performance indicators for conferences and sessions
- session completion ratios
- total bandwidth usage
- bandwidth usage per location

- total bandwidth savings
- bandwidth savings per location

If you place your mouse over a bar in a graph, details for the associated bar are displayed. You can view data for the last hour, 24 hours, 7 days, or 30 days.

Procedure

1. In the Conferencing Reports & Monitors window, click the **General** tab.
2. On the Dashboard page, click the **Performance History** tab. For more information, see General page - Performance History tab field descriptions on page 62.
3. From the Showing historical data for box, select the time period in which you are interested.
4. From the Instance box, select the instance of the application server from which you want to view data. If you have a redundant configuration, be sure to select the active instance.
5. To view the historical bandwidth usage and savings, click the **Bandwidth History** tab.

Related links

Monitoring key performance indicators on page 56
General page - Performance History tab field descriptions on page 62

General page - Performance History tab field descriptions

Use this page to view historical performance information about the Avaya Aura® Conferencing system.

Place the mouse over any bar in a chart to view more detailed information.

The system provides alerts for the following data:

- Percentage of failed sessions compared to the overall session attempts
- Percentage of sessions with R-factor < 70 compared to the number of active sessions
- Percentage of sessions with packet loss compared to the number of active sessions
- Session completion ratio

Name	Description
Conference Usage by Size/Minutes/User Agent	Shows the conference usage. You can click **Size**, **Minutes**, or **User Agent** to view a pie chart of the breakdown of conference usage. For example, if you click **Size**, the chart shows the percentage of conferences that contained the various numbers of participants: 1–2, 5–6, and so on.
Showing historical data for	Select the time period for which you want to view historical data. Choices are: • Last Hour • Last 24 Hours • Last 7 Days

Table continues…

Name	Description
	• Last 30 Days
Instance	Select the instance of the application server from which you want to view data. If you have a redundant configuration (the application server has more than one instance), be sure to select the active instance.
Usage	Shows the duration (in minutes) of all audio calls, video calls, web collaboration sessions, and recordings during the specified time period.
Performance	The **Conferences** chart shows the number of successful conferences during the specified time period. The **Sessions** chart shows the number of successful audio sessions, video sessions, and web sessions during the specified time period. This chart also shows the number of failed sessions, dropped sessions, downgraded sessions, sessions with an R-factor of less than 70, and packet loss during the specified time period.
Session Completion Ratio	Shows the session completion ration during the specified time period.
EXPORT	Saves the displayed historical data to a .CSV file.

See also:

- General tab on page 59
- Viewing the historical data for Conferencing on page 61

Related links

Viewing the historical performance data for Avaya Aura Conferencing on page 61

Viewing location data

Viewing the data for a location

About this task

The Conferencing Reports & Monitors application will display the following performance data for the location(s) you specify:

- number of sessions (audio and video)
- total negotiated and actual bandwidth (Kbps)
- transmit negotiated and actual bandwidth (Kbps) for audio conferences

- receive negotiated and actual bandwidth (Kbps) for audio conferences
- transmit negotiated and actual bandwidth (Kbps) for video conferences
- receive negotiated and actual bandwidth (Kbps) for video conferences
- total network bandwidth and multimedia network bandwidth
- total bandwidth (Kbps) allocated for audio conferences only
- total bandwidth (Kbps) allocated for multimedia conferences
- total bandwidth savings (Kbps), cascaded savings (Kbps), gap savings (Kbps), and thinning (Kbps)

You can view this data by media type or conference type. The performance data displayed depends on whether you select **Media Type**, **Conference Type**, or **Bandwidth Savings** from the Show box at the top of the page.

Procedure

1. In the Conferencing Reports & Monitors window, click the **Locations** tab.
2. On the Locations search page, select the appropriate application server from the Application Server box.
3. Click **SEARCH**.

   By default, the Locations details page displays all of the data for all of the locations on the selected application server.
4. From the Show box, perform one of the following steps:
   - If you want to view the bandwidth data by media type, select **Media type** .
   - If you want to view the bandwidth data by conference type, select **Conference Type** .
   - If you want to view the bandwidth savings by location, select **Bandwidth Savings**.
5. From the drop-down box at the top of each column, select your data display criterion. For more information, see Locations search results page field descriptions on page 65.
6. To view current and/or historical data for a specific location, click on the appropriate location in the Location column.

Related links

Monitoring key performance indicators on page 56
Locations tab on page 64
Locations search criteria page field descriptions on page 65
Locations search results page field descriptions on page 65

Locations tab

The Locations tab enables you to monitor information about the locations provisioned in the Avaya Aura® Conferencing system.

To view the current location information, use the Locations search criteria page. See Locations search criteria page field descriptions on page 65.

See also:

- Locations search results page field descriptions on page 65
- Viewing the data for a location on page 63
- Viewing the current data for a specific location on page 69
- Viewing the historical data for a specific location on page 77

Related links

Viewing the data for a location on page 63

Locations search criteria page field descriptions

Use this page to view search for information about the locations provisioned on the Avaya Aura® Conferencing system.

Name	Description
Application Server	Select the appropriate application server.
SEARCH	Displays the information for the locations that are associated with the application server you specified.

After you click **SEARCH**, the Locations search results page displays the locations that are associated with the application server you specified. See Locations search results page field descriptions on page 65.

See also:

- Locations tab on page 64
- Viewing the data for a location on page 63
- Viewing the current data for a specific location on page 69

Related links

Viewing the data for a location on page 63

Locations search results page field descriptions

Use this page to view:

- the current and historical bandwidth information for each location
- information about sessions related to a location
- the total bandwidth savings, cascaded savings, gap savings, and thinning for each location

The system provides alerts for the following data:

- Total bandwidth usage percentage threshold
- Multimedia bandwidth usage percentage threshold

After you click **SEARCH** on the Locations search criteria page, the Locations search results page displays the locations that are associated with the application server you specified.

You can view the location information by selecting the appropriate option (**Media Type**, **Conference Type**, or **Bandwidth Savings**) from the Show box.

The following information is displayed if you select **Media Type** from the Show box.

Name	Description
Location	Shows the locations associated with the application server. Click the corresponding link to view more information about the location. The list box at the top of this column enables you to filter the displayed data.
Sessions – Audio User/MS	Shows the number of user and media server audio sessions for the location. Media server sessions include cascaded trunk sessions The list box at the top of this column enables you to filter the displayed data.
Sessions – Video User/MS	Shows the number of user and media server video sessions for the location. Media server sessions include cascaded trunk sessions. The list box at the top of this column enables you to filter the displayed data.
Sessions – Wait User/MS	Shows the number of user and media server wait sessions for the location. The list box at the top of this column enables you to filter the displayed data.
Total Neg/Act (Kbps)	Shows the total negotiated bandwidth and actual bandwidth for the location. The list box at the top of this column enables you to filter the displayed data.
Audio Bandwidth – Send Neg. /Actual (Kbps)	Shows the negotiated send bandwidth and actual send bandwidth for audio streams. The list box at the top of this column enables you to filter the displayed data.
Audio Bandwidth – Receive Neg. /Actual (Kbps)	Shows the negotiated receive bandwidth and actual receive bandwidth for audio streams. The list box at the top of this column enables you to filter the displayed data.
Video Bandwidth – Send Neg. /Actual (Kbps)	Shows the negotiated send bandwidth and actual send bandwidth for video streams. The list box at the top of this column enables you to filter the displayed data.
Video Bandwidth – Receive Neg. /Actual (Kbps)	Shows the negotiated receive bandwidth and actual receive bandwidth for video streams. The list box at the top of this column enables you to filter the displayed data.
EXPORT	Saves the displayed data to a .CSV file.

The following information is displayed if you select **Conference Type** from the Show box.

Name	Description
Location	Shows the locations associated with the application server. Click the corresponding link to view more information about the location. The list box at the top of this column enables you to filter the displayed data.
Sessions – Audio User/MS	Shows the number of user and media server audio sessions for the location. Media server sessions include cascaded trunk sessions. The list box at the top of this column enables you to filter the displayed data.
Sessions – Multimedia User/MS	Shows the number of user and media server multimedia sessions for the location. Media server sessions include cascaded trunk sessions. The list box at the top of this column enables you to filter the displayed data.
Sessions – Wait User/MS	Shows the number of user and media server wait sessions for the location. The list box at the top of this column enables you to filter the displayed data.
Bandwidth Audio/MM. (% in use)	Shows the total network bandwidth and multimedia network bandwidth for the location. The list box at the top of this column enables you to filter the displayed data.
Audio Conferences Allocated (Kbps)	Shows the bandwidth allocated for audio sessions only. The list box at the top of this column enables you to filter the displayed data.
Multimedia Conferences Allocated (Kbps)	Shows the bandwidth allocated for multimedia sessions. The list box at the top of this column enables you to filter the displayed data.
EXPORT	Saves the displayed data to a .CSV file.

The following information is displayed if you select **Bandwidth Savings** from the Show box.

Name	Description
Location	Shows the locations associated with the application server. Click the corresponding link to view more information about the location.

Table continues…

Name	Description
	The list box at the top of this column enables you to filter the displayed data.
Total Savings – Send (Kbps)	Shows the total send bandwidth savings for the location. The list box at the top of this column enables you to filter the displayed data.
Total Savings – Receive (Kbps)	Shows the total receive bandwidth savings for the location. The list box at the top of this column enables you to filter the displayed data.
Cascaded Savings – Send (Kbps)	Shows the cascaded send bandwidth savings for the location. The list box at the top of this column enables you to filter the displayed data.
Cascaded Savings – Receive (Kbps)	Shows the cascaded received bandwidth savings for the location. The list box at the top of this column enables you to filter the displayed data.
Gap Savings – Send (Kbps)	Shows the gap send bandwidth savings for the location. The list box at the top of this column enables you to filter the displayed data.
Gap Savings – Receive (Kbps)	Shows the gap receive bandwidth savings for the location. The list box at the top of this column enables you to filter the displayed data.
Thinning – Send (Kbps)	Shows the thinning send bandwidth savings for the location. The list box at the top of this column enables you to filter the displayed data.
Thinning – Receive (Kbps)	Shows the thinning receive bandwidth savings for the location. The list box at the top of this column enables you to filter the displayed data.
EXPORT	Saves the displayed data to a .CSV file.

See also:

- Locations tab on page 64
- Viewing the data for a location on page 63
- Viewing the current data for a specific location on page 69

Related links

Viewing the data for a location on page 63

Viewing the current data for a specific location

About this task

The Conferencing Reports & Monitors application will display the following current performance data for the location you specify:

- audio and multimedia bandwidth usage (percentage) for the network and Avaya Aura® Conferencing
- audio and multimedia bandwidth usage (Kbps) for the network and Avaya Aura® Conferencing
- user requested, connection requested, negotiated, and acquired overall WAN bandwidth
- user requested, connection requested, negotiated, and acquired WAN bandwidth for audio conferences
- user requested, connection requested, negotiated, and acquired WAN bandwidth for video conferences
- requested, negotiated, and acquired overall LAN bandwidth
- requested, negotiated, and acquired LAN bandwidth for audio conferences
- requested, negotiated, and acquired LAN bandwidth for video conferences
- number of user sessions (audio and video)

If you place your mouse over a bar in a graph, details for the associated bar are displayed. This data is constantly updated at the time interval you specify.

Procedure

1. In the Conferencing Reports & Monitors window, click the **Locations** tab.
2. On the Locations search page, select the appropriate application server from the Application Server box.
3. Click **SEARCH**.

   By default, the Locations details page displays all of the data for all of the locations on the selected application server.
4. In the Location column, click on the location in which you are interested.

   The Bandwidth tab is selected and displays the current information for the selected location. For more information, see Location page - Bandwidth tab field descriptions on page 70.
5. From the Update period box, enter the number of seconds at which you want the updated data to be displayed.
6. Click the **Sessions** tab to view information about the current sessions at the selected location. See Location page - Sessions tab field descriptions on page 76.

Related links

Monitoring key performance indicators on page 56
Location page - Bandwidth tab field descriptions on page 70
Location page - Sessions tab field descriptions on page 76

Location page - Bandwidth tab field descriptions

Use this page to view bandwidth usage and bandwidth savings information about the selected location.

Place the mouse over any bar in a chart to view more detailed information.

The system provides alerts for the following data:

- Total network bandwidth usage chart
- Multimedia network bandwidth usage chart

Name	Description
Update period	Enter the number of seconds at which you want updated data to be displayed.
Network bandwidth Usage	Use these charts to determine how much bandwidth is used for this location on Avaya Aura® System Manager and Avaya Aura® Conferencing. These charts can help reveal a problem regarding lack of bandwidth. The **Audio** chart shows the audio bandwidth usage (percentage) for the network and Avaya Aura® Conferencing. The **Multimedia** chart shows the multimedia bandwidth usage (percentage) for the network and Avaya Aura® Conferencing.
Network bandwidth	The **Audio** chart shows the audio bandwidth usage (Kbps) for the network and Avaya Aura® Conferencing. The **Multimedia** chart shows the multimedia bandwidth usage (Kbps) for the network and Avaya Aura® Conferencing.
Overall	Use these charts to view: • the total audio and video WAN bandwidth usage for the location • the total audio and video LAN bandwidth usage for the location • the total WAN bandwidth savings for the location From the drop-down list box, select **WAN Bandwidth Usage** , **LAN Bandwidth Usage**, or **WAN Bandwidth Savings**.

Table continues…

Name	Description
	When **WAN Bandwidth Usage** is selected, the following charts are displayed: • The **Theo** (Theoretical) chart shows the amount of WAN bandwidth that the client would use if there was no CAC or bandwidth management, and the client connected directly to the host location over the WAN. • The **Req** (Requested) chart shows the amount of bandwidth requested from the bandwidth pool that is allocated to a location based on the client's request. • The **Neg** (Negotiated) chart shows the amount of bandwidth that is negotiated with the clients after CAC is applied. Normally, the negotiated bandwidth would be the same as the requested bandwidth. The negotiated bandwidth may be less than the requested bandwidth and depends on the network conditions at that time. • The **Act** (Actual) chart shows the actual amount of bandwidth used by the clients at any moment of time. The actual bandwidth may be less than the negotiated bandwidth in cases where Avaya Aura Conferencing applies advanced bandwidth management techniques (thinning) to lower the bit rate used based on network conditions. When **LAN Bandwidth** is selected, the following charts are displayed: • The **Theo** (Theoretical) chart shows the amount of LAN bandwidth that the client would use if there was no CAC or bandwidth management, and the client connected directly to the host location over the WAN. • The **Req** (Requested) chart shows the amount of bandwidth requested from the bandwidth pool that is allocated to a location based on the client's request. • The **Neg** (Negotiated) chart shows the amount of bandwidth that is negotiated with the clients after CAC is applied. Normally, the negotiated bandwidth would be the same as the requested bandwidth. The negotiated bandwidth may be less than the requested bandwidth and depends on the network conditions at that time. • The **Act** (Actual) chart shows the actual amount of bandwidth used by the clients at any moment of

Table continues…

Name	Description
	time. The actual bandwidth may be less than the negotiated bandwidth in cases where Avaya Aura Conferencing applies advanced bandwidth management techniques (thinning) to lower the bit rate used based on network conditions. When **WAN Bandwidth Usage** is selected, the following charts are displayed: • The **Tot** (Total Savings) chart shows the amount of WAN bandwidth saved due to all forms of bandwidth optimization. This value is the difference between theoretical bandwidth and actual bandwidth. • The **Casc** (Cascading Savings) chart shows the amount of bandwidth saved due to media cascading. This value is the difference between theoretical bandwidth and negotiated bandwidth. • The **Gap** (Gap Savings) chart shows the amount of bandwidth saved over and above the CAC requested bandwidth. This value is the difference between the negotiated bandwidth and actual bandwidth. You can monitor the Gap savings over time to determine whether over-allocation is warranted. • The **Thin** (Thinning) chart shows the amount of bandwidth saved due to thinning, which is an advanced bandwidth management technique. This value is the difference requested bandwidth and negotiated bandwidth.
Video	Use these charts to view: • the WAN bandwidth usage for video sessions • the LAN bandwidth usage for video sessions • the total WAN bandwidth savings for video sessions If there are any problems with video (for example, poor quality), these charts will be useful. When **WAN Bandwidth Usage** is selected, the following charts are displayed: • The **Theo** (Theoretical) chart shows the amount of WAN bandwidth that the client would use for video if there was no CAC or bandwidth management, and the client connected directly to the host location over the WAN.

Table continues…

Name	Description
	• The **Req** (Requested) chart shows the amount of bandwidth requested for video from the bandwidth pool that is allocated to a location based on the client's request. • The **Neg** (Negotiated) chart shows the amount of bandwidth that is negotiated with the clients for video after CAC is applied. Normally, the negotiated bandwidth would be the same as the requested bandwidth. The negotiated bandwidth may be less than the requested bandwidth and depends on the network conditions at that time. • The **Act** (Actual) chart shows the actual amount of bandwidth used by the clients for video at any moment of time. The actual bandwidth may be less than the negotiated bandwidth in cases where Avaya Aura Conferencing applies advanced bandwidth management techniques (thinning) to lower the bit rate used based on network conditions. When **LAN Bandwidth Usage** is selected, the following charts are displayed: • The **Theo** (Theoretical) chart shows the amount of LAN bandwidth that the client would use for video if there was no CAC or bandwidth management, and the client connected directly to the host location over the WAN. • The **Req** (Requested) chart shows the amount of bandwidth requested for video from the bandwidth pool that is allocated to a location based on the client's request. • The **Neg** (Negotiated) chart shows the amount of bandwidth that is negotiated with the clients for video after CAC is applied. Normally, the negotiated bandwidth would be the same as the requested bandwidth. The negotiated bandwidth may be less than the requested bandwidth and depends on the network conditions at that time. • The **Act** (Actual) chart shows the actual amount of bandwidth used by the clients for video at any moment of time. The actual bandwidth may be less than the negotiated bandwidth in cases where Avaya Aura Conferencing applies advanced bandwidth management techniques (thinning) to lower the bit rate used based on network conditions.

Table continues…

Name	Description
	When **WAN Bandwidth Savings** is selected, the following charts are displayed: • The **Tot** (Total Savings) chart shows the amount of WAN bandwidth saved for video sessions due to all forms of bandwidth optimization. This value is the difference between theoretical bandwidth and actual bandwidth. • The **Casc** (Cascading Savings) chart shows the amount of bandwidth saved for video sessions due to media cascading. This value is the difference between theoretical bandwidth and negotiated bandwidth. • The **Gap** (Gap Savings) chart shows the amount of bandwidth saved for video sessions over and above the CAC requested bandwidth. This value is the difference between the negotiated bandwidth and actual bandwidth. You can monitor the Gap savings over time to determine whether over-allocation is warranted.. • The **Thin** (Thinning) chart shows the amount of bandwidth saved for video sessions due to thinning, which is an advanced bandwidth management technique. This value is the difference requested bandwidth and negotiated bandwidth.
Audio	Use these charts to view the bandwidth usage for audio sessions. When **WAN Bandwidth Usage** is selected, the following charts are displayed: • The **Theo** (Theoretical) chart shows the amount of WAN bandwidth that the client would use for audio if there was no CAC or bandwidth management, and the client connected directly to the host location over the WAN. • The **Req** (Requested) chart shows the amount of bandwidth requested for audio from the bandwidth pool that is allocated to a location based on the client's request. • The **Neg** (Negotiated) chart shows the amount of bandwidth that is negotiated with the clients for audio after CAC is applied. Normally, the negotiated bandwidth would be the same as the requested bandwidth. The negotiated bandwidth

Table continues…

Name	Description
	may be less than the requested bandwidth and depends on the network conditions at that time. • The **Act** (Actual) chart shows the actual amount of bandwidth used by the clients for audio at any moment of time. The actual bandwidth may be less than the negotiated bandwidth in cases where Avaya Aura Conferencing applies advanced bandwidth management techniques (thinning) to lower the bit rate used based on network conditions. When **LAN Bandwidth Usage** is selected, the following charts are displayed: • The **Theo** (Theoretical) chart shows the amount of LAN bandwidth that the client would use for audio if there was no CAC or bandwidth management, and the client connected directly to the host location over the WAN. • The **Req** (Requested) chart shows the amount of bandwidth requested for audio from the bandwidth pool that is allocated to a location based on the client's request. • The **Neg** (Negotiated) chart shows the amount of bandwidth that is negotiated with the clients for audio after CAC is applied. Normally, the negotiated bandwidth would be the same as the requested bandwidth. The negotiated bandwidth may be less than the requested bandwidth and depends on the network conditions at that time. • The **Act** (Actual) chart shows the actual amount of bandwidth used by the clients for audio at any moment of time. The actual bandwidth may be less than the negotiated bandwidth in cases where Avaya Aura Conferencing applies advanced bandwidth management techniques (thinning) to lower the bit rate used based on network conditions. When **WAN Bandwidth Savings** is selected, the following charts are displayed: • The **Tot** (Total Savings) chart shows the amount of WAN bandwidth saved for audio sessions due to all forms of bandwidth optimization. This value is the difference between theoretical bandwidth and actual bandwidth. • The **Casc** (Cascading Savings) chart shows the amount of bandwidth saved for audio sessions due to media cascading. This value is the difference

Name	Description
	between theoretical bandwidth and negotiated bandwidth. • The **Gap** (Gap Savings) chart shows the amount of bandwidth saved for audio sessions over and above the CAC requested bandwidth. This value is the difference between the negotiated bandwidth and actual bandwidth. You can monitor the Gap savings over time to determine whether over-allocation is warranted.. • The **Thin** (Thinning) chart shows the amount of bandwidth saved for audio sessions due to thinning, which is an advanced bandwidth management technique. This value is the difference requested bandwidth and negotiated bandwidth.

See also Viewing the current data for a specific location on page 69.

Related links

Viewing the current data for a specific location on page 69

Location page - Sessions tab field descriptions

Use this page to view information about sessions at the selected location.

Place the mouse over any bar in a chart to view more detailed information.

The system provides alerts for the following data:

- Percentage of failed sessions compared to the overall session attempts – overall, audio and video
- Percentage of sessions with R-factor < 70 compared to the number of active sessions – audio
- Percentage of sessions with packet loss compared to the number of active sessions – audio and video

Name	Description
Update period	Enter the number of seconds at which you want updated data to be displayed.
Overall	From the drop-down list box, select **User sessions** or **MS sessions**. The **Active** chart shows the current number of active user/media server sessions (audio and video) and packet loss. The **Last x minutes** chart shows the number of started and failed sessions for the last 15 minutes.

Table continues…

Name	Description
Video	The **Active** chart shows the current number of active video user/media server sessions and packet loss. The **Last x minutes** chart shows the number of successful, failed, dropped, and downgraded video sessions for the last 15 minutes.
Audio	The **Active** chart shows the current number of active audio user/media server sessions. This chart also shows active sessions with an R-factor of less than 70 and packet loss. The **Last x minutes** chart shows the number of started and failed audio sessions for the last 15 minutes.

See also Viewing the current data for a specific location on page 69.

Related links

Viewing the current data for a specific location on page 69

Viewing the historical data for a specific location

About this task

The Conferencing Reports & Monitors application will display the following historical performance data for the location you specify:

- total bandwidth usage
- audio bandwidth usage
- user requested WAN bandwidth at a specific day and time (received and transmitted)
- connection requested WAN bandwidth at a specific day and time (received and transmitted)
- negotiated WAN bandwidth at a specific day and time (received and transmitted)
- acquired WAN bandwidth at a specific day and time (received and transmitted)

If you place your mouse over a bar in a graph, details for the associated bar are displayed. You can view data for the last hour, 24 hours, 7 days, or 30 days.

Procedure

1. In the Conferencing Reports & Monitors window, click the **Locations** tab.
2. On the Locations search page, select the appropriate application server from the Application Server box.
3. Click **SEARCH**.

   By default, the Locations details page displays all of the data for all of the locations on the selected application server.

4. In the Location column, click on the location in which you are interested.
5. Click the **Network bandwidth** tab.
6. From the Showing historical data for box, select the time period in which you are interested. For more information, see Location page - Network bandwidth tab field descriptions on page 78.
7. From the Instance box, select the instance of the application server from which you want to view data. If you have a redundant configuration, be sure to select the active instance.
8. Click the **AAC bandwidth** tab to view historical information about the receive and transmit bandwidth usage for Avaya Aura® Conferencing. For more information, see Location page - AAC bandwidth tab field descriptions on page 79.

Related links

Monitoring key performance indicators on page 56
Location page - Network bandwidth tab field descriptions on page 78
Location page - AAC bandwidth tab field descriptions on page 79

Location page - Network bandwidth tab field descriptions

Use this page to view historical information about bandwidth usage.

The system provides alerts for the following data:

- Total network bandwidth usage chart
- Multimedia network bandwidth usage chart

Name	Description
Showing historical data for	Select the time period for which you want to view historical data. Choices are: • Last Hour • Last 24 Hours • Last 7 Days • Last 30 Days
Instance	Select the instance of the application server from which you want to view data. If you have a redundant configuration (the application server has more than one instance), be sure to select the active instance.
Audio	Shows the audio bandwidth usage (%) for the network and Avaya Aura® Conferencing during the specified time period.
Multimedia	Shows the multimedia bandwidth usage (%) for the network and Avaya Aura® Conferencing during the specified time period.
EXPORT	Saves the displayed historical data to a .CSV file.

See also Viewing the historical data for a specific location on page 77.

Related links

Viewing the historical data for a specific location on page 77

Location page - AAC bandwidth tab field descriptions

Use this page to view the following historical receive and transmit bandwidth information for the time interval you specify:

- peak bandwidth usage
- bandwidth width usage
- total savings
- cascaded savings
- gap savings
- thinning savings

Place the mouse over any bar in a chart to view more detailed information.

Name	Description
Showing	Select the bandwidth statistic you in which you are interested. Choices are: • Peak Bandwidth Usage • Bandwidth Usage • Total Savings • Cascaded Savings • Gap Savings • Thinning
for	Select the time period for which you want to view historical data. Choices are: • Last Hour • Last 24 Hours • Last 7 Days • Last 30 Days
Instance	Select the instance of the application server from which you want to view data. If you have a redundant configuration (the application server has more than one instance), be sure to select the active instance.
Default or **Custom**	**Default** and **Custom** views are used to compare values on the Received and Transmitted charts. **Default** shows a maximum of three bandwidth values in the selected period. These bandwidth values are theoretical, negotiated, and actual.

Table continues…

Name	Description
	Custom lets you select two points that you want to compare. To select these points, move the mouse over the first point you want to select, and click to choose that point and bandwidth type. Then, move the mouse to the second point you want to select, and click to choose that point and bandwidth type. To cancel a selection, click one more time anywhere on the chart.
Received	Shows the received values for theoretical requested bandwidth, connection requested bandwidth, negotiated bandwidth, actual bandwidth, total bandwidth saving, cascading bandwidth savings, and thinning during the specified time period. Total bandwidth saving is the amount of bandwidth saved due to all forms of bandwidth optimization. This value is the difference between theoretical bandwidth and actual bandwidth. Cascading bandwidth savings is the amount of WAN bandwidth saved due to media cascading. This value is the difference between theoretical bandwidth and negotiated bandwidth. Thinning is the amount of bandwidth saved due to thinning, which is an advanced bandwidth management technique. This value is the difference requested bandwidth and negotiated bandwidth.
Transmitted	Shows the transmitted values for theoretical requested bandwidth, connection requested bandwidth, negotiated bandwidth, actual bandwidth, total bandwidth saving, cascading bandwidth savings, and thinning during the specified time period. Total bandwidth saving is the amount of bandwidth saved due to all forms of bandwidth optimization. This value is the difference between theoretical bandwidth and actual bandwidth. Cascading bandwidth savings is the amount of WAN bandwidth saved due to media cascading. This value is the difference between theoretical bandwidth and negotiated bandwidth. Thinning is the amount of bandwidth saved due to thinning, which is an advanced bandwidth management technique. This value is the difference requested bandwidth and negotiated bandwidth.
EXPORT	Saves the displayed historical data to a .CSV file.

See also Viewing the historical data for a specific location on page 77.

Related links

Viewing the historical data for a specific location on page 77

Viewing media server data

Viewing the data for a media server

About this task

The Conferencing Reports & Monitors application will display the following information for the media server(s) you specify:

- long name
- short name
- IP address
- location
- number of hosted conferences
- number of cascaded conferences
- number of recording sessions
- number of user sessions

Procedure

1. In the Conferencing Reports & Monitors window, click the **Media Servers** tab.
2. On the Media Servers search page, select the appropriate application server from the Application Server box.
3. If you want to view media servers at a specific location, select the location from the Location box.
4. Click **SEARCH**.
5. From the drop-down box at the top of each column on the Media Servers details page, select your data display criterion. For more information, see Media Servers search results page field descriptions on page 83.
6. To view current data for a media server, click on the name of the appropriate server in the Long Name column. For more information, see Media Server page - Performance tab field descriptions on page 85.
7. To view current and/or historical data for a location, click on the appropriate location in the Location column. For more information, see Location page - Bandwidth tab field descriptions on page 70.

Related links

Monitoring key performance indicators on page 56
Media Servers tab on page 82
Media Servers search criteria page field descriptions on page 82
Media Servers search results page field descriptions on page 83

Media Servers tab

The Media Servers tab enables you to

- view information about media servers provisioned on the Avaya Aura® Conferencing system.
- access media server-specific monitoring tools.

To view the current information for media servers, use the Media Servers search criteria page. See Media Servers search criteria page field descriptions on page 82.

See also:

- Media Servers search results page field descriptions on page 83
- Media Server page - Performance tab field descriptions on page 85
- Media Server page - Sessions tab field descriptions on page 85
- Viewing the data for a media server on page 81
- Viewing the current data for a specific media server on page 84

Related links

Viewing the data for a media server on page 81

Media Servers search criteria page field descriptions

Use this page to search for information about the media servers provisioned in the Avaya Aura® Conferencing system.

Name	Description
Application Server	Select the appropriate application server.
Location	Enables you to view media servers at a specific location.
SEARCH	Displays the information for the media servers that meet the criteria you specified.

After you click **SEARCH**, the Media Servers search results page displays the media servers that match the criteria you specified. See Media Servers search results page field descriptions on page 83.

See also:

- Media Servers tab on page 82
- Viewing the data for a media server on page 81
- Viewing the current data for a specific media server on page 84

Related links

Viewing the data for a media server on page 81

Media Servers search results page field descriptions

Use this page to:

- view the current information for each media server
- access performance information for a specific media server
- access performance information for a specific location

After you click **SEARCH** on the Media Servers search criteria page, the Media Servers search results page displays the media servers that match the criteria you specified.

Name	Description
Long Name	Shows the long name for the media server administered on Element Manager Console. Click the corresponding link to view more information about the media server. The list box at the top of this column enables you to filter the displayed data.
Short Name	Shows the short name for the media server administered on Element Manager Console. The list box at the top of this column enables you to filter the displayed data.
IP Address	Shows the IP address of the media server. The list box at the top of this column enables you to filter the displayed data.
Location	Shows the location associated with the media server. Click the corresponding link to view more information about the location. The list box at the top of this column enables you to filter the displayed data.
Number of Hosted Conferences	Shows the number of active hosted conferences on the media server. The list box at the top of this column enables you to filter the displayed data.
Number of Cascaded Conferences	Shows the number of active cascaded conferences on the media server. The list box at the top of this column enables you to filter the displayed data.
Number of Recording sessions	Shows the number of active recording sessions on the media server.

Table continues…

Name	Description
	The list box at the top of this column enables you to filter the displayed data.
Number of User sessions	Shows the number of active user sessions on the media server. The list box at the top of this column enables you to filter the displayed data.
EXPORT	Saves the displayed data to a .CSV file.

See also:

- Media Servers tab on page 82
- Viewing the data for a media server on page 81
- Viewing the current data for a specific media server on page 84

Related links

Viewing the data for a media server on page 81

Viewing the current data for a specific media server

About this task

Use this procedure to view the current performance data for a media server.

Procedure

1. In the Conferencing Reports & Monitors window, click the **Media Servers** tab.
2. On the Media Servers search page, select the appropriate application server from the Application Server box.
3. If you want to view media servers at a specific location, select the location from the Location box.
4. Click **SEARCH**.
5. In the Long Name column on the Media Servers details page, click on the media server in which you are interested.
6. To view the current performance information for the media server, click the **Performance** tab. For more information, see Media Server page - Performance tab field descriptions on page 85.
7. To view the current session on the selected media server, click the **Sessions** tab. For more information, see Media Server page - Sessions tab field descriptions on page 85.

Related links

Monitoring key performance indicators on page 56
Media Server page - Performance tab field descriptions on page 85
Media Server page - Sessions tab field descriptions on page 85

Media Server page - Performance tab field descriptions

Use this page to view current performance information for the selected media server.

Place the mouse over any bar in a chart to view more detailed information.

Name	Description
Session Distribution	Shows the number of active sessions, MRCP sessions, IVR sessions, and conference sessions on the media server.
Session Requests	Shows the number of session requests for inbound sessions, inbound sessions rejected, outbound sessions, and outbound session rejected on the media server.
CPU Utilization	Shows the current and historical CPU utilization for the media server.
Dialog Requests	Shows the number of recognition requests, text-to-speech requests, play requests, and record requests on the media server.

See also Viewing the current data for a specific media server on page 84.

Related links

Viewing the current data for a specific media server on page 84

Media Server page - Sessions tab field descriptions

Use this page to view the following information about active sessions on the selected media server:

- remote party
- when the timestamp started
- application name
- endpoint
- QoS R-factor
- QoS round trip delay (msec)
- QoS jitter
- QoS local packet loss
- QoS remote packet loss
- audio codec
- audio Ptime
- video codec
- video frame rate
- remote IP
- remote port

- local IP
- local port
- application URL
- locale
- opaque
- global session ID
- AMS server host name

Note:

The letter “a” or “v” is appended to the information displayed in the Remote IP column, Remote Port column, Local IP column, and Local Port column to indicate that the associated session is an audio call (“a”) or a video call (“v”).

Name	Description
Active Sessions	Displays the number of active sessions on the media server.
IVR Resources	Displays the number of IVR resources in use on the media server.
Conference Resources	Displays the number of conference resources in use on the media server.
MRCP Resources	Displays the number of MRCP resources in use on the media server.
Session Attempts/Interval	Displays the number of sessions attempted on the media server.
CPU Load (%)	Displays the CPU load on the media server.
Viewing Active Sessions area	Enables you to specify the criteria for the sessions you want to view on the media server.
Filter	Select the filter you want to use to view the active sessions. Choices are: • None • Global Session ID • Application • AMS Server Hostname • Remote Party • Endpoint • Remote IP Address • Time Stamp
Criteria	Enter the criteria you want to use with the selected filter.

Table continues…

Name	Description
Session Listed	
Filtered Sessions	
Select	
Refresh	Displays the most current data.
Every	Select the time interval at which you want to view the most current data. Choices are: • 1 Second • 5 Seconds • 10 Seconds • 15 Seconds • 30 Seconds • 45 Seconds • 1 Minute • No Refresh

See also Viewing the current data for a specific media server on page 84.

Related links

Viewing the current data for a specific media server on page 84

Viewing web conferencing server data

Viewing the data for a web conferencing server

About this task

The Conferencing Reports & Monitors application will display the following information for the web conferencing server(s) you specify:

- long name
- short name
- IP address
- number of conferences
- number of sessions

Procedure

1. In the Conferencing Reports & Monitors window, click the **Web Conferencing** tab.

2. On the Web Conference Servers search page, select the appropriate application server from the Application Server box.
3. Click **SEARCH**.
4. From the drop-down box at the top of each column on the Web Conference Servers details page, select your data display criterion. For more information, see Web Conference Servers search results page field descriptions on page 89.
5. To view current data for a web conferencing server, click on the name of the appropriate server in the Long Name column. See Web Conferencing Server page – Performance tab field descriptions on page 91.

Related links

Monitoring key performance indicators on page 56
Web Conferencing tab on page 88
Web Conference Servers search criteria page field descriptions on page 88
Web Conference Servers search results page field descriptions on page 89

Web Conferencing tab

The Web Conferencing tab enables you to view and monitor information about web conferences occurring on the Avaya Aura® Conferencing system.

To view the current web conferencing information, use the Web Conferencing search criteria page. See Web Conference Servers search criteria page field descriptions on page 88.

See also:

- Web Conference Servers search results page field descriptions on page 89
- Web Conferencing Server page – Performance tab field descriptions on page 91
- Viewing the data for a web conferencing server on page 87
- Viewing the current data for a specific web conferencing server on page 90

Related links

Viewing the data for a web conferencing server on page 87

Web Conference Servers search criteria page field descriptions

Use this page to view search for information about the web conferences occurring on the Avaya Aura® Conferencing system.

Name	Description
Application Server	Select the application server for which you want to view information about web conference servers.
SEARCH	Displays the information for the web conference servers that are associated with the application server you specified.

After you click **SEARCH**, the Web Conference Servers search results page displays the web conference servers that are associated with the application server you specified.

See also:

- Web Conference Servers search results page field descriptions on page 89
- Viewing the data for a web conferencing server on page 87
- Viewing the current data for a specific web conferencing server on page 90

Related links

Viewing the data for a web conferencing server on page 87

Web Conference Servers search results page field descriptions

Use this page to view the following information about each web conference server on the Avaya Aura® Conferencing system:

- long name
- short name
- IP address
- number of web conferences currently in progress
- number of web conference sessions currently in progress

The system provides alerts for percentage of failed meetings requests compared to the overall meeting requests attempts.

After you click **SEARCH** on the Web Conference Servers search criteria page, the Web Conference Servers search results page displays the web conference servers that are associated with the application server you specified.

Name	Description
Long Name	Shows the long name administered on Element Manager Console for the associated web conference server. Click the corresponding link to view more information about this web conference server. The list box at the top of this column enables you to filter the displayed data.
Short Name	Shows the short name administered on Element Manager Console for the associated web conference server. The list box at the top of this column enables you to filter the displayed data.
IP Address	Shows the service address (if configured) for the associated web conference server. If the service address is not configured, the server internal OAM address is displayed. The list box at the top of this column enables you to filter the displayed data.

Table continues…

Name	Description
Number of Conferences	Shows the number of web conferences currently running on the associated web conference server. The list box at the top of this column enables you to filter the displayed data.
Number of Sessions	Shows the number of web conference sessions currently running on the associated web conference server. The list box at the top of this column enables you to filter the displayed data.

See also

- Viewing the data for a web conferencing server on page 87
- Viewing the current data for a specific web conferencing server on page 90

Related links

Viewing the data for a web conferencing server on page 87

Viewing the current data for a specific web conferencing server

About this task

Use this procedure to view the current performance data for a web conferencing server.

Procedure

1. In the Conferencing Reports & Monitors window, click the **Web Conferencing** tab.
2. On the Web Conferences Servers page, select the appropriate application server from the Application Server box.
3. Click **SEARCH**.
4. From the drop-down box at the top of each column on the Web Conference Servers details page, select your data display criterion. For more information, see Web Conference Servers search results page field descriptions on page 89.
5. In the Long Name column, click on the web conferencing server in which you are interested.

   The Performance tab displays the number of conference requests that occurred during the last office transfer period. For more information, see Web Conferencing Server page – Performance tab field descriptions on page 91.
6. From the Update period box, enter the number of seconds at which you want the updated data to be displayed.

Related links

Monitoring key performance indicators on page 56

Web Conferencing Server page – Performance tab field descriptions on page 91

Web Conferencing Server page – Performance tab field descriptions

Use this page to view detailed information about the selected web conference server.

Name	Description
Update period	Enter the number of seconds at which you want updated data to be displayed.
Conference Requests	Shows the number of conference requests that occurred during the last office transfer period. The number of conference requests is increased each time a web conference is started. At the end of the office transfer period, the conference requests counter is reset to zero and starts counting again.

See also Viewing the current data for a specific web conferencing server on page 90.

Related links

Viewing the current data for a specific web conferencing server on page 90

Viewing conference data

Viewing the data for conferences

About this task

The Conferencing Reports & Monitors application will display the following information for the conference(s) you specify:

- moderator
- type of conference
- moderator code
- number of participant sessions
- host location
- host media server
- WAN bandwidth usage (send and receive)
- total bandwidth savings (send and receive)
- cascaded bandwidth savings (send and receive) for cascaded conferences
- state
- start time

Procedure

1. In the Conferencing Reports & Monitors window, click the **Conferences** tab.
2. On the Conferences search page, select the appropriate search criteria from the left panel. For more information, see Conferences search criteria page field descriptions on page 92.
3. Click **SEARCH**.
4. From the drop-down box at the top of each column on the Conferences details page, select your data display criterion.
5. To view information about a specific conference, click on the link for the conference in the Moderator column. See Conferences page – Summary tab field descriptions on page 97.

Related links

Monitoring key performance indicators on page 56
Conferences tab on page 92
Conferences search criteria page field descriptions on page 92
Conferences search results page field descriptions on page 94

Conferences tab

The Conferences tab enables you to

- view information about conferences occurring currently on the Avaya Aura® Conferencing system.
- access details for a specific conference.

To view the current information for conferences, use the Conferences search criteria page. See Conferences search criteria page field descriptions on page 92.

See also:

- Conferences search results page field descriptions on page 94
- Conferences page – Summary tab field descriptions on page 97
- Conference page – Audio Video tab field descriptions on page 99
- Conferences page – Web Conferencing tab field descriptions on page 103
- Viewing the data for conferences on page 91
- Viewing the current data for a specific conference on page 96

Related links

Viewing the data for conferences on page 91

Conferences search criteria page field descriptions

Use this page to search for information about conferences on the Avaya Aura® Conferencing system.

Name	Description
Application Server	Select the application server for which you want to view information about conferences.
Conference Type	Enables you to specify the type of conference you want to view. Choices are: • **All** • **MeetMe** • **AdHoc** • **Event** • **Web**
Media Server	Enables you to view information about conferences that use a particular media server.
Web Conference Server	Enables you to view information about conferences that use a particular web conferencing server.
Location	Enables you to view information about conferences that are hosted at a particular location.
Communication Address	Enables you to view information about conferences that use a particular moderator communication address.
Client Display Name	Enables you to view information about conferences that have a specific client display name.
Collaboration Code	Enables you to view information about conferences that use a particular collaboration code.
Conference ID	Enables you to view information about a conference with a particular conference ID.
Session ID	Enables you to view information about a conference with a particular session ID.
Number of Sessions More than	Enables you to view information about conferences that contain more than a specified number of sessions.
Bandwidth Use More than (Mbps)	Enables you to view information about conferences that use more than a specified amount of bandwidth.
SEARCH	Displays the information for the conferences that match the criteria you specified.

After you click **SEARCH**, the Conferences search results page displays the conferences that match the criteria you specified.

See also:

- Conferences search results page field descriptions on page 94
- Viewing the data for conferences on page 91
- Viewing the current data for a specific conference on page 96

Related links

Viewing the data for conferences on page 91

Conferences search results page field descriptions

Use this page to view the following information about conferences on the Avaya Aura® Conferencing system:

- communication address of the moderator
- type of conference
- collaboration code
- number of participant sessions
- host location
- host media server
- WAN bandwidth usage (send/receive)
- total bandwidth savings (send/receive)
- cascading bandwidth savings (send/receive) for cascaded conferences
- state
- start time

The system provides alerts for live monitoring activity events with major and minor severity.

After you click **SEARCH** on the Conference search criteria page, the Conferences search results page displays the conferences that match the criteria you specified.

Name	Description
Moderator	Shows the communication address of the moderator. If there is no moderator in the conference, the message **no moderator joined** appears. Click the corresponding link to view more information about this conference. The list box at the top of this column enables you to filter the displayed data.
Type	Shows the type of conference. The list box at the top of this column enables you to filter the displayed data. Choices are: • All • MeetMe • Adhoc • Event • Web

Table continues…

Name	Description
Collaboration Code	Shows the collaboration code for the conference. The list box at the top of this column enables you to filter the displayed data.
# of Sessions	Shows the number of sessions in the conference. The list box at the top of this column enables you to filter the displayed data.
Host Location	Shows the host location for the conference. Click the corresponding link to view more information about the location. The list box at the top of this column enables you to filter the displayed data.
Host Media Server	Shows the host media server (long name) for the conference. Click the corresponding link to view more information about the host media server. The list box at the top of this column enables you to filter the displayed data.
WAN Bandwidth (Kbps) Send/Receive	Shows the total send/receive WAN bandwidth for the conference. The list box at the top of this column enables you to filter the displayed data.
Total Bandwidth Savings (Kbps) Send/Receive	Shows the total bandwidth savings for the conference. Total bandwidth savings is the difference between the user requested bandwidth and the actual bandwidth used. (The user requested bandwidth is the sum of all the bandwidth requested by each user session in the conference.)
Casc. Bandwidth Savings (Kbps) Send/Receive	Shows the bandwidth savings for a conference that is cascaded. Cascaded bandwidth savings is the difference between the user requested bandwidth and the connection requested bandwidth. Keep in mind the following: • The user requested bandwidth is the sum of all the bandwidth requested by each user session in the conference. • For a cascaded trunk, the user requested bandwidth is the sum of all users' bandwidth at the cascaded location. • For a non-cascaded session, the user requested bandwidth is the user's requested bandwidth. • The connection requested bandwidth is the bandwidth requested from System Manager.

Table continues…

Name	Description
	N/A indicates that the conference is not cascaded. The list box at the top of this column enables you to filter the displayed data.
State	Shows the conference state. The list box at the top of this column enables you to filter the displayed data.
Start Time	Shows the conference start time. The list box at the top of this column enables you to filter the displayed data. Choices are: • All • Less than one hour ago • Less than three hours ago • More than three hours ago
EXPORT	Saves the displayed data to a .CSV file.

See also:

- Viewing the data for conferences on page 91
- Viewing the current data for a specific conference on page 96

Related links

Viewing the data for conferences on page 91

Viewing the current data for a specific conference

About this task

The Conferencing Reports & Monitors application will:

- display detailed information about the conference you specify
- enable you to activate the live monitor, which allows you to view conference events in real time
- display detailed information about sessions associated with the web conferencing server (if web conferencing is used in the conference)

Note:

In this procedure, you will turn on the Live Monitoring feature, which will impact system performance.

Procedure

1. In the Conferencing Reports & Monitors window, click the **Conferences** tab.
2. On the Conferences search page, select the appropriate search criteria from the left panel. For more information, see Conferences search criteria page field descriptions on page 92.

3. Click **SEARCH**.
4. From the drop-down box at the top of each column on the Conferences details page, select your data display criterion.
5. In the Moderator column, click on the link for the conference in which you are interested.

   The Summary tab is selected and displays information about the selected conference. For more information , see Conferences page – Summary tab field descriptions on page 97.
6. From the Update period box, enter the number of seconds at which you want the updated data to be displayed.
7. To turn on Live Monitoring, click **OFF**.
8. From the Turn off live monitor in box, select the number of minutes after which you want to turn off the live monitor.
9. Click the **Audio/Video** tab to view audio and video information for the conference. For more information, see Conference page – Audio Video tab field descriptions on page 99.
10. From the Update period box, enter the number of seconds at which you want the updated data to be displayed.
11. Click the **Web Conferencing** tab to view detailed information about sessions associated with the web conferencing server (if web conferencing is used in the conference). For more information, see Conferences page – Web Conferencing tab field descriptions on page 103.
12. From the Update period box, enter the number of seconds at which you want the updated data to be displayed.

Related links

Monitoring key performance indicators on page 56
Conferences page – Summary tab field descriptions on page 97
Conference page – Audio/Video tab field descriptions on page 99
Media Server cascaded trunk page field descriptions on page 101
Conferences page – Web Conferencing tab field descriptions on page 103

Conferences page – Summary tab field descriptions

Use this page to view detailed information about the selected conference.

From this page, you can activate the live monitor, which enables you to view conference events in real time.

Name	Description
Update period	Enter the number of seconds at which you want updated data to be displayed.
Moderator Communication Address	Shows the communication address of the moderator. If there is no moderator in the conference, the message **no moderator joined** appears.

Table continues…

Name	Description
Moderator Display Name	Shows the display name of the moderator for the conference.
Conference Type	Shows the type of conference.
Moderator Code	Shows the moderator code for the conference.
Participant Code	Shows the participant code for the conference.
Presenter Code	Shows the presenter code for the conference.
Host Location	Shows the host location for the conference. Click the corresponding link to view more information about the location.
Host Media Server	Shows the name of the host media server (long name) for the conference. Click the corresponding link to view more information about the host media server.
Web Host Conference Server	Shows the name of the host web conferencing server (long name) for the conference. Click the corresponding link to view more information about the host web conferencing server.
Number of User Sessions	Shows the number of user sessions in the conference.
Number of Audio/Video Sessions	Shows the number of audio and video sessions in the conference.
Number of Web Conferencing Sessions	Shows the number of web conferencing sessions in the conference.
Conference ID	Shows the unique ID for the conference.
State	Shows the conference state.
Start Time	Shows the conference start time.
Cascaded	Shows whether the conference is cascaded.
Audio Muted	Shows whether the conference audio is muted.
Video Muted	Shows whether the conference video is muted.
Lecture Mode	Shows whether the conference is in lecture mode.
Continuation	Shows whether the Continuation feature is enabled for the conference.
Fast Start	Shows whether the Fast Start feature is enabled for the conference.
Entry/Exit Tone	Shows whether the Entry/Exit Tone feature is enabled for the conference.
Locked	Shows whether the conference is locked.
Recording	Shows whether the conference is being recorded.
Passcode Flow	Shows whether the conference uses passcodes.

Table continues…

Name	Description
Live Monitor	Enables you to enable/disable the live monitor. When the live monitor is enabled, you can see conference event in real time. (For example, you can see when participants join and drop the conference and when the web conference starts and stops.)
EXPORT	Saves the displayed data to a .CSV file.

See also Viewing the current data for a specific conference on page 96.

Related links

Viewing the current data for a specific conference on page 96

Conference page – Audio/Video tab field descriptions

Use this page to view the following information about the selected conference:

- media servers used
- recording
- cascading
- user session communication address of each party in the conference
- R-factor for each party
- packet loss audio/video for each party
- WAN send/receive bandwidth for each party
- location for each party

The system provides alerts for the following data:

- Sessions with R-factor < 70
- Sessions with packet loss

Name	Description
Update period	Enter the number of seconds at which you want updated data to be displayed.
Media Server	Shows information about media servers, recording, and cascading. The host media server appears at the top, the recording server appears next, and all other media servers used for cascading are displayed below. Each media server used by the conference provides the following information: • media server long name • media server host location

Table continues…

Name	Description
	• WAN/LAN bandwidth usage - The **Theo** (Theoretical) chart shows the amount of bandwidth that the client would use if there was no CAC or bandwidth management, and the client connected directly to the host location over the WAN. - The **Req** (Requested) chart shows the amount of bandwidth requested from the bandwidth pool that is allocated to a location based on the client's request. - The **Neg** (Negotiated) chart shows the amount of bandwidth that is negotiated with the clients after CAC is applied. Normally, the negotiated bandwidth would be the same as the requested bandwidth. The negotiated bandwidth may be less than the requested bandwidth and depends on the network conditions at that time. - The **Act** (Actual) chart shows the actual amount of bandwidth used by the clients at any moment of time. The actual bandwidth may be less than the negotiated bandwidth in cases where Avaya Aura Conferencing applies advanced bandwidth management techniques (thinning) to lower the bit rate used based on network conditions. • WAN bandwidth savings - *Total Savings*, which is the amount of bandwidth saved due to all forms of bandwidth optimization. This value is the difference between theoretical bandwidth and actual bandwidth. - *Cascading Savings*, which is the amount of bandwidth saved due to media cascading. This value is the difference between theoretical bandwidth and negotiated bandwidth. - *Gap Savings*, which is the amount of bandwidth saved over and above the CAC requested bandwidth. This value is the difference between the negotiated bandwidth and actual bandwidth. You can monitor the Gap savings over time to determine whether over-allocation is warranted. - *Thinning*, which is the amount of bandwidth saved due to thinning (an advanced bandwidth management technique). This value is the difference requested bandwidth and negotiated bandwidth.

Table continues…

Name	Description
	You can select the bandwidth type (WAN or LAN) you want to view for the host media server. If you want to see more detailed information about bandwidth usage, click **Show Details**. This information indicates how much bandwidth is used by audio or video on this particular media server. Clicking on the **cascaded** link for a cascaded server displays real-time data about the cascaded trunk session between the cascaded and host media servers. For more information, see Media Server cascaded trunk page field descriptions on page 101. Clicking on the **recording** link for a recording media server displays real-time data about the recording trunk session.
Sessions	Shows the following information about sessions associated with the media server: • user session communication address • R-factor • packet loss • bandwidth usage (send/receive) • location to which the user is provisioned This information can help you determine If there are any performance issues with the particular media server.

See also:

- Media Server cascaded trunk page field descriptions on page 101
- Viewing the current data for a specific conference on page 96

.

Related links

Viewing the current data for a specific conference on page 96

Media Server cascaded trunk page field descriptions

Use this page to view live data about the cascaded trunk session between cascaded and host media servers. This page displays the following information for the cascaded trunk session:

- host server
- cascaded server
- host location
- cascaded location

- trunk ID
- moderator
- start time
- session priority
- overall data
- audio data
- video data

The system provides alerts for the following data:

- R-factor < 70 chart
- Jitter chart
- Delay chart
- Packet loss

Name	Description
Update period	Enter the number of seconds at which you want updated data to be displayed.
Host Server	Shows the host media server and provides a link to the media server details.
Cascaded Server	Shows the cascaded media server and provides a link to the media server details.
Host Location	Shows the originating location for the trunk session and provides a link to the location details.
Cascaded Location	Shows the cascaded location for the trunk session and provides a link to the location details.
Trunk ID	Shows the session ID for the cascaded trunk.
Moderator	Shows the communication address of the conference moderator and provides a link to the conference details.
Start Time	Shows the trunk session start time.
Session Priority	Shows the trunk session priority.
Overall data	Shows the requested, negotiated, and actual receive and transmit bandwidth values for audio and video. Also provides R-factor, delay, jitter, and signal-to-noise values.
Audio data	Shows the requested, negotiated, and actual receive and transmit bandwidth values for audio. Also provides audio codec, packet time, speech level, noise level, activity factor, and packet loss values.
Video data	Shows the requested, negotiated, and actual receive and transmit bandwidth values for video. Also

Table continues…

Name	Description
	provides stream status, video codec, frame rate, and resolution values.
EXPORT	Saves the displayed data to a .CSV file.

See also Viewing the current data for a specific conference on page 96.

Related links

Viewing the current data for a specific conference on page 96

Conferences page – Web Conferencing tab field descriptions

Use this page to view the following information about the selected conference:

- web conferencing servers used
- user session communication address/display name
- user role

Name	Description
Update period	Enter the number of seconds at which you want updated data to be displayed.
Web Conferencing Server	Shows information about the host web conferencing server.
Party	Shows the user session communication address/ display name for each party.
User role	Shows the role for each party.

See also Viewing the current data for a specific conference on page 96.

Related links

Viewing the current data for a specific conference on page 96

Viewing session data

Viewing the data for sessions

About this task

The Conferencing Reports & Monitors application will display the following information for the session(s) you specify:

- communication address of the client
- media server

- transmit and receive bandwidth
- audio codec used
- video codec used
- R-factor
- packet loss audio/video
- state
- start time
- web server

Procedure

1. In the Conferencing Reports & Monitors window, click the **Sessions** tab.
2. On the Sessions search page, select the appropriate search criteria from the left panel. For more information, see Sessions search criteria page field descriptions on page 105.
3. Click **SEARCH**.
4. From the drop-down box at the top of each column on the Sessions details page, select your data display criterion.
5. If you want to view information about a specific session, click on the link for the session in the Party column. See Session page – Summary tab field descriptions on page 108.

Related links

Monitoring key performance indicators on page 56
Sessions tab on page 104
Sessions search criteria page field descriptions on page 105
Sessions search results page field descriptions on page 106

Sessions tab

The Sessions tab enables you to

- view information about sessions occurring currently on the Avaya Aura® Conferencing system.
- access details for a specific session.

To view the current information for sessions, use the Sessions search criteria page. See Sessions search criteria page field descriptions on page 105.

See also:

- Sessions search results page field descriptions on page 106
- Session page – Summary tab field descriptions on page 108
- Session page – Performance tab field descriptions on page 109
- Viewing the data for sessions on page 103
- Viewing the current data for a specific session on page 107

Related links

Viewing the data for sessions on page 103

Sessions search criteria page field descriptions

Use this page to search for information about sessions occurring on the Avaya Aura® Conferencing system.

Name	Description
Application Server	Select the application server for which you want to view information about sessions.
Session Type	Select the type of session you want to view. Choices are: • All • Audio • Video • Web
Media Server	Enables you to view information about sessions that use a particular media server.
Web Conference Server	Enables you to view information about sessions that use a particular web conferencing server.
Location	Enables you to view information about sessions that are hosted at a particular location.
Client Communication Address	Enables you to view information about sessions that use a particular user communication address.
Client Display Name	Enables you to view information about sessions that have a particular client display name.
Session ID	Enables you to view information about a session with a particular session ID.
Conference ID	Enables you to view information about a session with a particular conference ID.
R-Factor	Enables you to view information about sessions that have an R-factor value in the range you specify. Choices are: • All • Less than 70 • Less than 90 • Greater than 90
Packet loss more than	Enables you to view information about sessions that have a packet loss value that exceeds the value you specify.
SEARCH	Displays the information for the sessions that match the criteria you specified.

After you click **SEARCH**, the Sessions search results page displays the sessions that match the criteria you specified.

See also:

- Sessions search results page field descriptions on page 106
- Viewing the data for sessions on page 103
- Viewing the current data for a specific session on page 107

Related links

Viewing the data for sessions on page 103

Sessions search results page field descriptions

Use this page to view details for each session that meets the search criteria you specified.

The system provides alerts for live monitoring activity events with major and critical severity.

After you click **SEARCH** on the Sessions search criteria page, the Sessions search results page displays the sessions that match the criteria you specified.

Name	Description
Party	Shows the communication address of the user. Click the corresponding link to view more information about this session. The list box at the top of this column enables you to filter the displayed data.
Media Server	Shows the media server (long name) that processed the session. Click the corresponding link to view more information about the media server. The list box at the top of this column enables you to filter the displayed data.
Web Conference Server	Shows the web conference server that was used by the session. The list box at the top of this column enables you to filter the displayed data.
WAN Bandwidth (kbps) Send/Receive	Shows the total send/receive WAN bandwidth for audio and video for the session. The list box at the top of this column enables you to filter the displayed data.
Audio Codec	Shows the audio codec used by the session. The list box at the top of this column enables you to filter the displayed data.
Video Codec	Shows the video codec used by the session. The list box at the top of this column enables you to filter the displayed data.
R-Factor	Shows the R-factor for the session.

Table continues…

Name	Description
	The list box at the top of this column enables you to filter the displayed data.
Packet Loss Last 60 Sec (%) Audio/Video	Shows the percentage of packet loss for audio and video. The list box at the top of this column enables you to filter the displayed data.
State	Shows the session state. The list box at the top of this column enables you to filter the displayed data.
Start Time	Shows the date and time the session started. The list box at the top of this column enables you to filter the displayed data. Choices are: • All • Less than one hour ago • Less than three hours ago • More than three hours ago
EXPORT	Saves the displayed data to a .CSV file.

See also:

- Viewing the data for sessions on page 103
- Viewing the current data for a specific session on page 107

Related links

Viewing the data for sessions on page 103

Viewing the current data for a specific session

About this task

The Conferencing Reports & Monitors application will:

- display detailed information about the session you specify
- enable you to activate the live monitor, which allows you to view session events in real time
- display detailed information about bandwidth and current state for the session you specify

Note:

In this procedure, you will turn on the Live Monitoring feature, which will impact system performance.

Procedure

1. In the Conferencing Reports & Monitors window, click the **Sessions** tab.

2. On the Sessions search page, select the appropriate search criteria from the left panel. For more information, see Sessions search criteria page field descriptions on page 105.
3. Click **SEARCH**.
4. From the drop-down box at the top of each column on the Sessions details page, select your data display criterion.
5. In the Party column, click on the link for the session in which you are interested.

   The Summary tab is selected and displays information about the selected session. For more information, see Session page – Summary tab field descriptions on page 108.
6. From the Update period box, enter the number of seconds at which you want the updated data to be displayed.
7. To turn on Live Monitoring, click **OFF**.
8. From the Turn off live monitor in box, select the number of minutes after which you want to turn off the live monitor.
9. Click the **Performance** tab to view detailed information about bandwidth and current state for the selected session. For more information, see Session page – Performance tab field descriptions on page 109.
10. From the Update period box, enter the number of seconds at which you want the updated data to be displayed.

Related links

Monitoring key performance indicators on page 56
Session page – Summary tab field descriptions on page 108
Session page – Performance tab field descriptions on page 109

Session page – Summary tab field descriptions

Use this page to view detailed information about the selected session.

From this page, you can activate the live monitor, which enables you to view session events in real time.

Name	Description
Update period	Enter the number of seconds at which you want updated data to be displayed.
Communication Address	Shows the communication address of the user.
Display Name	Shows the display name of the user.
Media Server	Shows the name of the host media server (long name) for the session. Click the corresponding link to view more information about the host media server.
Web Conference Server	Shows the name of the web conferencing server (long name) used by the session. Click the

Table continues…

Name	Description
	corresponding link to view more information about the web conferencing server.
Is Moderator	Shows whether the session is a moderator session.
Moderator	Shows the display name and communication address of the moderator.
Conference Type	Shows the type of conference.
User Location	Shows the location of the user for the session.
MS Location	Shows the location of the media server for the session.
Session ID	Shows the unique ID for the session.
Session State	Shows the session state.
Start Time	Shows the session start time.
Audio Muted	Shows whether the conference audio is muted.
Video Muted	Shows whether the conference video is muted.
On Hold	Shows whether the session is on hold.
Live Monitor	Enables you to enable/disable the live monitor. When the live monitor is enabled, you can see session events in real time.
EXPORT	Saves the displayed data to a .CSV file.

See also Viewing the current data for a specific session on page 107.

Related links

Viewing the current data for a specific session on page 107

Session page – Performance tab field descriptions

Use this page to view detailed information about bandwidth and current session state.

The system provides alerts for the following data:

- R-factor chart
- Packet loss
- Jitter
- Delay

Name	Description
Update period	Enter the number of seconds at which you want updated data to be displayed.
Overall	Shows the requested, negotiated, and actual receive and transmit bandwidth values for audio and video.

Table continues…

Name	Description
	Also provides R-factor, delay, jitter, and signal-to-noise values.
Audio	Shows the requested, negotiated, and actual receive and transmit bandwidth values for audio. Also provides whether the selected party is currently the active speaker in the conference, session audio status, audio codec, packet time, speech level, noise level, activity factor, and packet loss.
Video	Shows the requested, negotiated, and actual receive and transmit bandwidth values for video. Also provides video stream status, video codec, frame rate, resolution, and packet loss.
EXPORT	Saves the displayed data to a .CSV file.

See also Viewing the current data for a specific session on page 107.

Related links

Viewing the current data for a specific session on page 107

Generating a report for a server

About this task

Use this procedure to generate a report for the following types of servers:

- media server
- accounting manager
- application server
- element manager
- provisioning manager
- CA server
- database

Procedure

1. In the Conferencing Reports & Monitors window, click the **Report Builder** tab.
2. On the Report criteria page, select the appropriate criteria from the left panel. For more information, see Report criteria page field descriptions on page 111
3. Click **SHOW REPORT**.

Related links

Monitoring key performance indicators on page 56
Report Builder tab on page 111
Report criteria page field descriptions on page 111

Operational Measurements (OM) Groups field descriptions on page 112
Report results page field descriptions on page 115
Examples of Avaya Aura Conferencing reports on page 115

Report Builder tab

The Report Builder tab enables you to generate custom reports using almost any operational measurement (OM) supported on the Avaya Aura® Conferencing system. You can create up to five charts at one time, which is helpful when comparing OMs in a specific group over the same time period.

To view the generate a report, use the Report criteria page. See Report criteria page field descriptions on page 111.

See also:

- Report results page field descriptions on page 115
- Generating a report for a server on page 110

Related links

Generating a report for a server on page 110

Report criteria page field descriptions

Use this page to specify the criteria for the historical data you want to view.

Name	Description
Report history from	Select the network element for which you want to view historical data.
Instance	Select the appropriate instance for the selected network element.
Show data from	Select the time period in which you are interested. Choices are: • Last Hour • Last 24 Hours • Last 7 Days • Last 30 Days
OM group to show	Select the OM group for which you want to view historical data.
OM registers	Select the OM registers you want to view.

Table continues…

Name	Description
	Note: You can select up to five OM registers and one OM row key, or you can select one OM register and up to five OM row keys.
OM row keys	Select the OM rows you want to view.
SHOW REPORT	Displays the data that meets the criteria you specified.

After you click **SHOW REPORT**, the Report results page displays the data that matches the criteria you specified.

Related links

Generating a report for a server on page 110

Operational Measurements (OM) Groups field descriptions

OM Group to Show	Description
CPCheckpoint	Tracks the number of calls that the inactive application server is checkpointing. If a failover occurs, these calls survive the failover.
Ccmp	Tracks CCMP requests.
ConfByDuration	Lists total conference duration, including the total time and the time used by each conference type.
ConfBySize	Lists total participants number, including the total number of participants and the participants by conference type.
ConfClassAndQuality	Lists information regarding the quality of the conference/session. For example, it shows information about packet loss.
ConfLocBandwidth	Lists information regarding the bandwidth usage of the conference/session, including statistics for audio and video, for a specific location.
ConfLocBandwidthSavings	Lists information regarding the bandwidth savings for the conference/session, for example, the savings provided by cascading servers, for a specific location.
ConfLocSessionTypes	Lists information regarding the various types of sessions, such as the number of video, audio, and web collaboration sessions, for a specific location.

Table continues…

OM Group to Show	Description
ConfLocSessions	Lists information regarding the quality of the media server sessions during the conference for a specific location.
ConfSession	Lists general information about the conferences/ sessions, such as, whether there were unsuccessful connections, and so on.
ConfSessionByServers	Lists the number of conferences/sessions on the server, including the total number of conferences and the numbers of each type of conference for each media server.
ConfSessionByWcs	Lists the number of conferences/sessions that used web-sharing on each Web Collaboration Server (WCS).
ConfSessionTypes	Provides information about the numbers of successful audio, video, and web collaboration conferences/sessions that were part of the call.
ConfSessionUA	Provides information about the numbers of successful audio, video, and web collaboration conferences/sessions that were part of the call. Similar to <ConfSessionTypes> but provides an information regarding User Agents (phone types).
ConfTotalBandwidth	Provides information about the bandwidth used, including the bandwidth requested and the bandwidth actually received.
ConfTotalBandwidthSavings	Provides information about the bandwidth savings, for example, the savings provided by cascading servers.
ConfTypeLocBandwidth	Provides information about the bandwidth used, including the total audio network bandwidth usage and the multimedia network bandwidth usage for a particular location.
Conference	Provides general information about conferences, such as how many conferences were cascaded, recorded and so on.
DBFramework	Provides performance data regarding the use of cached database resources. These measurements provide valuable raw data that you can use to engineer the cache sizes for various system configurations.
DBPerformance	Provides performance data regarding the amount of (elapsed) time required to perform database queries and updates. Timestamps are taken immediately before and after each database operation.

Table continues…

OM Group to Show	Description
DNSPJM	The Domain Name Server Persistence Job Manager (DNSPJM) OM group measures the performance of the DNS Persistence Job Manager. The DNSPJM is a software subsystem that performs DNS lookups on behalf of call-processing tasks.
IOChannel	Provides data regarding the use of input and output channels.
JvmGarbageCollection	Collects statistics for Java Virtual Machine (JVM) garbage collection.
JvmMemory	Collects statistics for JVM memory usage.
JvmThreads	Collects statistics for JVM thread usage.
MsgVal	Captures counters for the Message Validator service.
PJM	Measures the performance of the Persistence Job Manager. The PJM is a software subsystem that performs database queries on behalf of call-processing tasks.
Publish	Provides counters for the use of the PUBLISH service.
RecordStreamSender	Monitors the performance of standard record streams for each network element instance. Each particular stream and particular system (log, om, and accounting) contains a particular OM row.
RecordingSystem	Contains operational measurements related to the recording system that writes operational measurement records into files. In this release, the recording system contains only one register: closedFileCount.
SIPSecurity	Provides data regarding the enforcement of SIPS.
Session	Tracks counters for IP Telephony transactions that the application server processes.
SipDelay	Provides information about processing time for SIP transactions on a network element.
SipIncomingResponses	Provides a count of the number of specific SIP responses received.
SipOutgoingResponses	Provides a count of the number of specific SIP responses sent.
SipStack	Tracks resources in the SIP stack per application server.
SipTcp	Tracks the events related to Transmission Control Protocol (TCP) connections. This group collects

Table continues…

OM Group to Show	Description
	statistics of TCP connections, specifically in terms of the usage, persistency, and reuse.
SipTls	Tracks the events related to Transport Layer Security (TLS) connections. This group collects statistics of TLS connections, specifically in terms of the usage, persistency, and reuse.
SipTransactions	Provides information about incoming or outgoing SIP transactions.
SyncSystem	Tracks the processing of synchronization checkpoints between two synchronization peers. One peer is the checkpoint sender containing information to be checkpointed.

Related links

Generating a report for a server on page 110

Report results page field descriptions

Use this page to view the historical data that matches the criteria you specified on the Report criteria page.

Place the mouse over any section in a chart to view more detailed information.

Click **EXPORT** to save the displayed data to a .CSV file.

Related links

Generating a report for a server on page 110

Examples of Avaya Aura® Conferencing reports

Avaya Aura® Conferencing is capable of producing a wide range of reports, based on the key performance indicators. Here are some examples.

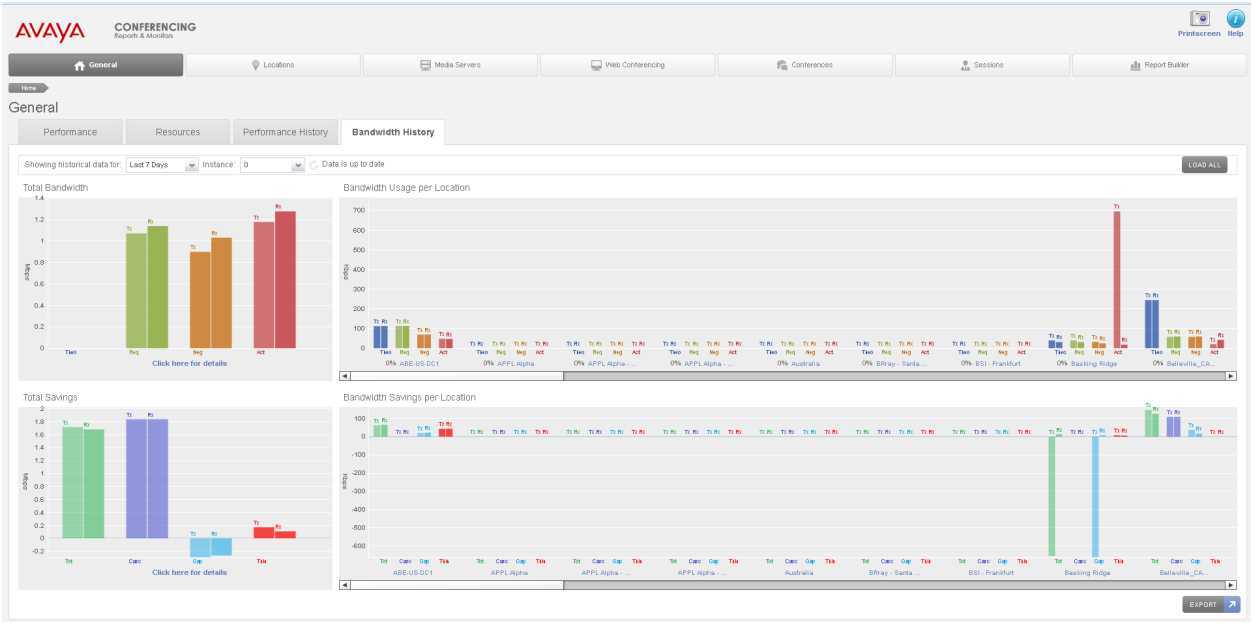


Figure 3: Historical bandwidth usage and bandwidth savings

Figure 4: Peak bandwidth usage by location

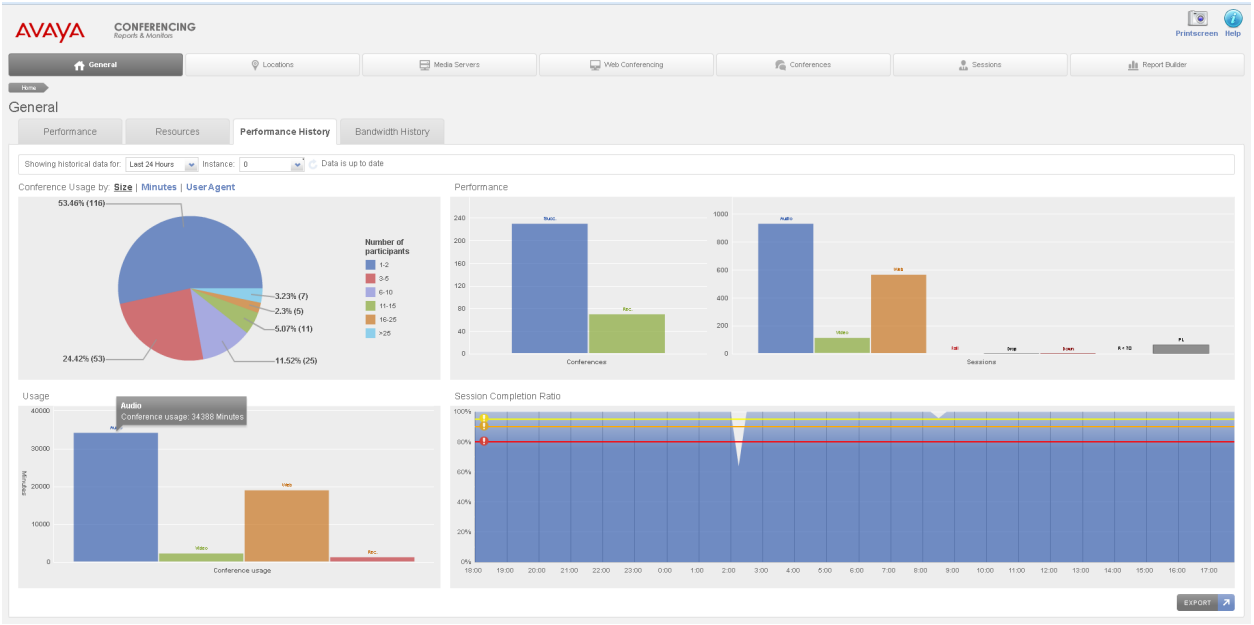


Figure 5: Historical data (Number of conferences, sessions (Audio, Video, Web), Minutes

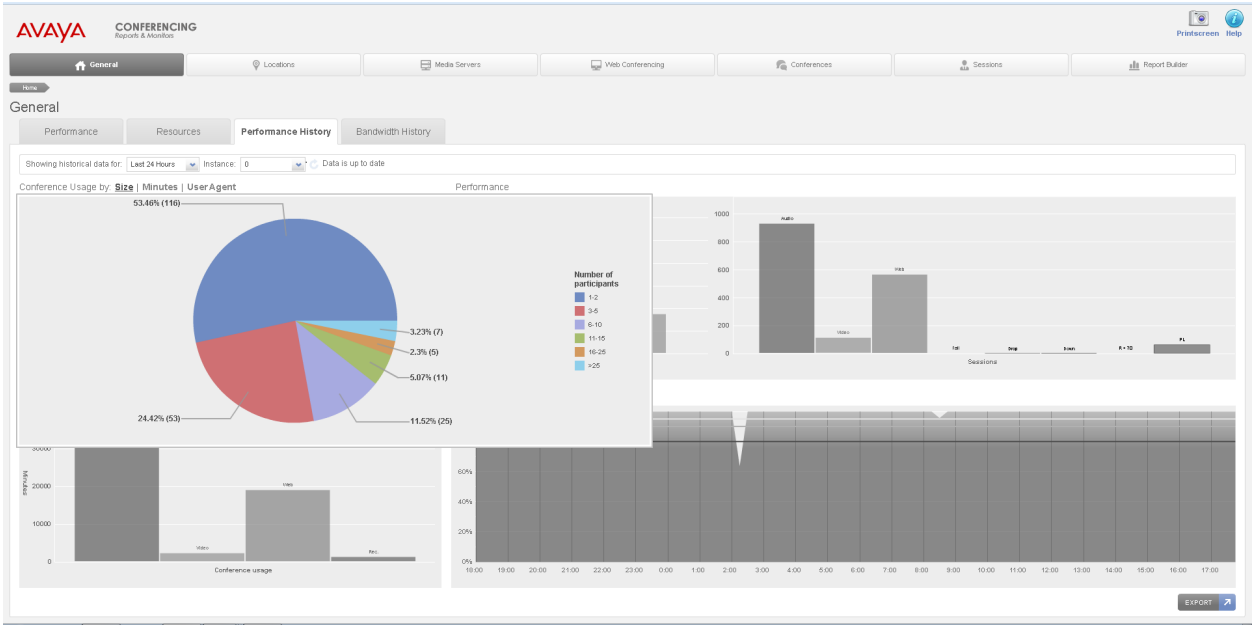


Figure 6: Conference usage breakdown by size (Number of participants)

Related links

[Generating a report for a server](#) on page 110

Chapter 8: Managing server and database monitors

Use the procedures in this chapter to:

- view information about the monitor for a server
- start and stop the monitor for a server
- configure the threshold settings of the monitor for a server
- generate an analysis of all servers
- view information about the monitor for a database instance
- start and stop the monitor for a database instance

Managing server monitors

Viewing the monitor service for a server

About this task

Use this procedure to view the monitor service for a server.

The monitor service reports the following critical resource information about the server:

- CPU usage
- physical memory usage
- network I/O usage
- file system disk usage

Procedure

1. In the navigation pane of Element Manager Console, click **Servers > <*Server name*> > Monitor**.
2. In the Server Monitor window, look at the bottom of the window to verify that the server monitor is not running.

3. If the server monitor is not running, click **Start Monitor** in the Server Monitor window.

   The following message appears at the bottom of the window: “The server monitor is running.”

4. Click the appropriate tab to view the monitor information.

Related links

Managing server and database monitors on page 118

Starting the monitor service for a server

About this task

Use this procedure to start the monitor service for a server.

The monitor service reports the following critical resource information about the server:

- CPU usage
- physical memory usage
- network I/O usage
- file system disk usage

Procedure

1. In the navigation pane of Element Manager Console, click **Servers > <*Server name*> > Monitor**.
2. In the Server Monitor window, look at the bottom of the window to verify that the server monitor is not running.
3. In the Server Monitor window, click **Start Monitor**.

   The following message appears at the bottom of the window: “The server monitor is running.”

Related links

Managing server and database monitors on page 118
Viewing alarms from the Logical View window of Element Manager Console on page 45
Viewing alarms from the navigation pane of Element Manager Console on page 44
Viewing alarms from the Physical View window of Element Manager Console on page 46
Viewing logs from the Logical View window of Element Manager Console on page 50
Viewing logs from the navigation pane of Element Manager Console on page 49
Viewing logs from the Physical View window of Element Manager Console on page 50

Stopping the monitor service for a server

About this task

Use this procedure to stop the monitor service for a server.

Procedure

1. In the navigation pane of Element Manager Console, click **Servers > <*Server name*> > Monitor**.
2. In the Server Monitor window, look at the bottom of the window to verify that the server monitor is running.
3. In the Server Monitor window, click **Stop Monitor**.

   The following message appears at the bottom of the window: “The server monitor is not running.”

Related links

Managing server and database monitors on page 118

Configuring alarm thresholds for a server

About this task

Use this procedure to configure alarm thresholds for a server.

Procedure

1. In the navigation pane of Element Manager Console, click **Servers > <*Server name*> > Monitor**.
2. In the Server Monitor window, click **Configure Thresholds**.
3. In the Server Monitor Alarm Thresholds dialog box, select or clear the **Minor**, **Major**, and **Critical** check boxes for the CPU, RAM, Disk, and Interface sections as required.
4. Modify the threshold values for the CPU, RAM, Disk, and Interface sections as required.
5. When finished, click **OK**.

Related links

Managing server and database monitors on page 118

Generating an analysis of all servers

About this task

Use this procedure to generate an analysis of all servers.

You can save the server analysis information to a file.

Procedure

1. From the Tools menu, select **Server Analysis**.

2. In the Server Analysis window, click the tab of the server in which you are interested.
3. If you want to save the information for all of the servers to a file:
   a. From the File menu in the Server Analysis window, select **Save Server Analysis**.
   b. In the Save Server Analysis dialog box, specify the location and name of the file to which you want to save the server analysis data.
   c. Click **Save**.
4. When finished, click the **X** button to close the Server Analysis window.

Related links

Managing server and database monitors on page 118

Managing the database monitor

Viewing the monitor service for the database

About this task

Use this procedure to view the monitor service for the database.

The monitor service reports the data replication status for the mcpdb database.

Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Database > mcpdb > Monitor**.
2. In the mcpdb Monitor window, select the database instance in which you are interested.
3. Click **Monitor**.
4. In the mcpdb Database Instance Monitor window, look at the bottom of the window to verify that the database monitor is not running.
5. If the database monitor is not running, click **Start Monitor** in the mcpdb Database Instance Monitor window.

   The following message appears at the bottom of the window: “The database instance monitor is running.”
6. Click the appropriate tab to view the monitor information.

Related links

Managing server and database monitors on page 118

Starting the monitor service for the database

About this task

Use this procedure to start the monitor service for the database.

The monitor service reports the data replication status for the mcpdb database.

Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Database > mcpdb > Monitor**.
2. In the mcpdb Monitor window, select the database instance for which you want to start the monitor service.
3. Click **Monitor**.
4. In the mcpdb Database Instance Monitor window, look at the bottom of the window to verify that the database monitor is not running.
5. In the mcpdb Database Instance Monitor window, click **Start Monitor**.

   The following message appears at the bottom of the window: “The database instance monitor is running.”

Related links

Managing server and database monitors on page 118

Stopping the monitor service for the database

About this task

Use this procedure to stop the monitor service for the database.

Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Database > mcpdb > Monitor**.
2. In the mcpdb Monitor window, select the database instance for which you want to stop the monitor service.
3. Click **Monitor**.
4. In the mcpdb Database Instance Monitor window, look at the bottom of the window to verify that the database monitor is running.
5. In the mcpdb Database Instance Monitor window, click **Stop Monitor**.

   The following message appears at the bottom of the window: “The database instance monitor is not running.”

Related links

Managing server and database monitors on page 118

Chapter 9: Troubleshooting user problems

Use the tasks in this chapter to identify and correct problems users encounter with Avaya Aura® Conferencing.

Related links

Connection issues on page 124
Collaboration issues on page 125
Recording issues on page 129
Playback issues on page 132

Connection issues

Connection issues relate to any problems that users experience when trying to dial the Avaya Aura® Conferencing server.

Related links

Troubleshooting user problems on page 124
Receive a fast busy when calling into the bridge on page 124
Unable to hear audio on a SIP call on page 125

Receive a fast busy when calling into the bridge

Related links

Connection issues on page 124
Proposed solution on page 124

Proposed solution

Procedure

1. Check the SIP trunk configuration on Avaya Session Manager.
2. Turn on traces on Avaya Session Manager to ensure SIP headers on INVITE address From/To fields verify calling IP is Avaya Aura® Conferencing.
3. Using Provisioning Client, verify that the media server resources are allocated to a media server cluster.

4. Run traces on Avaya Session Manager to determine dial-in DDI or DNIS matches with the service URI.
5. Make sure the service URIs are provisioned on Avaya Aura® Conferencing.

Related links

Receive a fast busy when calling into the bridge on page 124

Unable to hear audio on a SIP call

Related links

Connection issues on page 124
Proposed solution on page 125

Proposed solution

Procedure

1. Check the RTP ports on SIP SDP parameters and ensure the firewall is not blocking it.
2. Verify media servers are operational and in service on Avaya Aura® Conferencing.
3. Check the location on which media servers turn on traces on Avaya Session Manager to make sure SIP headers on INVITE address From/To fields verify calling IP is Avaya Aura® Conferencing.

Related links

Unable to hear audio on a SIP call on page 125

Collaboration issues

Collaboration issues relate to any problems that users experience when using the features of Collaboration Agent.

Related links

Troubleshooting user problems on page 124
Unable to start web collaboration from Collaboration Agent on page 125
Unable to upload files to the Library on page 126
Font issues on page 126

Unable to start web collaboration from Collaboration Agent

Related links

Collaboration issues on page 125
Proposed solution on page 126

Proposed solution

Procedure

1. Verify FQDN entries on Element Manager Console for Web Conferencing server under hostname field.
2. Make sure local host files have FQDN entries for Element Manager server and Web Conferencing server and it is resolvable on the network.
3. Add DNS records to the DNS servers permanently.
4. Check the firewall ports.
5. Try HTTP access and eliminate certificate issues.

Related links

Unable to start web collaboration from Collaboration Agent on page 125

Unable to upload files to the Library

If the write master Web Conferencing Management server (WCMS) is “down,” users will be unable to upload files to their Library. If the write master WCMS is down, you must manually change the “library write master” role to another WCMS using Element Manager Console. In a similar way, if the Document Conversion Server (DCS) is “down”, users will be unable to upload files to their Library.

Related links

Collaboration issues on page 125
Proposed solution on page 126

Proposed solution

Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Web Conferencing > Web Conferencing Servers and Clusters > Collaboration Library**.
2. From the Write Master box in the Collaboration Library dialog box, select the active WCMS.
3. Click **Apply**.
4. Restart all Web Conferencing Servers that are associated with the WCMS.

Related links

Unable to upload files to the Library on page 126

Font issues

For sharing presentations and documents, Avaya Aura® Conferencing supports most of the commonly-used fonts. If a document or presentation uses an unusual or lesser-known font, the format may not be preserved. Avaya Aura® Conferencing supports the following fonts:

Arial Bold
Arial Bold Italic
Arial Italic
Arial Arial Narrow WGL Bold Italic
Arial Narrow WGL Bold
Arial Narrow WGL Italic
Arial Narrow WGL
BookAntiqua-BoldItalic
BookAntiqua-Bold
BookAntiqua-Italic
BookAntiqua
Bookman Old Style
Bookman Old Style Bold
Bookman Old Style Bold Italic
Bookman Old Style Italic
Comic Sans
Corsiva
Courier New Bold
Courier New Bold Italic
Courier New Italic
Courier New
CSongGB18030C-Light
FBBlueMingL
Georgia
Georgia Bold
Georgia Italic
Georgia Bold Italic
Century Gothic
Century Gothic Bold
Century Gothic Bold Italic
Century Gothic Italic
Impact
MSung HK Light

MotoyaExMincho W3 KP
Century Schoolbook
Century Schoolbook Bold
Century Schoolbook Bold Italic
Century Schoolbook Italic
Sorts
Symbol
Tahoma Bold Italic
Tahoma Italic
Tahoma Bold
Tahoma
Times New Roman Bold
Times New Roman Bold Italic
Times New Roman Italic
Times New Roman
Trebuchet
Trebuchet-Bold
Trebuchet-BoldItalic
Trebuchet-Italic
Verdana Bold
Verdana Italic
Verdana Bold Italic
Verdana
Webdings
Wingdings
Wingdings 2
Wingdings 3

Note:

Avaya Aura® Conferencing matches any unsupported fonts with one of the fonts from this list.

Related links

Collaboration issues on page 125
Proposed solution on page 129

Proposed solution

Procedure

Ensure that any shared files use a supported font. It is a good idea to preview files before sharing them in a meeting.

Related links

Font issues on page 126

Recording issues

Recording issues relate to any problems that users experience when using the recording feature of Avaya Aura® Conferencing.

Related links

Troubleshooting user problems on page 124
The stages of recording on page 129
Recording checklist on page 130

The stages of recording

When attempting to troubleshoot problems with the recording feature, the first step is to identify the stage of the recording process which is causing the issue. Typically, there are two types of errors.

- Errors related to starting the recording
- Errors related to encoding the recording

Users can start recording by way of the Collaboration Agent GUI or the `*21` command on the telephone user interface (TUI). If there is an issue related to starting the recording, the user hears the audio message: **Conference recording is not available**.

When the recording ends, Avaya Aura® Conferencing schedules it for encoding by the encoding server, which resides on the WCS. The recording shows as **Processing** at this time and **Ready** when ready to be played. If there is an error related to encoding the recording, the recording shows a status of **Error** in the recording management screen of the Collaboration Agent.

It is possible to divide the recording process into a number of smaller stages. For your information, these stages are described here.

Stage	Description
1	The application server receives the start recording command from the user, by way of the Collaboration Agent GUI or the `*21` command on the telephone user interface (TUI).
2	The application server initiates audio recording.

Table continues…

Stage	Description
3	The application server sends a start recording message to the Web Conferencing Management Server (WCMS).
4	The WCMS stores the data for the entire recording in the database and instructs the WCS to start web recording.
5	The application server intermittently sends recording events to the WCMS.
6	The application server receives the stop recording command from the user, by way of the Collaboration Agent GUI or the `*21` command on the telephone user interface (TUI). Alternatively, the application server receives the stop recording command automatically when the conference ends (or the media server ends the recording due to the maximum recording length being exceeded.)
7	The application server stops audio recording.
8	The application server sends a stop recording messages to the WCMS.
9	The WCMS stops web recording and marks the recording file as ready for processing.
10	The WCMS queues the recording for encoding. The encoding service on the WCS processes the recording file by converting it from a raw recording to an Adobe Flash recording.
11	The user plays the recording.

Related links

Recording issues on page 129

Recording checklist

If you can identify the point at which the fault occurred, there are a number of investigative and corrective actions which you can take to fix the problem.

When the recording functionality is not available, the audio message **Conference Recording is not available at this time** is played when you press the `*21` keypad command. In this situation, generally, the first step of troubleshooting is to check user permissions, system permissions, and licenses for recording. Also, you should check the Avaya Media Server (AMS) to ensure that the server is not currently offline.

The second step of troubleshooting is to check the alarms, as described in *Avaya Aura® Conferencing Alarms and Logs Reference*, which is available on support.avaya.com.

#	Issue	Avaya recommendation	Reference
1	Is recording enabled for the user?	Avaya Aura® Conferencing administrators can enable the recording feature for certain users and disable it for other users.	On the Avaya Provisioning Client, navigate to **User Management**. Search for the user and on the **Actions** tab, click **Conferencing**. Ensure that the **Enable Recording** checkbox is selected.

Table continues…

#	Issue	Avaya recommendation	Reference
			These steps are described in more detail in *Administering Avaya Aura® Conferencing*, which is available on support.avaya.com
2	Is recording enabled on the system?	Avaya Aura® Conferencing administrators can enable or disable the recording feature for the entire system.	On the Avaya Provisioning Client, navigate to **System Management**. In **System Default Settings**, ensure that the **Allow Recording** checkbox is selected. These steps are described in more detail in *Administering Avaya Aura® Conferencing*, which is available on support.avaya.com
3	If yours is a co-resident deployment, have you correctly configured a media server cluster?	Avaya Aura® Conferencing administrators must assign the **Conferencing and Recording Role** to a media server cluster in a co-resident deployment.	You can configure this setting using the Element Manager Console. You must navigate to **Feature Server Elements** > **Media Servers and Clusters** > **Media Server Clusters**. Click **Edit** and in the **Edit Media Server Cluster** dialog box, select **CONFERENCING AND RECORDING**. These steps are described in more detail in *Deploying Avaya Aura® Conferencing*, which is available on support.avaya.com
4	If yours is a dedicated recording server deployment, is there a media server cluster that is dedicated to recording?	Avaya Aura® Conferencing administrators must assign a media server that will be dedicated for recording.	You can check this assignation in the navigation pane of Element Manager Console by selecting **Feature Server Elements** > **Media Servers and Clusters** > **Media Server Clusters**. Specifically, you must ensure that the **Role** field has the following value: **RECORDING ONLY**.
5	Is there a recording media server assigned to service the user's location?	Avaya Aura® Conferencing administrators must assign a recording media server to service the user's location.	On the Avaya Provisioning Client, navigate to **System Management**. In **Routing** > **Media Server Resources**, ensure that the **Media Server Cluster for Recording** is correctly assigned. These steps are described in more detail in *Deploying Avaya Aura® Conferencing*, which is available on support.avaya.com
6	Are the correct licenses in place?	Avaya Aura® Conferencing requires a license key on Avaya Aura® System Manager.	Licenses are managed on a WebLM server. The installation steps for these licenses are described in more detail in *Deploying Avaya Aura® Conferencing*, which is available on support.avaya.com

Table continues…

#	Issue	Avaya recommendation	Reference
7	Is the recording media server currently offline?	There are a number of possible issues related to the AMS. To address some of these issues, Avaya Aura® Conferencing administrators may require assistance from their Avaya Support Representative. For example, the recording media server may have reached full capacity, there may be a SIP communication issue between the application server and the recording media server, or there may be no available bandwidth from Avaya Aura® Session Manager .	Restart the recording media server by restarting the Avaya Media Server (AMS). If the issue persists, prepare to contact an Avaya Support Representative.
8	Is the system producing any alarms?	The recording feature on Avaya Aura® Conferencing produces a number of alarms that indicate issues with the recording feature.	For more information, see *Avaya Aura® Conferencing Alarms and Logs Reference*, which is available on support.avaya.com
9	Is the system outputting any logs?	The recording feature on Avaya Aura® Conferencing produces a number of logs that indicate issues with the recording feature.	You can view these logs on the Element Manager Console. Specifically, the application server logs are most relevant for issues starting recording. The WCS log has the most relevant information for issues encoding the recording. For more information, see Viewing logs from the Logical View window on page 50.
10	Can you play the recording file?	If the file has been successfully created, but you cannot play the file, there may be an issue with the playback process.	Introducing playback on page 133

Related links

Recording issues on page 129

Playback issues

Playback issues relate to any problems that users experience when playing conference recordings.

Related links

Troubleshooting user problems on page 124
Introducing playback on page 133
Common issues on page 133

Introducing playback

When issues occur with the playback of recorded files, Avaya recommends looking at the error on the playback GUI.

The playback application is located here: `MCP_xx/WCSxx/apache/www/playback/`

Related links

Playback issues on page 132

Common issues

Related links

Playback issues on page 132
Cannot load localization files on page 133
Locale not recognized on page 133
General issue on page 134

Cannot load localization files

If the Player is unable to load the localization .swf files, the initialization of the application will stop.

Related links

Common issues on page 133

Proposed solution

Procedure

Check if the files are present in the following directory: `../playback/assets/bundles/`.

The following files should be present: en_US, de_DE, es_ES, fr_FR, it_IT, ja_JP, ko_KR, pt_BR, ru_RU, zh_CN, en_CA, en_GB, fr_CA, and es_MX.

Locale not recognized

This issue occurs if the default language files are always loaded even when the user's computer has a non-English locale. The default language files are the US English files, en_US.

Related links

Common issues on page 133

Proposed solution

Procedure

Check if the files are present in the following directory: `../playback/assets/bundles/`.

General issue

There are a number of general issues which may occur. For example, the following message may be displayed: **Unexpected error occurred. [error stack trace in details section]**. This issue occurs when the application logic generates an error. If this issue occurs, open the details section and save the message. Contact the vendor and attach the error logs.

Related links

Common issues on page 133

Chapter 10: Troubleshooting the system

This chapter provides a task for general troubleshooting and tasks to troubleshoot configuration errors and patching problems.

General troubleshooting

About this task

Use this task to determine the cause of a fault within the system — that is, whether the fault is caused by a software error or by a hardware, installation, configuration, administration, or security problem.

Prerequisites

- You are familiar with the procedures to monitor alarms using the Element Manager Console. For more information, see Monitoring alarms on page 44 and Viewing logs from the navigation pane of Element Manager Console on page 49.
- You are familiar with the procedure to detect hardware faults. For more information, see Troubleshooting hardware faults on page 143.

Procedure

1. Determine whether the fault is a software error by monitoring the Element Manager Console alarms.
2. Determine whether the fault is a hardware problem by monitoring the server LEDs.
3. Determine whether the fault is an installation problem.
4. Determine whether the fault is a configuration problem. See *Deploying Avaya Aura® Conferencing* for valid system installation, configuration, and administration.
5. Determine whether the fault is an administration problem.
6. Determine whether the fault is a security problem. See *Avaya Aura® Conferencing Security Guide*.

Element Manager Console problems

This section addresses various error conditions you may encounter while using Element Manager Console.

Element Manager Console does not start

You are unable to access the Element Manager Console window.

Proposed solution

Procedure

1. Check the browser settings (for example, pop-up window blocker and trusted site).
2. Confirm that Element Manager Console is not already running.
3. Confirm TCP ports 443 and 12121 are open.
4. Confirm that you are using the IP address of Element Manager Console and **not** the IP address of the Element Manager server.

Cannot access Element Manager Console because Element Manager services were accidentally stopped while restarting all network element services

While restarting all network element services, you accidently stopped Element Manager services and now you cannot access Element Manager Console, even after rebooting the Element Manager server.

Proposed solution

Procedure

Log into the Element Manager server and restart Element Manager Console from the command line.

Unable to log into Element Manager Console or Provisioning Client via Single Signon (SSO)

Proposed solution

Procedure

1. Verify the element configuration on System Manager.
2. Verify network connectivity by both the IP address and FQDN between the Element Manager server and System Manager is working.

3. Confirm the host files on the workstation from which you are accessing System Manager has FQDN entries for both Element Manager and System Manager.
4. Confirm the security policies on the workstation from which you are accessing System Manager are not blocking you from adding a trusted network site, certificate, or entry to host file.
5. Confirm the TCP ports between the workstation you are using and System Manager are open on TCP 443, 12121 and 8443. These ports are used by Element Manager Console and the Provisioning Client.
6. Verify Certificates Common Name matches with FQDN, and make sure FQDN translates to appropriate IP addresses to Element Manager Console.
7. Determine if the Element Manager Console service IP address is different from the Element Manager server IP address (physical server).
8. Disable the pop-up blocker on the browser settings and add the Element Manager Console URL, Provisioning Client URL, and System Manager URL as trusted sites.
9. Ensure on System Manager that the SSO security task settings have correct entries.
10. Launch the URLs independently for Element Manager Console and Provisioning Client and see if that works first.
11. Verify if there are permanent DNS entries to Element Manager (recommended).
12. Confirm that certificates are assigned to Element Manager and PROV on Element Manager Console.

Unable to change the Web Conferencing server IP address in Element Manager Console

After installation, you are unable to change the IP address of the Web Conferencing server in Element Manager Console. This occurs because the Web Conferencing server IP address you assigned previously is bound to the services deployed.

Proposed solution

Procedure

1. Stop the network element service.
2. Undeploy the network element.
3. Change the IP address of the Web Conferencing server.

Element Manager Console always receives a bandwidth publish error

This error is related to SIP trunk bandwidth management configuration on Avaya Session Manager.

Proposed solution

Procedure

Verify Avaya Session Manager SIP trunk configurations are correct.

Provisioning Client problems

This section addresses various error conditions you may encounter while using Provisioning Client.

Unable to log into Element Manager Console or Provisioning Client via Single Signon (SSO)

Proposed solution

Procedure

1. Verify the element configuration on System Manager.
2. Verify network connectivity by both the IP address and FQDN between the Element Manager server and System Manager is working.
3. Confirm the host files on the workstation from which you are accessing System Manager has FQDN entries for both Element Manager and System Manager.
4. Confirm the security policies on the workstation from which you are accessing System Manager are not blocking you from adding a trusted network site, certificate, or entry to host file.
5. Confirm the TCP ports between the workstation you are using and System Manager are open on TCP 443, 12121 and 8443. These ports are used by Element Manager Console and the Provisioning Client.
6. Verify Certificates Common Name matches with FQDN, and make sure FQDN translates to appropriate IP addresses to Element Manager Console.
7. Determine if the Element Manager Console service IP address is different from the Element Manager server IP address (physical server).
8. Disable the pop-up blocker on the browser settings and add the Element Manager Console URL, Provisioning Client URL, and System Manager URL as trusted sites.
9. Ensure on System Manager that the SSO security task settings have correct entries.
10. Launch the URLs independently for Element Manager Console and Provisioning Client and see if that works first.
11. Verify if there are permanent DNS entries to Element Manager (recommended).

12. Confirm that certificates are assigned to Element Manager and PROV on Element Manager Console.

Unable to delete the SIP domain or service URI on Provisioning Client

When you try to delete the SIP domain or service URI on Provisioning Client, you are prompted for a password.

Proposed solution

Procedure

Enter the System Manager enrollment password to authenticate that the action is being performed by a trusted user.

System Manager problems

This section addresses various error conditions you may encounter while using System Manager.

Unable to provision the conference template to a user provisioned on System Manager

When you select Conferencing Profile and assign the conference template to a user in System Manager, no data is populated in the conference template.

Proposed solution

Procedure

1. Confirm System Manager has been upgraded to Avaya Aura 6.2 SP1 or above and that the hot fix patch (PSN Ref PSN003677u) has been applied.
2. Confirm TCP ports 443 and 8443 are open between the Element Manager server and System Manager.

SIP response message 488 is received on Avaya Session Manager when you call into Avaya Aura Conferencing

When you try calling into Avaya Aura Conferencing, you receive the SIP response message 488 on Avaya Session Manager.

Proposed solution

Procedure

Verify licensing is applied and the license is valid.

Configuration errors

To protect the system against Denial of Service (DoS) attacks, check the SIP Denial of Service mitigation configuration and the HTTP Denial of Service mitigation configuration.

Checking SIP Denial of Service mitigation configuration

About this task

Denial of Service attacks cause excessive SIP messaging, which can degrade system performance. The SIP Denial of Service mitigation feature protects the call server from Denial of Service attacks. You can enable this feature on each network element Instance. The SIP Denial of Service mitigation feature applies to Provisioning Client and Personal Agent.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** , **<*network element type*>, <*network element*>, Configuration Parameters**.
2. From the **Parm Group** drop-down box, select **SIPDoS**.
3. Select **Enable DoS filter**.
4. Click **Edit**.
5. From the **Value** drop-down box, select **true**.
6. Click **Apply**.

Checking HTTP Denial of Service mitigation configuration

About this task

Denial of service attacks cause excessive HTTP messaging, which can degrade system performance. The HTTP Denial of Service (DoS) Mitigation feature protects the web server from Denial of Service attacks. Administrators can enable this feature on each network element Instance. The HTTP Denial of Service mitigation feature applies to Provisioning Client and Personal Agent.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** , **<*network element type*>, <*network element*>, Configuration Parameters**.

2. From the **Parm Group** drop-down box, select **HTTPDoS**.
3. Select the filter parameter you want to modify. See HTTP Denial of Service mitigation configuration parameters on page 141.
4. Click **Edit**.
5. From the **Value** drop-down box, select **true**.
6. Click **Apply**.

HTTP Denial of Service mitigation configuration parameters

The following table describes the configuration parameters for the HTTPDoS parameter group.

Configuration parameter	Description
Enable MMS DoS filter	This parameter enables or disables the HTTP Denial of Service protection feature for the Provisioning Manager. Range: true or false Default: false
Enable PA Manager DoS filter	This parameter enables or disables the HTTP Denial of Service protection feature for the Personal Agent Manager. Range: true or false Default: false
Enable Presence DoS filter	This parameter enables or disables the HTTP Denial of Service protection feature for Presence. Range: true or false Default: false
Enable Prov Manager DoS filter	This parameter enables or disables the HTTP Denial of Service protection feature for the Provisioning Manager. Range: true or false Default: false
Enable SOPI DoS filter	This parameter enables or disables the HTTP Denial of Service protection feature for the Subscriber Open Provisioning Interface (SOPI). Range: true or false Default: false
Enable TPCC DoS filter	This parameter enables or disables the HTTP Denial of Service protection feature for Third Party Call Control. Range: true or false Default: false

Patching problems

You can manually downgrade the system software with the previous Maintenance Release or patch if an error occurred during patching. Reverting to a previous load consists of downgrading the network elements to the previous Maintenance Release or patch load. All network elements except the database are downgraded. The database stays at the newer software load. The database is not restored from a database backup of the previous MR or patch load.

Maintenance Releases and patch upgrades of the database are typically backwards compatible. If the database is corrupted or the database upgrade failed, you can only downgrade the database to a previous Maintenance Release or patch. For most database upgrade failures, a database downgrade is not required. Typically you can fix the database upgrade failure by checking the error logs, resolve any issues, and then execute the upgrade again.

Important:

Do not downgrade the system or database unless you understand the impacts associated with downgrading. A database downgrade is a last resort solution to a database problem. Downgrading the database from a backup causes data loss. All database changes, including provisioning and configuration since the last database backup, are lost after a database downgrade.

Chapter 11: Troubleshooting hardware faults

This chapter describes methods for managing and resolving problems with the Avaya Aura® Conferencing hardware.

Maintaining and Troubleshooting the HP ProLiant DL360 G9 Server

HP Server overview

The Avaya Common Servers category includes HP servers that support several Avaya software solutions, some requiring more hardware, and memory requirements beyond the standard configuration. This document covers the standard configuration only—consult specific Avaya product documentation for application-specific or solution-specific server configurations.

- Avaya Common Servers are supplied under an OEM relationship and Avaya servers are treated differently than other commercially available servers from the vendors.
- Avaya Common Servers are turnkey appliances. No server designed for a particular application can be repurposed for use with another application. The only exception to this is when an application has provided an upgrade or migration path from one server state to a different server state with the appropriate kits, tools, documentation, and training materials. For example, System Platform is providing a kit plus documentation for migrating a server running System Platform to Appliance Virtualization Platform.
- Neither customers, business partners, distributors, nor Avaya Associates interacting with customers and business partners, should get BIOS or other firmware updates for any third-party OEM servers forming part of Avaya's turnkey appliance offers. Only consult Avaya-provided downloads, information and support. All BIOS or firmware updates are provided through Avaya. Go to the Avaya Support website at http://support.avaya.com for additional information.
- Remote access and use of HP iLO hardware management tools for the HP servers are employed by a limited number of Avaya applications. If HP iLO is supported, that application's documentation will define its configuration and use. Please check with the Avaya application product manager or appropriate documentation to confirm support.

- Do not contact HP for Service; all support, warranty, repair, and maintenance are through the Avaya processes. If the server is purchased from Avaya, customer first point of contact is Avaya to troubleshoot hardware issues.

  Service and repair of consumable accessories and cables are not covered under maintenance. Customers must purchase these items.
- Avaya strongly recommends that all servers are protected with an Uninterruptable Power Supply for power surge and interruption protection. Avaya is not responsible for servers damaged by power surges, brown outs, black outs etc.
- Substitution of a DC power supply for a server must be approved by the Application Product Manager before substitution. If there is a significant demand for a turnkey solution with a DC power supply, an Avaya GRIP (Global Requirements Integration Process) request must be submitted. Partners registered to use this process can submit a GRIP request at https://portal.avaya.com/apps/grip/partner.asp. Avaya Associates may assist and can find information about this process at http://spark4.avaya.com/grip. Note, a GRIP request must be made for the Avaya application product, not the server model. The decision on whether to include a turnkey offer with a DC power supply is the responsibility of each Avaya application Product Manager. The name of the Product Managers for each application is at the bottom of the application page on the Avaya Global Sales portal.
- Product labels on the servers themselves have the 9-digit base server codes and a base server description for Avaya Services in service and support. These 9-digit codes differ from the 6-digit orderable codes under which servers are ordered. On every server package, there is a Packing Label and a Hierarchy Label. The Hierarchy Label itemizes the stock list in the box of the 6-digit orderable code and Avaya recommends retaining them for reference.
- Quality assurance – product integrity testing and environmental international restrictions were completed by HP and verified with Avaya using Design for Environmental Checklists. The list includes: batteries, printed wiring boards, plastic parts, product packaging, RoHS, green requirements, and energy efficiency.

How to use this document

This guide contains information for installing the server as part of an Avaya deployment and provides:

- Instructions for how to find the appropriate online server documentation from HP.
- References to specific topics in standard HP documentation
- Suggested changes, details, and notes to assist the user in interpreting the manufacturer’s documentation and to clarify Avaya's recommended implementation of the equipment
- Topics not covered in standard HP documentation, but which are necessary for successful installation and maintenance of Avaya products

Downloading HP documentation

Use this procedure to find and download the server documentation.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter Your Product Here** search box, type `Common Servers` and then select 3.0.x from the drop-down list.

   If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
6. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
7. Click **Enter**.

HP ProLiant DL360 G9 document set

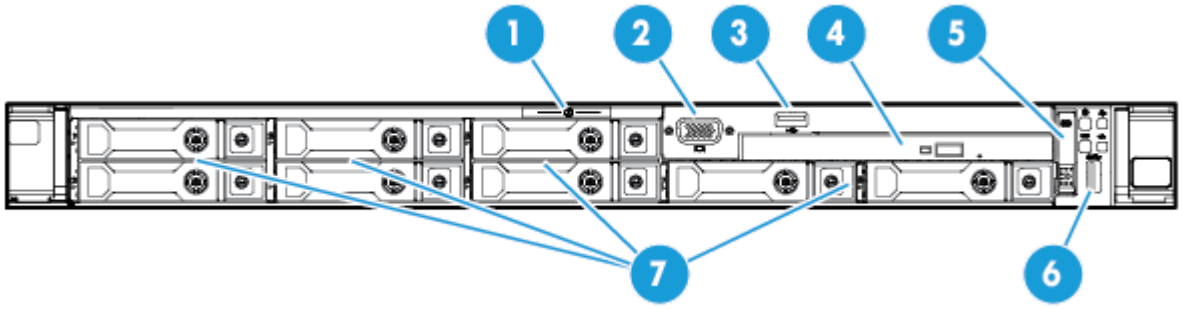
Documents

- HP ProLiant DL360 G9 Server User Guide
- HP ProLiant DL360 G9 Server Maintenance and Service Guide
- HP ProLiant DL360 G9 Troubleshooting Guide, Volume I: Troubleshooting
- HP ProLiant DL360 G9 Troubleshooting Guide, Volume II: Error Messages
- HP Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products

Documents included in the shipping container

Title	Part number
Safety, Compliance, and Warranty Information	703828 - 023
Quick Deploy Rail System Installation Instructions (located in rail kit box)	740122-002

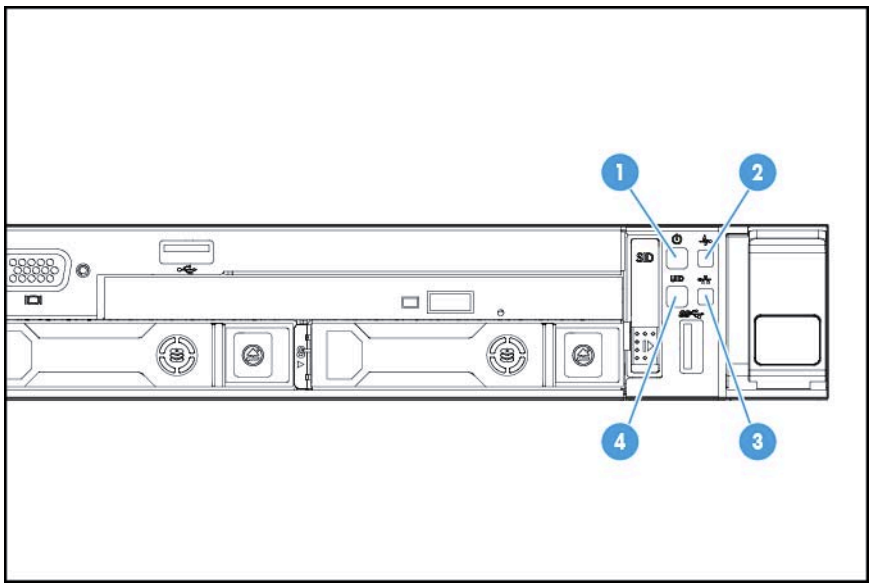
Front view of HP ProLiant DL360 G9 Server



No.	Description
1	Serial label pull tab
2	Front video connector
3	USB 2.0 connector
4	Optical drive
5	Systems Insight Display (Not used in Avaya configurations)
6	USB 3.0 connector
7	Hard Drive bays* * The HDDs read starting with top left, then bottom left, and continues to the right.

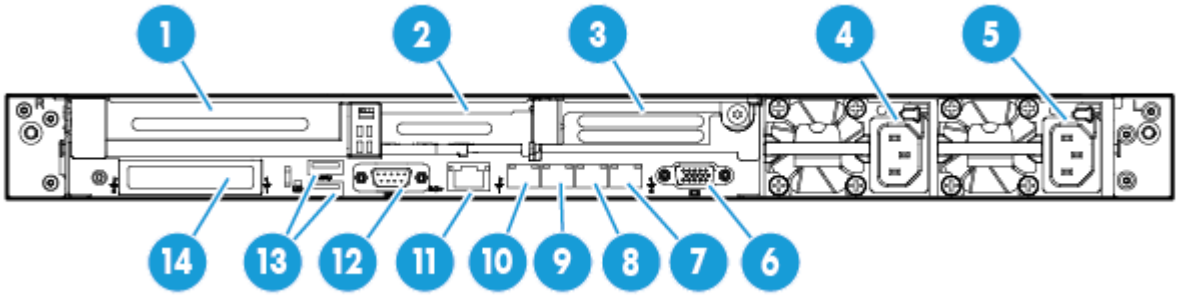
Front panel LEDs of HP ProLiant DL360 G9 Server

Use these LEDs to identify hardware status and problems.



Item	Description	Status
1	Power On/Standby Button/LED	Solid Green = System is on Flashing Green = Waiting for server power sequence Solid Amber = System is in standby, but power is still applied Off = Power cord is not attached, power supply failure has occurred, no power supplies are installed, facility power is not available or the power button cable is disconnected
2	Health LED	Solid Green = System health is normal Flashing Green = Power fault (check system and devices). See *HP ProLiant DL360 Gen9 Server User Guide*. Flashing Amber = System health is degraded. To identify the component in a degraded state, see Diagnosing system faults using Server console on page 150. Flashing Red = System health is critical. To identify the component in a critical state, see Diagnosing system faults using Server console on page 150. If possible check iLO/BIOS logs. Also check application's system log and SEL log from IPMI interface if possible.
3	NIC Status LED	Solid Green = Link to network Flashing Green = Network active Off = No network connection or activity
4	UID button/LED	Solid Blue = Identification is activated Flashing Blue = System is being managed remotely or firmware upgrade is in progress Off = Identification is deactivated

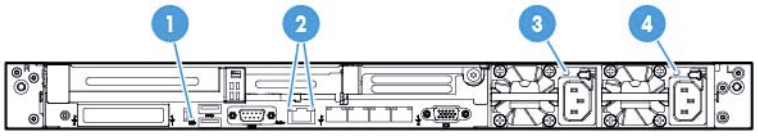
Rear view of HP ProLiant DL360 G9 Server



No.	Description
1	Slot 1 PCIe3 x16 (16, 8, 4, 1)
2	Slot 2 PCIe 3 x8 (8, 4, 1)
3	Slot 3 PCIe 3 x16 (16, 8, 4, 1) (Not used in Avaya configurations)
4	Power supply 2
5	Power supply 1
6	Video connector
7	NIC connector 4
8	NIC connector 3
9	NIC connector 2
10	NIC connector 1
11	iLO 4 connector
12	Serial connector
13	USB 3.0 connectors
14	FlexibleLOM bay (Not used in Avaya configurations)

Rear panel LEDs of HP ProLiant DL360 G9 Server

Use these LEDs to identify hardware status and problems.



Item	Description	Status
1	UID button/LED	Solid Blue = Identification is activated Flashing Blue = System is being managed remotely Off = Identification is deactivated
2 (left)	HP iLO/Standard NIC activity LED	Solid Green = Activity exists Flashing Green = Activity exists Off = No activity exists
2 (right)	HP iLO/Standard NIC link LED	Solid Green = Link exists Off = No link exists
3	Power supply 2 LED	Solid Green = Normal Off = One or more of the following conditions exists: • AC power unavailable • Power supply failed • Power supply in standby mode • Power supply exceeded current limit
4	Power supply 1 LED	Solid Green = Normal Off = One or more of the following conditions exists: • AC power unavailable • Power supply failed • Power supply in standby mode • Power supply exceeded current limit

Diagnosing system faults using Server console

About this task

Use this procedure to view health status, run system tests, run component tests, and view test logs. Individual component troubleshooting steps are discussed throughout this document, but this section will be referenced often for querying system health status and running component tests.

Note:

Before performing any maintenance or tests on the server and its components, ensure that you take full backup of your system data.

Procedure

1. Connect a monitor, USB keyboard, and mouse to Server.

   Note:

   Avaya customer must provide a keyboard, mouse, and monitor for the system when an Avaya or Business Partner tech must do work on-site.

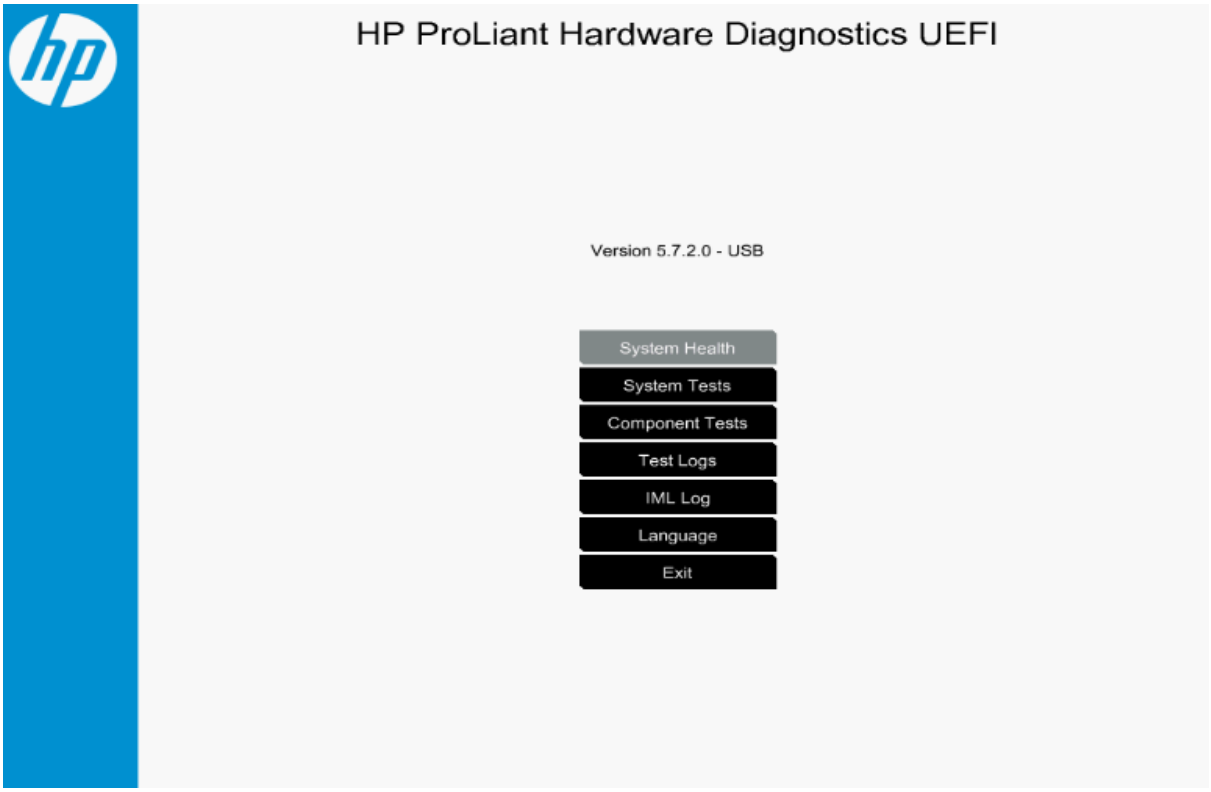
2. Power up or reboot the server.

   Follow Avaya application procedure, if applicable.

3. When the system displays the HP splash screen, press `F9` to go to **System Utilities**.

4. From **System Utilities**, navigate to **Embedded Applications** > **Embedded Diagnostics** and press **ENTER**.

   The system displays the HP ProLiant Hardware Diagnostics UEFI screen.



5. On the HP ProLiant Hardware Diagnostics UEFI screen, select one of the following options:
   - **System Health** to diagnose the health status of BIOS Hardware, Fans, Temperature, Power Supplies, Battery, Processors, Memory, NIC and Network information, Storage, and Firmware information. You can run a query to know the state of health for each of these components.

     The system displays the health analysis. Based on the analysis of any failed components, the component must be identified and replaced.
   - **System Tests** to diagnose the function of hardware subsystems. You can run a quick test of the hardware for 10 minutes or an extensive hardware test that might take two or more hours to complete.
   - **Component Tests** to diagnose Processor, Memory, Hard Drive, Keyboard, Mouse, Network, Optical Drive, System Board, USB Port, and Video.
   - **Test Logs** displays test logs that includes Start Time, type, Result, Failure ID, and description.
   - **IML Log** displays IML logs that includes severity, class, initial time, and update time information.
   - **Language** to select the language to perform the Embedded Diagnostics.
   - **Exit** to close the Embedded Applications and go back to **System Utilities**.

External Maintenance Field Replaceable Units

Note:

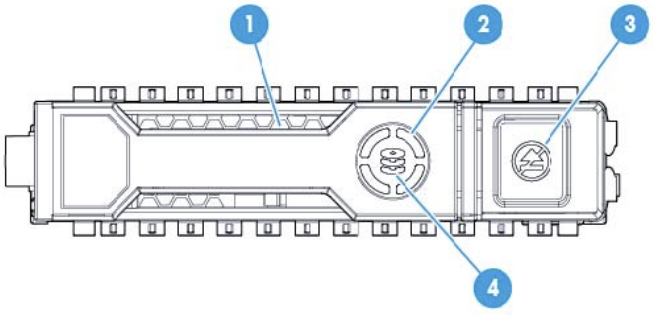
HDD Field Replaceable Units (FRUs) are Hot Swappable assuming you have RAID 1 configuration with 2 HDDs, and 1 of the HDDs is in working order. A RAID 5 Configuration is hot-swappable only if you are swapping 1 HDD, and the other 2 through 7 HDDs are in working order.

Description	Hot-swappable?
DL360/380G9 300GB 10K SAS 2.5" HDD	Y
DL360/380G9 300GB 15K SAS 2.5" HDD	Y
DL360/380G9 600GB 10K SAS 2.5" HDD	Y
DL360/380G9 900GB 10K SAS 2.5" HDD	Y
DL360/380G9 1.2TB 10K SAS 2.5" HDD	Y
DL360/380G9 200GB SATA 2.5" SSD	Y, if redundant
DL360/380G9 500 WAC PWR SUP	Y, if redundant
DL360/380G9 800 WAC PWR SUP	Y, if redundant
DL360/380G9 800 WDC PWR SUP	Y, if redundant

Hard disk drive problems

Hard drive LEDs

Use these indicators to identify status and problems with a hard drive.



Item	LED	Status	Definition	Avaya recommendations and information
1	Locate	Solid blue	The drive is being identified by a host application	This is normal operation if application supports this feature or if disk array is being created/ selected.

Table continues…

Item	LED	Status	Definition	Avaya recommendations and information
		Flashing blue	The drive carrier firmware is being updated or requires an update	Check support.avaya.com for HP DL360 G9 firmware updates. View release notes for Avaya firmware update inclusions for HDD update.
2	Activity ring	Rotating green	Drive activity	This is normal operation and indicates that the drive is currently operating as part of the RAID array.
		Off	No drive activity	This indicates that the drive may currently have no activity or is not part of the RAID array.
3	Do not remove	Solid white	Do not remove the drive. Removing the drive causes one or more of the logical drives to fail.	This indicates that the RAID array is operating in degraded mode because one of the drives in the array has failed or is currently rebuilding. Removing a drive in this state will destroy the logical drive array. If the array is currently rebuilding this status will clear when the new replacement drive has rebuilt. Rebuild can take from 20 minutes up to 2 hours depending on the size of drive and activity of the system.
		Off	Removing the drive does not cause a logical drive to fail.	If an active drive is removed, the other drives that are part of the array will indicate a status of “do not remove”.
4	Drive status	Solid green	The drive is a member of one or more logical drives	This indicates normal operation.
		Flashing green	The drive is rebuilding or performing a RAID migration, stripe size migrations, capacity expansion, or logical drive extension, or is erasing.	A newly inserted replacement drive should start this LED pattern within 10-15 seconds of insertion to indicate a rebuild of the logical drive. If action does not start, unplugging and reinserting new drive can be performed.
		Flashing amber/ green	The drive is a member of one or more logical drives and predicts the drive will fail.	This signature indicates future failure and drive should be replaced asap.
		Flashing amber	The drive is not configured and predicts the drive will fail	The drive must be replaced ASAP if it is needed for current array.
		Solid amber	The drive has failed	The drive must be replaced ASAP.

Table continues…

Item	LED	Status	Definition	Avaya recommendations and information
		Off	The drive is not configured by a RAID controller	Reinsert drive if expected to rebuild as part of array. If no LED activity continues, try another unused drive if possible. Tools to recreate the RAID array can be accessed at support.avaya.com. If a new array is created all data from the previous array will be destroyed.

Hard disk drive problems

Symptoms

Some possible symptoms indicating hard drive problems are:

- Drives have failed as indicated by HDD LEDs (Hard drive LEDs on page 152) or alarmed by Avaya application.
- There is an active disk drive failure alarm from an Avaya application
- Drives are not recognized by Avaya application
- Data is inaccessible
- Server response time is slower than usual

HP documentation references

- Troubleshooting Guide Volume 1: SAS, SATA, and SSD drive guidelines
- Troubleshooting Guide Volume 1: Drive problems (hard drives and solid state drives)

Helpful guidelines

When adding drives to the server, observe the following general guidelines:

- Drives must be of the same capacity to provide the greatest storage space efficiency when drives are grouped together into the same drive array. Larger capacity drives can be used, but will only utilize their capacity to match the size of the smallest drive in the array.
- Drives in the same logical volume must be of the same type. ACU does not support mixing SAS, SATA, and SSD drives in the same logical volume.

Troubleshooting a hard disk drive

About this task

Follow the steps below to troubleshoot hard drive problems on one of these drives:

- DL360/380G9 300GB 10K SAS 2.5" HDD
- DL360/380G9 300GB 15K SAS 2.5" HDD
- DL360/380G9 600GB 10K SAS 2.5" HDD
- DL360/380G9 900GB 10K SAS 2.5" HDD
- DL360/380G9 1.2TB 10K SAS 2.5" HDD

- DL360/380G9 200GB SATA 2.5" SSD

Procedure

1. Ensure there are no loose connections, and all drives are fully seated.
2. Check HDD/SSD LEDs for indication of possible problems. See Hard drive LEDs on page 152.
3. Ensure drive blanks are installed properly when the server is operating. Drives might overheat and cause sluggish response or drive failure.
4. Ensure the replacement drives within an array are the same size or larger.
5. Ensure the replacement drives within an array are the same drive type, such as SAS, SATA, or SSD.
6. Power cycle the server. Shutdown server according to Avaya application procedures.
7. Go to **System Health** > **Storage**, to diagnose the hard drive problem, see Diagnosing system faults using Server console on page 150.

   Running **Component Tests** > **Hard Drive tests** might not work because a RAID controller is installed in this server. However, you can view the Hard Drive status and health from **System Health** > **Storage**.
8. Check the Avaya Support website: http://support.avaya.com to see if a firmware update is available from Avaya for this model of server. View notes to see if firmware update is applicable to the observed problem before applying the update.

Next steps

If the part is defective, continue with the following removal and replacement procedures.

Replacing a hard disk drive

Before you begin

Best practice is to ensure the customer has a good separate backup of their system data before performing any maintenance on the server.

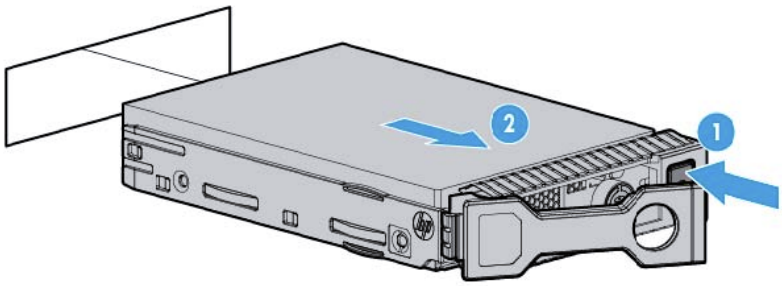
About this task

Follow the steps below to replace one of these drives:

- DL360/380G9 300GB 10K SAS 2.5" HDD
- DL360/380G9 300GB 15K SAS 2.5" HDD
- DL360/380G9 600GB 10K SAS 2.5" HDD
- DL360/380G9 900GB 10K SAS 2.5" HDD
- DL360/380G9 1.2TB 10K SAS 2.5" HDD
- DL360/380G9 200GB SATA 2.5" SSD

Procedure

1. Remove the drive.
   a. Push button to release locking latch. (#1 in the following image)
   b. Pull on unlocked latch to remove HDD/SSD. (#2 in the following image)



   Drives are hot-swappable so power down of server is not recommended. However, only one drive must be replaced at a time until RAID array rebuild is complete.

2. Replace the drive.
   a. Insert HDD/SSD into empty drive slot.
   b. Secure HDD/SSD by closing the latch.
   c. Refer to the Hard Drive LED table for the drive rebuild status.
   d. Check using Avaya application tools for RAID status if available.

Power supply problems

Symptoms

Some possible symptoms indicating power supply problems are:

- The server does not power on.
- The system power LED is Off or Solid Amber. See Front panel LEDs of HP ProLiant DL360 G9 Server on page 146.
- The health LED is Flashing Green, Flashing Amber, or Flashing Red. See Front panel LEDs of HP ProLiant DL360 G9 Server on page 146.

HP documentation references

- Troubleshooting Guide Volume 1: Power Source Problems
- Troubleshooting Guide Volume 1: Power Supply Problems
- Troubleshooting Guide Volume 1: Power-on problems flowchart

Possible Causes

List of possible causes for the above symptoms:

- Improperly seated or faulty power supply

- Loose or faulty power cord
- Power source problem
- Improperly seated component or interlock problem

If the power supply LED is off, it could mean any of the following:

- AC power unavailable
- Power supply failed
- Power supply in standby mode
- Power supply exceeded current limit

Troubleshooting a power supply

About this task

Follow the steps below to troubleshoot and replace one of these power supplies:

- DL360/380G9 500 W AC PWR SUP
- DL360/380G9 800 W AC PWR SUP
- DL360/380G9 800 W DC PWR SUP

Table 1: Power supply LEDs

System Power LED	Definition
Off (Server)	System has no power.
Solid Amber	System is in standby, **Power On**/**Standby** button service is initialized.
Flashing Green	System is waiting to power on; **Power On**/**Standby** button is pressed.
Solid Green	System is powered on.

Procedure

1. To troubleshoot possible power source problems:
   a. Plug another device into the grounded power outlet to be sure the outlet works. Also, be sure the power source meets applicable standards.
   b. Replace the power cord with a known functional power cord to be sure it is not faulty.
   c. Replace the power strip with a known functional power strip to be sure it is not faulty.
   d. Have a qualified electrician check the line voltage to be sure it meets the required specifications.
   e. Ensure the proper circuit breaker is in the On position.

   If power source is not the problem, continue with steps below to troubleshoot power supplies.
2. Ensure no loose connections exist.
3. Press the **Power On**/**Standby** button to be sure it is on. If the server has a **Power On**/**Standby** button that returns to its original position after being pressed, be sure you press the

switch firmly. For more information about system power LED status, see Rear panel LEDs of HP ProLiant DL360 G9 Server on page 148.

4. Check the power supply LEDs, ensure they indicate that each power supply is working properly. If the LEDs indicate a problem with a power supply (red, amber, or off), then check the power source. If the power source is working properly, then replace the power supply.
5. If running a redundant configuration, be sure that all of the power supplies in the system have the same spare part number and are supported by the server.
6. If power supplies are redundant and server is powered up, see Diagnosing system faults using Server console on page 150. Go to **System Health** > **Power Supplies** and view power supply health.

Next steps

If the part is defective, continue with the following removal and replacement procedures.

Replacing a power supply

About this task

Follow the steps below to replace one of these power supplies:

- DL360/380G9 500 W AC PWR SUP
- DL360/380G9 800 W AC PWR SUP
- DL360/380G9 800 W DC PWR SUP

Procedure

1. If system does not have redundant power, shut down the server according to Avaya application procedures. Server might already be down because of failed power supply. If server power is redundant, proceed to step 2.
   - If server does not power down according to normal shutdown procedures, press and release the **Power On/Standby** button. This method initiates a controlled shutdown of applications and the OS before the server enters standby mode.
   - Press and hold the **Power On/Standby** button for more than 4 seconds to force the server to enter standby mode. This method forces the server to enter standby mode without properly exiting applications and the OS. If an application stops responding, you can use this method to force a shutdown, but be aware that file corruption could occur using this method.
2. Replace failed power supply.
   a. Press tab (1 in the following figure).
   b. Pull supply out (2 in the following figure).
   c. Install new supply.

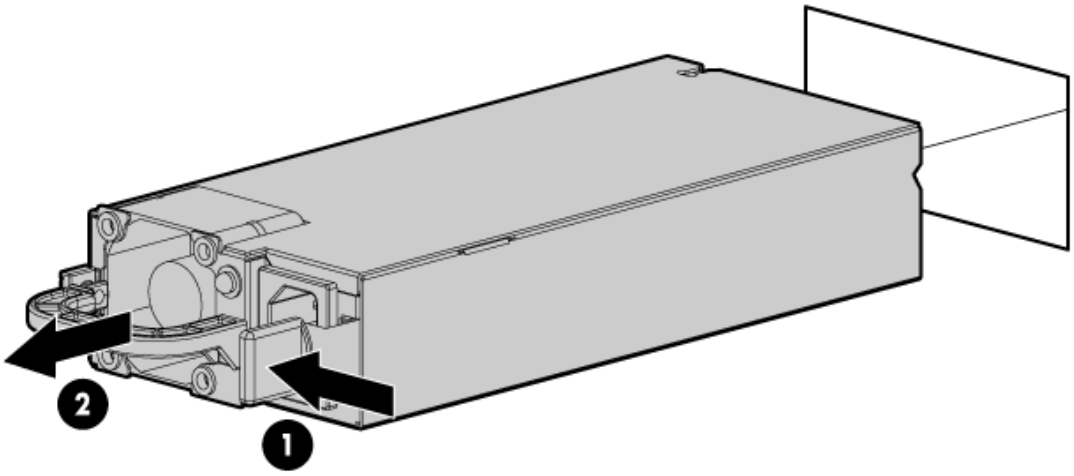


Figure 7: Replacing power supply

3. If disconnected, connect the power cables to the power supply.
4. If powered down, power up the server.

Internal Field Replaceable Units

Note:

Internal Field Replaceable Units (FRUs) require the server to be shutdown and the cover removed to access and replace the FRU.

Description
DL360G9 DVD-RW DRIVE W/BRKT
DL360/380G9 1Gb PCIE DUAL PT NIC
DL360/380G9 CHASSIS FAN
DL360/380G9 4GB RDIMM
DL360/380G9 10Gb ETH PCIe DUAL PT NIC
DL360/380G9 TAPE DRV SAS HBA ADPTR

DVD-RW problems

Symptoms

- System does not boot from the drive.
- Data read from the drive is inconsistent, or drive cannot read data.

- Drive is not detected.

HP documentation references

- Troubleshooting Guide Volume 1: Internal system problems
- Troubleshooting Guide Volume 1: CD-ROM and DVD drive problems

Troubleshooting a DVD-R/W drive

About this task

Follow the steps below to troubleshoot a DL360G9 DVD-RW DRIVE W/BRKT.

Warning:

Eliminate the risk of electric shock by removing all AC power from the system before installing or replacing any non hot-plug hardware option. Disconnect all power cords to completely remove power from the server. Always follow Avaya's application procedures when shutting down the server.

Warning:

To reduce the risk of personal injury from hot surfaces, allow the drives and the internal system components to cool before touching them.

Procedure

1. If system is not booting from drive:
   a. Ensure there are no loose connections.
   b. Ensure the media from which you are attempting to boot is not damaged and is a bootable CD or DVD.
   c. If possible, be sure the drive boot order in BIOS is set so that the server boots from the CD -ROM drive first.
2. If data read from drive is inconsistent:
   a. Clean the drive and media.
   b. If a paper or plastic label has been applied to the surface of the CD or DVD in use, remove the label and any adhesive residue.
3. If drive is not detected:
   a. Ensure there are no loose connections.
   b. Ensure the cables are working properly. If possible, replace with known functional cables to test whether the original cables were faulty.
4. Go to **Component Tests** > **Optical Drive**, run the component test, and test the optical drives. See Diagnosing system faults using Server console on page 150.

Next steps

If the part is defective, continue with the following removal and replacement procedures.

Replacing a DVD-R/W drive

About this task

Follow the steps below to replace a DL360G9 DVD-RW DRIVE W/BRKT.

Warning:

Eliminate the risk of electric shock by removing all AC power from the system before installing or replacing any non hot-plug hardware option. Disconnect all power cords to completely remove power from the server. Always follow Avaya's application procedures when shutting down the server.

Warning:

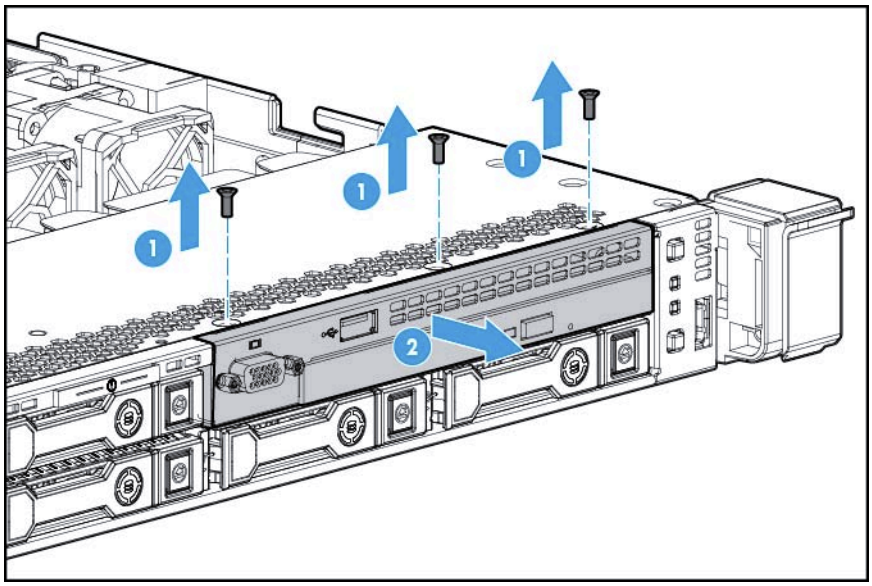
To reduce the risk of personal injury from hot surfaces, allow the drives and the internal system components to cool before touching them.

Procedure

1. Power down the server.

   Follow Application power down procedures, if applicable.
2. Remove all power:
   - Disconnect each power cord from the power source.
   - Disconnect each power cord from the server.
3. Extend the server from the rack.
4. Remove the access panel.
5. If installed, remove the FBWC capacitor pack.
6. To remove the DVD drive, do the following:
   a. Remove 3 Torx screws by using a T-10/T-15 Torx screwdriver as shown in the below illustration.
   b. Disconnect the SATA DVD cable from rear of DVD drive. Disconnect VGA/USB cables from rear of system board to fully remove the DVD drive from the bay.

c. Remove the DVD drive from the server.



d. Disconnect the SATA DVD cable from the rear of the DVD drive.

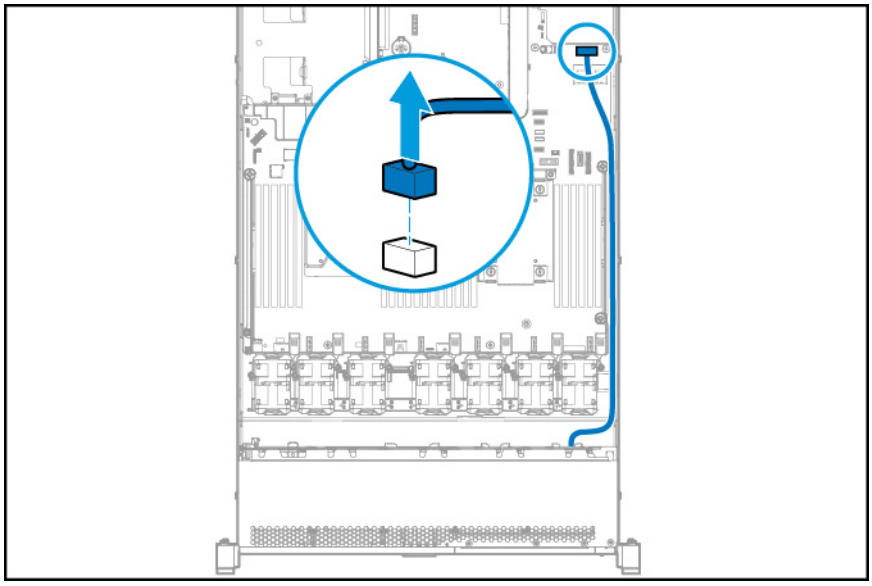
To insert DVD drive:

7. For an SFF DVD drive, do the following:

a. Install the DVD drive using the screws from this kit and a T-10/T-15 Torx screwdriver.

b. Reconnect SATA DVD cable to rear of DVD drive.

c. Connect VGA and USB cables to connectors at rear of motherboard.



d. Clip the cable to the power supply air baffle when routing it along the edge of the system board.

8. Install the access panel.
9. Slide the server into the rack.
10. Connect each power cord to the server.
11. Connect each power cord to the power source.
12. Power up the server.

NIC problems

Symptoms

- Network controller is installed, but not working.
- Network controller has stopped working.
- Network controller stopped working when an expansion board was added.

HP documentation references

- Troubleshooting Guide Volume 1: Network controller problems

Troubleshooting a NIC

Procedure

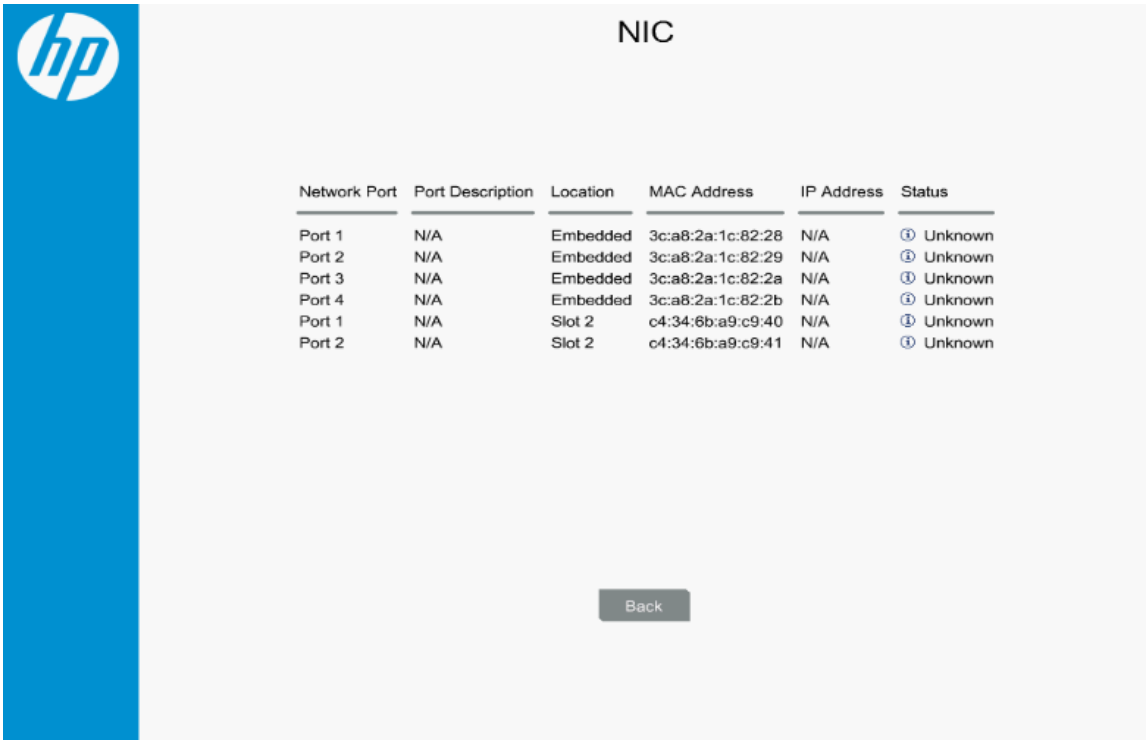
1. Check the network adopter LEDs for status indicating the potential source of the problem. These LEDs are located on each RJ-45 jack. Also, check the NIC Status LED located on the Front Panel of the DL360 G9, see Front panel LEDs of HP ProLiant DL360 G9 Server on page 146.

Table 2: NIC LED status

Item	Description	Status
RJ-45 Right LED	Activity LED	Solid green = Activity exists. Flashing green = Activity exists. Off = No activity exists.
RJ-45 Left LED	Link LED	Solid green = Link exists. Off = No link exists.

2. Ensure there are no loose connections.
3. Ensure the correct cable type is used for the network speed or that the correct SFP or DAC cable is used. For dual - port 10GB networking devices, both SFP ports must have the same media (for example, DAC cable or equal SFP+ module). Mixing different types of SFP (SR/LR) on a single device is not supported.
4. Ensure the network cable is working by replacing it with a known functional cable.
5. Ensure a valid IP address is assigned to the controller and that the configuration settings are correct according to Avaya's application documentation.
6. If the Avaya application is running utilize built in network test/debugging commands, if available.

7. If Avaya application is not running, see Diagnosing system faults using Server console on page 150.
   a. Navigate to **System Health** > **NIC Information** > **NIC**.
   b. On the NIC page, the system displays the NIC devices.



   c. Ensure that the **Location** field and **MAC Address** field are reported.
   d. The **IP Address** field and **Status** field will not report; that is normal.
   e. If a Network port is not recognized under **Location** or **MAC address** that NIC device might be bad.
   f. If bad Port is located in server slot 1 or slot 2 replace appropriate PCIe NIC card. If bad Port is in the Embedded location, you must replace the server as NIC device is integrated onto server motherboard.
8. If none of the ports are failed, navigate to **HP Diagnostics Menu** > **Component Tests** > **Networks** and follow on-screen directions to perform network tests.

Next steps

If PCIe NIC is defective, continue with the following removal and replacement procedures.

Replacing a NIC

About this task

Follow the steps below to replace the DL360/380G9 1Gb PCIE DUAL PT NIC.

Note:

Always follow safe electrostatic discharge practices.

Procedure

1. Power down the server according to Avaya's application instructions.
2. Remove all power:
   a. Disconnect each power cord from the power source.
   b. Disconnect each power cord from the server.
3. Remove any attached network cables.
4. Extend the server from the rack.
5. Remove the access panel.
6. Loosen the thumbscrew.
7. To replace the dual port PCIe 1GB NIC follow the expansion board removal instructions. See PCIe riser card assembly on page 165.
8. Install the access panel.
9. Slide the server into the rack.
10. Connect the LAN segment cables.
11. Connect each power cord to the server.
12. Connect each power cord to the power source.
13. Power up the server.

PCIe riser card assembly

About this task

Use this procedure when adding or removing NIC cards.

Note:

Always follow safe electrostatic discharge practices.

Procedure

1. Power down the server according to Avaya's application instructions.
2. Remove all power:
   a. Disconnect each power cord from the power source.
   b. Disconnect each power cord from the server.
3. Extend the server from the rack.
4. Remove the access panel.

5. Remove the installed expansion boards and PCIe riser board. Remove suspect PCIe NIC card from PCIe riser board connector. Insert replacement NIC card in riser board assembly and insert riser assembly into mother board socket ensuring connections are aligned.

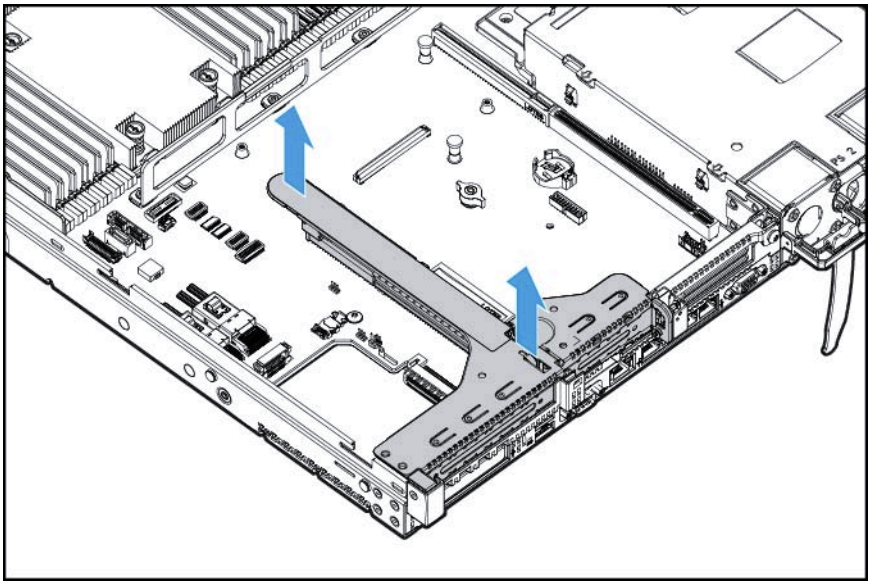


Figure 8: Removing PCIe riser cage

Thermal (fan) problems

Symptoms

- Server powers up but quickly shuts down.
- Flashing Amber LED indicates a fan failure. See Front panel LEDs of HP ProLiant DL360 G9 Server on page 146.
- Avaya application alarms fan failure.

Note:

For servers with redundant fans, backup fans might spin up periodically to test functionality. This is part of normal redundant fan operation.

HP documentation references

- Troubleshooting Guide Volume 1: Hot-plug fan problems are occurring
- User Guide: Hot-plug fan

Troubleshooting thermal fans

About this task

Follow the steps below to troubleshoot the HP DL360 G9 CHASSIS FAN.

Note:

Always follow safe electrostatic discharge practices.

Procedure

1. Ensure that the fans are properly seated and working.
   a. Follow the procedures and warnings in the server documentation for removing the access panels and accessing and replacing fans.
   b. Unseat, and then reseat a fan that has been flagged as failed. Fans are hot swappable. At a time, perform this step on one fan. Before reseating another fan (if required), ensure that the newly reseated fan has spun up.
   c. Replace the access panels, and then attempt to restart the server.
2. Ensure all fan slots have fans or blanks installed.

   Note:

   The server has seven fans. Install fans 1 and 2 only when processor 2 is installed. When only one processor is installed, install the fan blanks in bays 1 and 2.
3. Ensure no ventilation problems exist. If you have been operating the server for an extended period of time with the access panel removed, airflow may have been impeded, causing thermal damage to components.
4. Verify the fan airflow path is not blocked by cables or other material.
5. Ensure no POST error messages are displayed while booting the server that indicate temperature violation or fan failure information.
6. Go to **System Health** > **Fans**, see Diagnosing system faults using Server console on page 150.
7. Check the LEDs to be sure the hot-plug fans are working.
8. Ensure hot-plug fan requirements are being met.

Next steps

If the part is defective, continue with the following removal and replacement procedures.

Replacing thermal fans

About this task

Follow the steps below to replace the DL360G9 CHASSIS FAN.

Note:

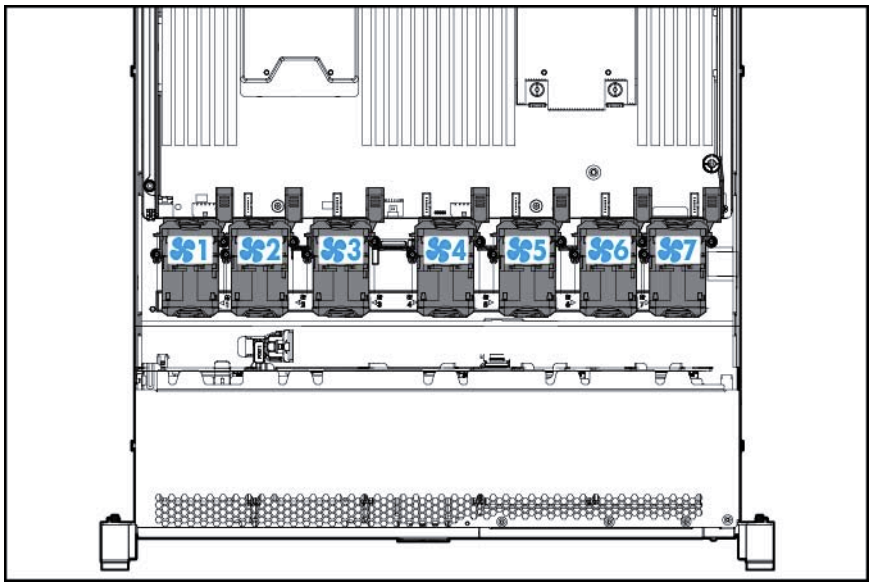
Always follow safe electrostatic discharge practices.

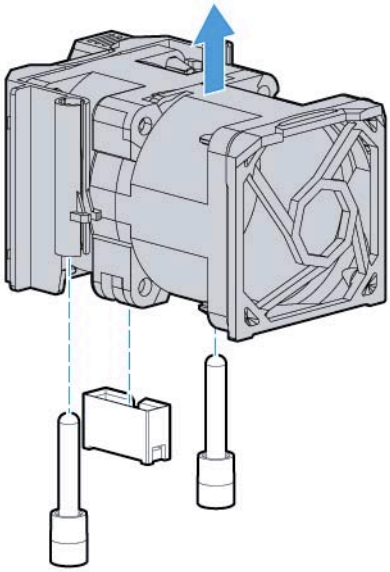
Procedure

1. Replace any required non - functioning fans and restart the server if necessary. Fans are hot-swappable.
2. To remove the component:
   a. Extend the server from the rack. If the server is to remain on with application up, ensure power cord does not disconnect when extending server from rack.

b. Remove the access panel.

c. Remove the fan module.





Caution:

To avoid server shutdown, a fan must be replaced within 60 seconds of being removed.

3. To replace the component:

   a. Install the Fan Module.

   b. Install the access panel.

   c. Slide the server into the rack.

DIMM problems

Symptoms

- General memory problems are occurring.
- Server is out of memory.
- Memory count error exists.
- Server fails to recognize existing memory.
- Server fails to recognize new memory.

HP documentation references

Troubleshooting Guide Volume 1: DIMM handling guidelines

Server Maintenance and Service Guide: DIMMS

Helpful Guidelines

- Always follow safe ESD practices.
- Avoid electrostatic discharge.
- Always hold DIMMs by the side edges only.
- Avoid touching the connectors on the bottom of the DIMM.
- Never wrap your fingers around a DIMM.
- Avoid touching the components on the sides of the DIMM.
- Never bend or flex the DIMM.

Troubleshooting memory DIMMs

About this task

Follow the steps below to troubleshoot a DL360/380G9 4GB RDIMM.

Procedure

1. If general memory problems are occurring:
    a. Navigate to **HP Embedded Diagnostics** > **System Health** > **Memory**, see Diagnosing system faults using Server console on page 150.
    b. Isolate and minimize the memory configuration.
    c. Check any server LEDs that correspond to memory slots.
    d. View power-up screen for any memory errors displayed if monitor is installed.
    e. If you are unsure which DIMM has failed, test each bank of DIMMs by removing all other DIMMs. Then, isolate the failed DIMM by switching each DIMM in a bank with a known working DIMM. Start installing CH1A first and then proceed to install CH2B, second and continue to populate in that order.
    f. Remove any third – party memory.
    g. To test the memory, navigate to **HP Embedded Diagnostics** > **Component Tests** > **Memory** to run the memory test.

2. If the server is out of memory:
    a. Ensure no operating system errors are indicated.
    b. Ensure a memory count error did not occur. Refer to the message displaying memory count during POST. This can only be viewed with monitor and keyboard.
3. If a memory count error exists, a possible cause is that the memory modules are not installed correctly.
    a. Ensure the memory modules are supported by the server.
    b. Ensure the memory modules have been installed correctly in a supported configuration.
    c. Ensure the memory modules are seated properly
    d. Ensure no operating system errors are indicated.
    e. Restart the server and check to see if the error message is still displayed.
    f. Run **HP Embedded Diagnostics** > **Component Tests**. Then, replace failed components as indicated.
4. If the server fails to recognize existing memory:
    a. Reseat the memory.
    b. Ensure the memory is configured properly.
    c. Ensure a memory count error does not occur. See the message displaying memory count during POST. This can only be viewed with monitor and keyboard.
5. If the server fails to recognize new memory:
    a. Ensure the memory is the correct type for the server and is installed according to the server requirements.
    b. Ensure you have not exceeded the memory limits of the server or operating system.
    c. Ensure the memory is seated properly.
    d. If possible test the memory by installing the memory into a known working server. Ensure the memory meets the requirements of the new server on which you are testing the memory.

Next steps

If the part is defective, continue with the following removal and replacement procedures.

Replacing memory DIMMs

About this task

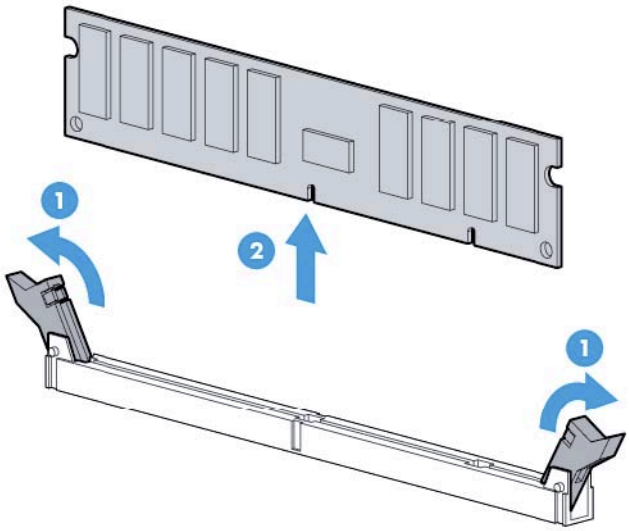
Follow the steps below to replace a defective DL360/380G9 4GB RDIMM.

Procedure

1. Power down the server.

    Follow Application power down procedures, if applicable.

2. Remove all power:
   a. Disconnect each power cord from the power source.
   b. Disconnect each power cord from the server.
3. Extend the server from the rack.
4. Remove the access panel.
5. Remove the DIMM.



6. To replace the component, reverse the removal procedure.

RAID Battery

The RAID battery is customer replaceable unit (CRU). The RAID battery is not covered under the maintenance agreement. The customer must order the RAID Battery by calling the appropriate Order Entry Fulfillment Collections (OEFC) center as listed in the following table.

Table 3: Order Entry Fulfillment Collections (OEFC) center

Country	Phone number
Avaya Order Entry Fulfillment Collections (Avaya OEFC)	
USA	+1 800 852 2436
EMEA	+91 20 30412500
APAC	+65 6872 8599
Canada	+1 905 474 6589
CALA	

Table continues…

Country	Phone number
Argentina	+5255 5278 7640
Brazil	+5511 5185 6610
Colombia	+571 616 6077
Mexico	+5255 5278 7720 +65 6872 8599

Table 4: RAID Battery part number

Part number	Description
700511627	DL360/380G9 RAID BATTERY

Note:

If the server needs to be replaced, the customer must move the RAID battery from the current server to the replacement server.

For information about HP ProLiant DL360 G9 RAID configuration, see *HP ProLiant DL360 G9 RAID Configuration* on the Avaya Support website at http://support.avaya.com.

Server Field Replaceable Unit

A Server FRU is based on the Server core components. A server FRU will have the correct number (1 or 2) and type of CPUs (High or Low), it will have 4 DIMMs and the 4 embedded NIC ports. The following components will need to be sourced from the existing server: HDDs, Power Supply Unit (PSU), PCIe Cards, and any additional DIMMs over 4.

Note:

S8800, Common Server Release 1, and Common Server Release 2 used the same FRU policy with these minor differences. They shipped setup for RAID 1 with 2 HDDs, and a single PSU. Also, these servers are shipped with 2 DIMMs, if you had a single CPU and 4 DIMMs, if you had 2 CPUs.

Global asset recovery policy

To return any failed part or component, check the Return merchandise authorization (RMA) policy on the Avaya Support website http://support.avaya.com under **Help & Policies** > **Policies & Legal** > **Global Asset Recovery Policy**.

Maintaining and Troubleshooting the HP DL360p G8 Server

Server overview

The Avaya Common Servers category includes the server that supports several Avaya software solutions, some requiring more hardware, and memory requirements beyond the standard configuration. This overview covers the standard configuration only—consult specific Avaya product documentation for application-specific or solution-specific server configurations.

- Avaya Common Servers are supplied under an OEM relationship and Avaya servers are treated differently than other commercially available servers from the vendors.
- Neither customers, business partners, distributors, nor Avaya Associates interacting with customers and business partners, should get BIOS or other firmware updates for any third-party OEM servers forming part of Avaya's turnkey appliance offers. Only consult Avaya-provided downloads, information and support. Send questions to the Server Product Management mailbox at srvrprodmgt@avaya.com.
- Avaya Common Servers are turnkey appliances. No server designed for a particular application can be repurposed for use with another application. The only exception to this is when an application has provided an upgrade or migration path from one server state to a different server state with the appropriate kits, tools, documentation, and training materials. For example, Avaya Aura® Messaging is providing a kit plus documentation for migrating a server running Modular Messaging to Avaya Aura® Messaging.
- Remote access and use of HP's hardware management tools for the server are not supported by any Avaya application (HP ILO).
- Do not contact HP for Service; all support, warranty, repair, and maintenance are through the Avaya processes.
- Avaya strongly recommends that all servers are protected with an Uninterruptable Power Supply for power surge and interruption protection. Avaya is not responsible for servers damaged by power surges, brown outs, black outs etc. when the server is connected to standard power mains and has no protection.
- Substitution of a DC power supply for a server must be approved by the Application Product Manager before substitution. If there is a significant demand for a turnkey solution with a DC power supply, an Avaya GRIP (Global Requirements Integration Process) request must be submitted. Partners registered to use this process can submit a GRIP request at https://portal.avaya.com/apps/grip/partner.asp. Avaya Associates may assist and can find information about this process at http://spark4.avaya.com/grip. Note, a GRIP request must be made for the Avaya application product, not the server model. The decision on whether to include a turnkey offer with a DC power supply is the responsibility of each Avaya application Product Manager. The name of the Product Managers for each application is at the bottom of the application page on the Avaya Global Sales portal.

- Product labels on the servers themselves have the 9-digit base server codes for Avaya Services in service and support. These 9-digit codes differ from the 6-digit orderable codes under which servers are ordered. On every server package, there is a Packing Label and a Hierarchy Label. The Hierarchy Label itemizes the stock list in the box of the 6-digit orderable code and Avaya recommends retaining them for reference.
- Quality assurance – product integrity testing and environmental international restrictions were completed by HP and verified with Avaya using Design for Environmental Checklists. These lists include: batteries, printed wiring boards, plastic parts, product packaging, RoHS, green requirements, and energy efficiency.

How to use this document

This guide contains information for installing the Server as part of an Avaya deployment and provides:

- Instructions for how to find the appropriate online server documentation from HP.
- References to specific topics in standard HP documentation
- Suggested changes, details, and notes to assist the user in interpreting the manufacturer's documentation and to clarify Avaya's recommended implementation of the equipment
- Topics not covered in standard HP documentation, but which are necessary for successful installation and maintenance of Avaya products

Downloading HP documentation

Use this procedure to find and download the documentation.

Procedure

1. Open a browser and go to http://support.avaya.com.
2. Click **Downloads & Documents** from the menu at the top.
3. Enter `Common Servers` in the **Enter Your Product Here** field, and select 2.0.x from the **release** dropdown.
4. Select the **Documents** option, and click **Enter**.
5. Download the documents that you need.

HP DL360p G8 document set

See the following documents for HP DL360p server information and procedures.

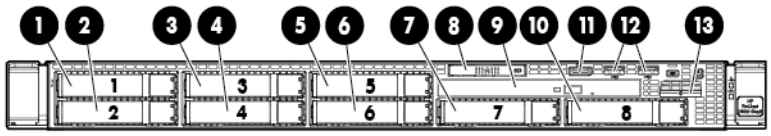
Documents

- HP ProLiant DL360p Gen8 Server User Guide
- HP ProLiant DL360p Gen8 Server Maintenance and Service Guide
- HP ProLiant Gen8 Troubleshooting Guide, Volume I: Troubleshooting
- HP ProLiant Gen8 Troubleshooting Guide, Volume II: Error Messages
- HP Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products

Documents included in the shipping container

Title	Part number
1U Rack Hardware Installation Instructions	365 494–004
Power Cord Strain Relief Kit	407 454–021
Assembly document set: • HP ProLiant Server Setup Poster • Important Safety Information • Limited Warranty and Material Limitations	660849–001 • 667798–002 • 377834–021 • 307797–029

Front-panel view



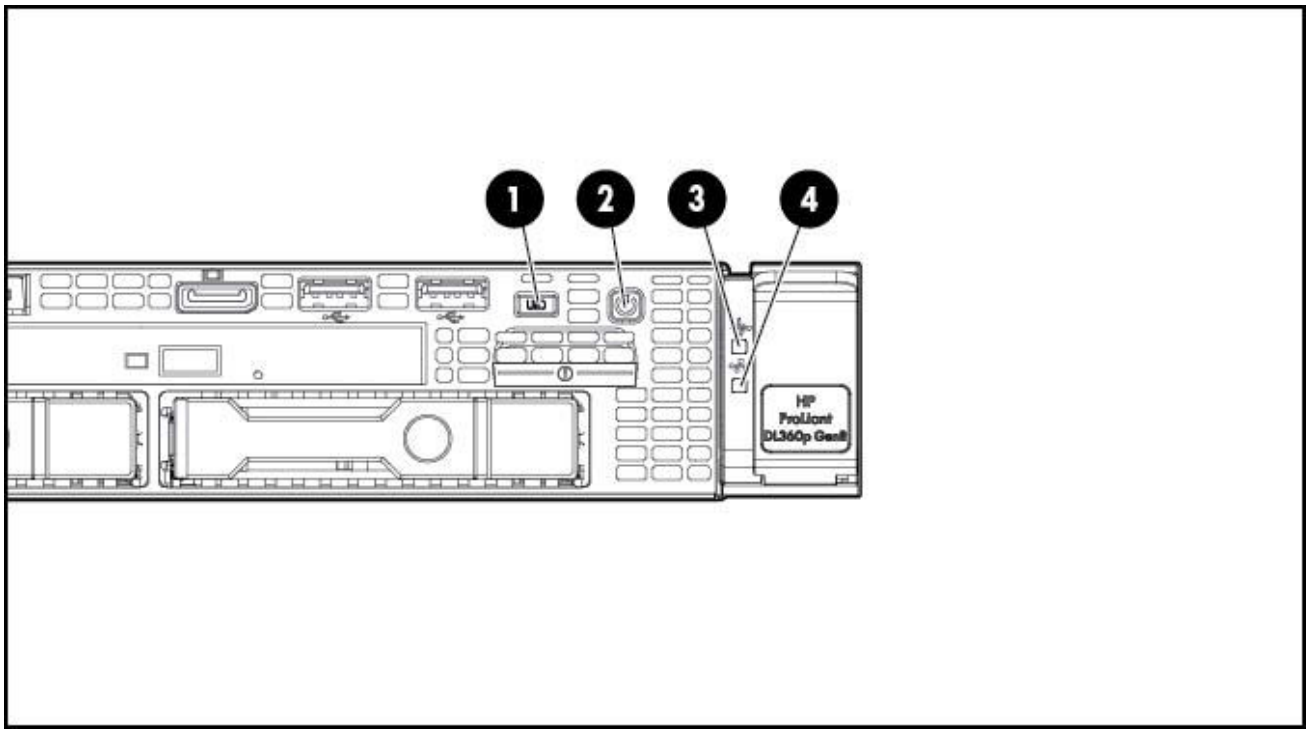
No.	Description
1	Hard Drive Bay
2	Hard Drive Bay
3	Hard Drive Bay
4	Hard Drive Bay
5	Hard Drive Bay
6	Hard Drive Bay
7	Hard Drive Bay

Table continues…

No.	Description
8	Slide-out System Insight Display (SID)
9	Optical Disk Drive Bay
10	Hard Drive Bay
11	Video connector (requires Front Video Adapter Kit)
12	Two (2) USB Connectors
13	Active Health and Network Status LEDs

Front panel LEDs

Use these LEDs to identify hardware status and problems.

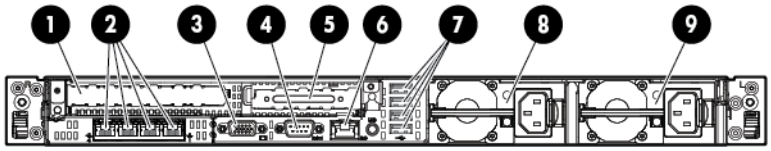


Item	Description	Status
1	UID LED/Button	Solid Blue = Identification is activated Flashing Blue = System is being managed remotely Off = Identification is deactivated
2	Power On/Standby Button/LED	Solid Green = System is on Flashing Green = Waiting for server power sequence Solid Amber = System is in standby, but power is still applied

Table continues…

Item	Description	Status
		Off = Power cord is not attached, power supply failure has occurred, no power supplies are installed, facility power is not available or the power button cable is disconnected
3	Health LED	Solid Green = System health is normal Flashing Amber = System health is degraded. To identify the component in a degraded state, see “Systems Insight Display LEDs (pg 75 in the Server Maintenance and Service Guide)” Flashing Red = System health is critical. To identify the component in a critical state, see “Systems Insight Display LEDs (pg 75).” If possible check iLO/BIOS logs. Also check application’s system log and SEL log from IPMI interface if possible. Fast Flashing Red = Power fault (check system and devices)
4	NIC Status LED	Solid Green = Link to network Flashing Green = Network activity Off = No network connection

Rear-panel view



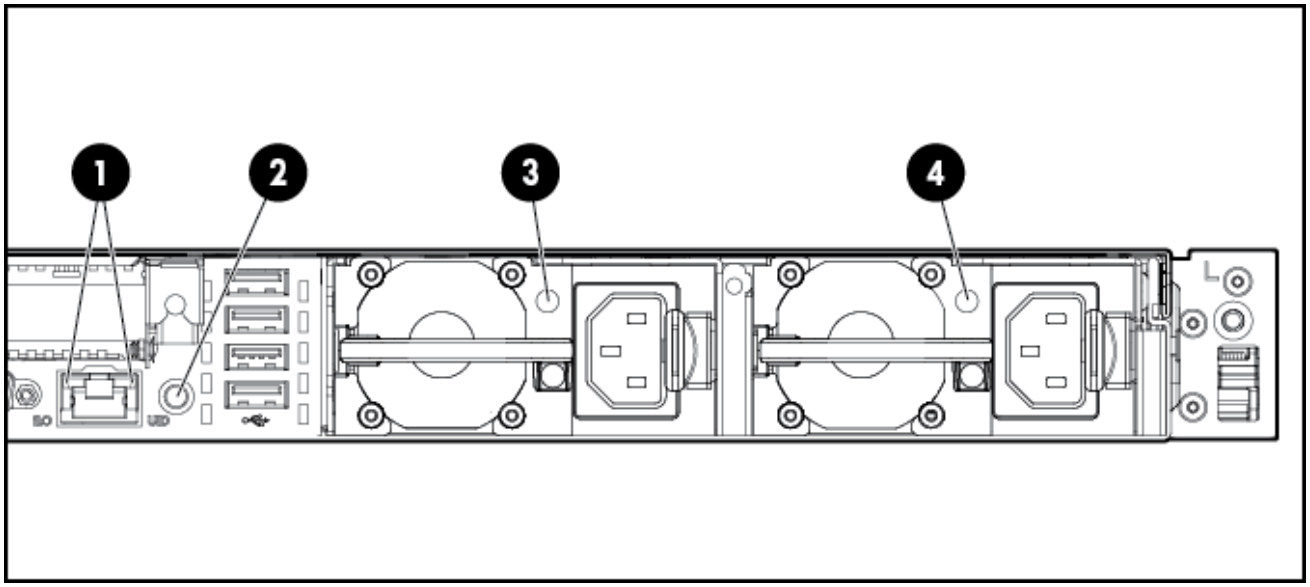
No.	Description
1	PCIe 3.0 Full height/half length x16 expansion slot
2	Flexible LOM ports (Shown: 4 ports 1 Gb each) The HP DL360p G8 server ports are labeled 1 to 4 from right to left.
3	Video connector
4	Serial connector
5	PCIe 3.0 Low Profile x8 expansion slot
6	iLO Management Engine NIC connector
7	Four (4) USB connectors

Table continues…

No.	Description
8	Power supply bay 2 (Shown populated: Optional Power Supply for Redundant Power)
9	Power supply bay 1 (Primary Power Supply)

Rear panel LEDs

Use these LEDs to identify hardware status and problems.



Item	Description	Status
1 (left)	HP iLO/Standard NIC activity LED	Solid Green = Activity exists Flashing Green = Activity exists Off = No activity exists
1 (right)	HP iLO/Standard NIC link LED	Solid Green = Link exists Off = No link exists
2	UID button/LED	Solid Blue = Identification is activated Flashing Blue = System is being managed remotely Off = Identification is deactivated
3	Power supply 2 LED	Solid Green = Normal Off = One or more of the following conditions exists: • AC power unavailable • Power supply failed • Power supply in standby mode

Table continues…

Item	Description	Status
		• Power supply exceeded current limit
4	Power supply 1 LED	Solid Green = Normal Off = One or more of the following conditions exists: • AC power unavailable • Power supply failed • Power supply in standby mode • Power supply exceeded current limit

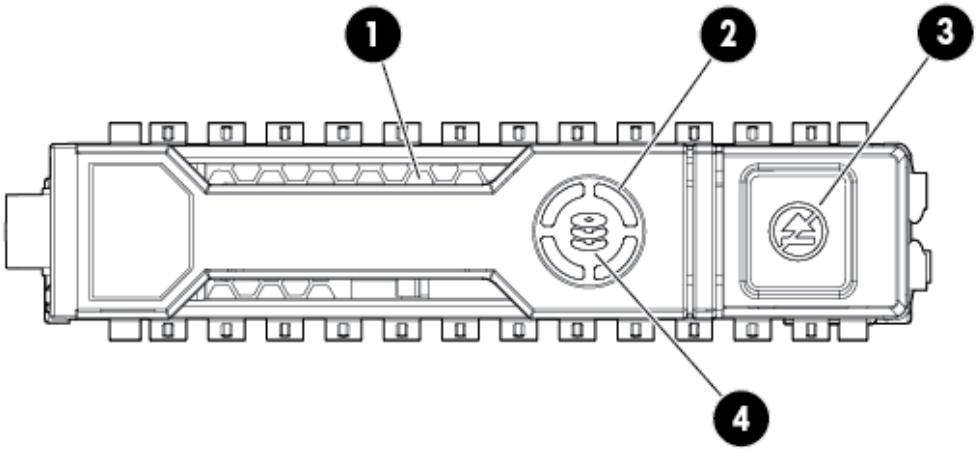
External server components

Part number	Description	Hot-swappable?
700506773	DL360p G8 SRVR 300GB 10K SAS 2.5” HDD	Y
700506781	DL360p G8 SRVR 300GB 15K SAS 2.5” HDD	Y
700506782	DL360p G8 SRVR 900GB 10K SAS 2.5” HDD	Y
700506770	DL360p G8 SRVR PWR Supply 460W AC, CS Gold Ht Power Supply	Y, if redundant
700506775	DL360p G8 SRVR PWR Supply 750W AC, CS Gold Ht Power Supply	Y, if redundant
700506776	DL360p G8 SRVR PWR Supply 750W DC, CS-48VDC Ht Power Supply	Y, if redundant

Hard disk drive problems

Hard drive LEDs

Use these indicators to identify status and problems with a hard drive.



Item	LED	Status	Definition	Avaya recommendations and information
1	Locate	Solid blue	The drive is being identified by a host application	This is normal operation if application supports this feature or if disk array is being created/ selected.
		Flashing blue	The drive carrier firmware is being updated or requires an update	Check support.avaya.com for HP DL360p G8 firmware updates. View release notes for Avaya firmware update inclusions for HDD update.
2	Activity ring	Rotating green	Drive activity	This is normal operation and indicates that the drive is currently operating as part of the RAID array.
		Off	No drive activity	This indicates that the drive may currently have no activity or is not part of the RAID array.
3	Do not remove	Solid white	Do not remove the drive. Removing the drive causes one or more of the logical drives to fail.	This indicates that the RAID array is operating in degraded mode because one of the drives in the array has failed or is currently rebuilding. Removing a drive in this state will destroy the logical drive array. If the array is currently rebuilding this status will clear when the new replacement drive has rebuilt. Rebuild can take from 20 minutes up to 2 hours depending on the size of drive and activity of the system.
		Off	Removing the drive does not cause a logical drive to fail.	If an active drive is removed, the other drives that are part of the array will indicate a status of “do not remove”.
4	Drive status	Solid green	The drive is a member of one or more logical drives	This indicates normal operation.
		Flashing green	The drive is rebuilding or performing a RAID migration, stripe size migrations, capacity expansion, or logical drive extension, or is erasing.	A newly inserted replacement drive should start this LED pattern within 10-15 seconds of insertion to indicate a rebuild of the logical drive. If action does not start, unplugging and reinserting new drive can be performed.
		Flashing amber/ green	The drive is a member of one or more logical drives and predicts the drive will fail.	This signature indicates future failure and drive should be replaced asap.

Table continues…

Item	LED	Status	Definition	Avaya recommendations and information
		Flashing amber	The drive is not configured and predicts the drive will fail	The drive must be replaced ASAP if it is needed for current array.
		Solid amber	The drive has failed	The drive must be replaced ASAP.
		Off	The drive is not configured by a RAID controller	Reinsert drive if expected to rebuild as part of array. If no LED activity continues, try another unused drive if possible. Tools to recreate the RAID array can be accessed at support.avaya.com. If a new array is created all data from the previous array will be destroyed.

Hard disk drive problems

Symptoms

Some possible symptoms indicating hard drive problems are:

- Drives have failed as indicated by HDD LEDs (Hard drive LEDs on page 179) or alarmed by Avaya application.
- There is an active disk drive failure alarm from an Avaya application
- Drives are not recognized by Avaya application
- Data is inaccessible
- Server response time is slower than usual

HP documentation reference(s)

Troubleshooting Guide Volume 1: SAS, SATA, and SSD drive guidelines

Troubleshooting Guide Volume 1: Drive problems (hard drives and solid state drives)

Helpful guidelines

When adding drives to the server, observe the following general guidelines:

- Drives must be the same capacity to provide the greatest storage space efficiency when drives are grouped together into the same drive array.
- Drives in the same logical volume must be of the same type. ACU does not support mixing SAS, SATA, and SSD drives in the same logical volume.

Troubleshooting a hard disk drive

About this task

Follow the steps below to troubleshoot hard drive problems on one of these drives:

- DL360p G8 SRVR 300GB 10K SAS 2.5” HDD
- DL360p G8 SRVR 300GB 15K SAS 2.5” HDD
- DL360p G8 SRVR 900GB 10K SAS 2.5” HDD

Procedure

1. Be sure there are no loose connections, and all drives are fully seated.
2. Check HDD LEDs for indication of possible problems. See hard drive LED section.
3. Be sure drive blanks are installed properly when the server is operating. Drives may overheat and cause sluggish response or drive failure.
4. Be sure the replacement drives within an array are the same size or larger.
5. Be sure the replacement drives within an array are the same drive type, such as SAS, SATA, or SSD
6. Power cycle the server. Shutdown server according to Avaya application procedures.
7. Check support.avaya.com to see if a firmware update is available from Avaya for this model of server. View notes to see if firmware update is applicable to the observed problem before applying the update.

Next steps

If the part is defective, continue with the following removal and replacement procedures.

Replacing a hard disk drive

Before you begin

Best practice is to ensure the customer has a good separate backup of their system data before performing any maintenance on the server.

About this task

Follow the steps below to replace one of these drives:

- DL360p G8 SRVR 300GB 10K SAS 2.5” HDD
- DL360p G8 SRVR 300GB 15K SAS 2.5” HDD
- DL360p G8 SRVR 900GB 10K SAS 2.5” HDD

Procedure

1. Remove the drive.
    a. Push button to release locking latch. (#1 in the following image)
    b. Pull on unlocked latch to remove HDD. (#2 in the following image)

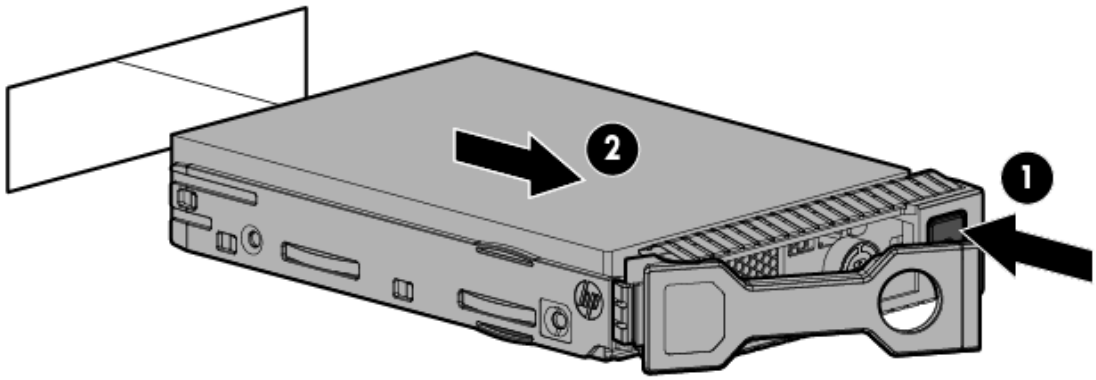


Figure 9: Removing hard disk drive

Drives are hot-swappable so power down of server is not recommended, however only one drive should be replaced at a time until RAID array rebuild is complete.

2. Replace the drive.
   a. Insert HDD into empty drive slot.
   b. Secure HDD by closing the latch.
   c. Refer to the Hard Drive LED table for the drive rebuild status.
   d. Check using Avaya application tools for RAID status if available.

Power supply problems

Symptoms

Some possible symptoms indicating power supply problems are:

- The server does not power on.
- The system power LED is off or solid amber. Front panel LEDs on page 176
- The health LED Front panel LEDs on page 176 is solid red, flashing red, solid amber, or flashing amber.

HP documentation reference(s)

Troubleshooting Guide Volume 1: Power Source Problems

Troubleshooting Guide Volume 1: Power Supply Problems

Troubleshooting Guide Volume 1: Power on Problems Flowchart

Possible Causes

List of possible causes for the above symptoms:

- Improperly seated or faulty power supply
- Loose or faulty power cord
- Power source problem

- Improperly seated component or interlock problem

If the power supply LED is off, it could mean any of the following:

- AC power unavailable
- Power supply failed
- Power supply in standby mode
- Power supply exceeded current limit

Troubleshooting a power supply

About this task

Follow the steps below to troubleshoot and replace one of these power supplies:

- DL360p G8 SRVR PWR Supply 460W AC, CS Gold Ht Power Supply
- DL360p G8 SRVR PWR Supply 750W AC, CS Gold Ht Power Supply
- DL360p G8 SRVR PWR Supply 750W DC, CS-48VDC Ht Power Supply

Table 5: Power supply LEDs

System Power LED	Definition
Off (Server)	System has no power
Solid Amber	System is in standby, Power On/Standby Button service is initialized
Flashing Green	System is waiting to power on; Power On/Standby button is pressed
Solid Green	System is powered on

Procedure

1. To troubleshoot possible power source problems:
   a. Plug another device into the grounded power outlet to be sure the outlet works. Also, be sure the power source meets applicable standards.
   b. Replace the power cord with a known functional power cord to be sure it is not faulty.
   c. Replace the power strip with a known functional power strip to be sure it is not faulty.
   d. Have a qualified electrician check the line voltage to be sure it meets the required specifications.
   e. Be sure the proper circuit breaker is in the On position.

   If power source is not the problem, continue with steps below to troubleshoot power supplies.
2. Be sure no loose connections exist.
3. Press the Power On/Standby button to be sure it is on. If the server has a Power On/Standby button that returns to its original position after being pressed, be sure you press the switch firmly. For more information about system power LED status, see Rear panel LEDs on page 178.

4. Check the Systems insight display LEDs on page 186.
5. Check the power supply LEDs, be sure they indicate that each power supply is working properly. If the LEDs indicate a problem with a power supply (red, amber, or off), then check the power source. If the power source is working properly, then replace the power supply.
6. If running a redundant configuration, be sure that all of the power supplies in the system have the same spare part number and are supported by the server.

Next steps

If the part is defective, continue with the following removal and replacement procedures.

Replacing a power supply

About this task

Follow the steps below to replace one of these power supplies:

- DL360p G8 SRVR PWR Supply 460W AC, CS Gold Ht Power Supply
- DL360p G8 SRVR PWR Supply 750W AC, CS Gold Ht Power Supply
- DL360p G8 SRVR PWR Supply 750W DC, CS-48VDC Ht Power Supply

Procedure

1. If system does not have redundant power, shut down server according to Avaya application procedures. (Server may already be down because of failed power supply)
   - If server does not power down according to normal shutdown procedures, press and release the Power On/Standby button. This method initiates a controlled shutdown of applications and the OS before the server enters standby mode.
   - Press and hold the Power On/Standby button for more than 4 seconds to force the server to enter standby mode. This method forces the server to enter standby mode without properly exiting applications and the OS. If an application stops responding, you can use this method to force a shutdown, but be aware that file corruption could occur using this method.
2. Replace failed power supply.
   a. Press tab (1 in the following figure)
   b. Pull supply out (2 in the following figure)
   c. Install new supply

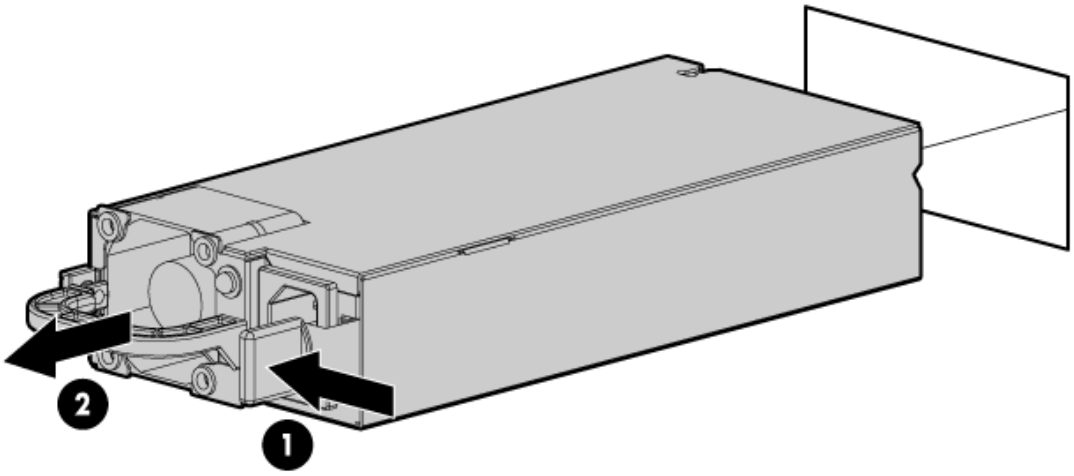


Figure 10: Replacing power supply

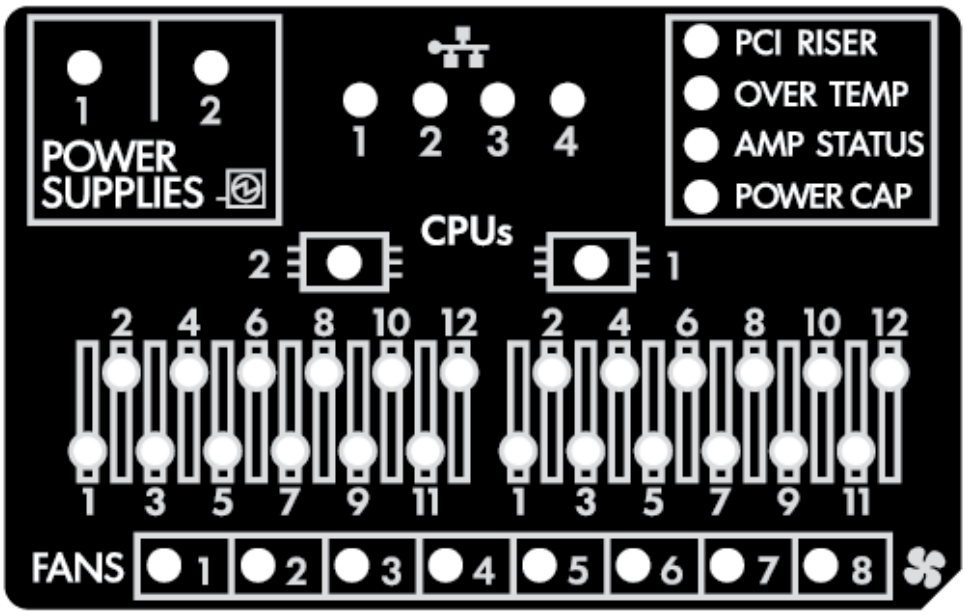
3. Connect the power cable(s) to the power supply (if disconnected)
4. Power up the server (if powered down)

Internal server components

Part number	Description
700506778	DL360p G8 SRVR DVD-R/W Drive HP 9.5mm SATA
700506777	DL360p G8 SRVR Dual Port PCIe 1GB NIC
700506779	DL360p G8 SRVR FAN FRU
700506774	DL360p G8 SRVR 4 GB Memory RDIMM
700506771	DL360p G8 SRVR Super Cap RAID Battery

HP DL360p G8 systems insight display LEDs

Use this display to identify hardware status and problems with the server.



Description	Status
Processor LEDs	Off = Normal Amber = Failed Processor
DIMM LEDs	Off = Normal Amber = Failed DIMM or configuration issue
Fan LEDs	Off = Normal Amber = Failed fan or missing fan
NIC LEDs	Off = No link to network Solid Green = Network Link Flashing Green = Network link with activity If power is off, the front panel LED is not active. For status, see “Rear panel LEDs and buttons (pg 71 Server Maintenance and Service Guide)
Power Supply LEDs	Off = Normal Amber = Failed power supply
PCI Riser LED	Off = Normal Amber = Incorrectly installed PCI riser board

Table continues…

Description	Status
Over Temp LED	Off = Normal Amber = High system temperature detected
Amp Status LED	Off = Disabled Solid Green = Advanced Memory Protection active Solid Amber = Memory failure has occurred Flashing Amber = Invalid AMP memory configuration
Power Cap LED	Off = System is in standby, or no cap is set Solid Green = Power cap applied

DVD-RW problems

Symptoms

- System does not boot from the drive
- Data read from the drive is inconsistent, or drive cannot read data
- Drive is not detected

HP documentation reference(s)

Troubleshooting Guide Volume 1: Internal system problems

Troubleshooting Guide Volume 1: CD - ROM and DVD drive problems

Troubleshooting a DVD-R/W drive

About this task

Follow the steps below to troubleshoot a DL360p G8 SRVR DVD-R/W Drive HP 9.5mm SATA.

Warning:

Eliminate the risk of electric shock by removing all AC power from the system before installing or replacing any non hot-plug hardware option. Disconnect all power cords to completely remove power from the server. Always follow Avaya's application procedures when shutting down the server.

Warning:

To reduce the risk of personal injury from hot surfaces, allow the drives and the internal system components to cool before touching them.

Procedure

1. If system is not booting from drive:
   a. Be sure there are no loose connections
   b. Be sure the media from which you are attempting to boot is not damaged and is a bootable CD or DVD.
   c. If possible, be sure the drive boot order in BIOS is set so that the server boots from the CD -ROM drive first.

2. If data read from drive is inconsistent:
    a. Clean the drive and media.
    b. If a paper or plastic label has been applied to the surface of the CD or DVD in use, remove the label and any adhesive residue.
3. If drive is not detected:
    a. Be sure there are no loose connections.
    b. Be sure the cables are working properly. If possible, replace with known functional cables to test whether the original cables were faulty.

Next steps

If the part is defective, continue with the following removal and replacement procedures.

Replacing a DVD-R/W drive

About this task

Follow the steps below to replace a DL360p G8 SRVR DVD-R/W Drive HP 9.5mm SATA.

Warning:

Eliminate the risk of electric shock by removing all AC power from the system before installing or replacing any non hot-plug hardware option. Disconnect all power cords to completely remove power from the server. Always follow Avaya's application procedures when shutting down the server.

Warning:

To reduce the risk of personal injury from hot surfaces, allow the drives and the internal system components to cool before touching them.

Procedure

1. Power down the server
2. Remove all power:
    - Disconnect each power cord from the power source.
    - Disconnect each power cord from the server.
3. Extend the server from the rack
4. Remove the access panel
5. If installed, remove the FBWC capacitor pack.
6. For an SFF DVD drive, do the following:
    a. Disconnect the SATA DVD cable from the system board to fully remove the DVD drive from the bay by removing Torx screws (1) and then pulling out DVD drive (2). The Torx service tool is located inside server next to the power supply housing.
    b. Remove the DVD drive from the server.

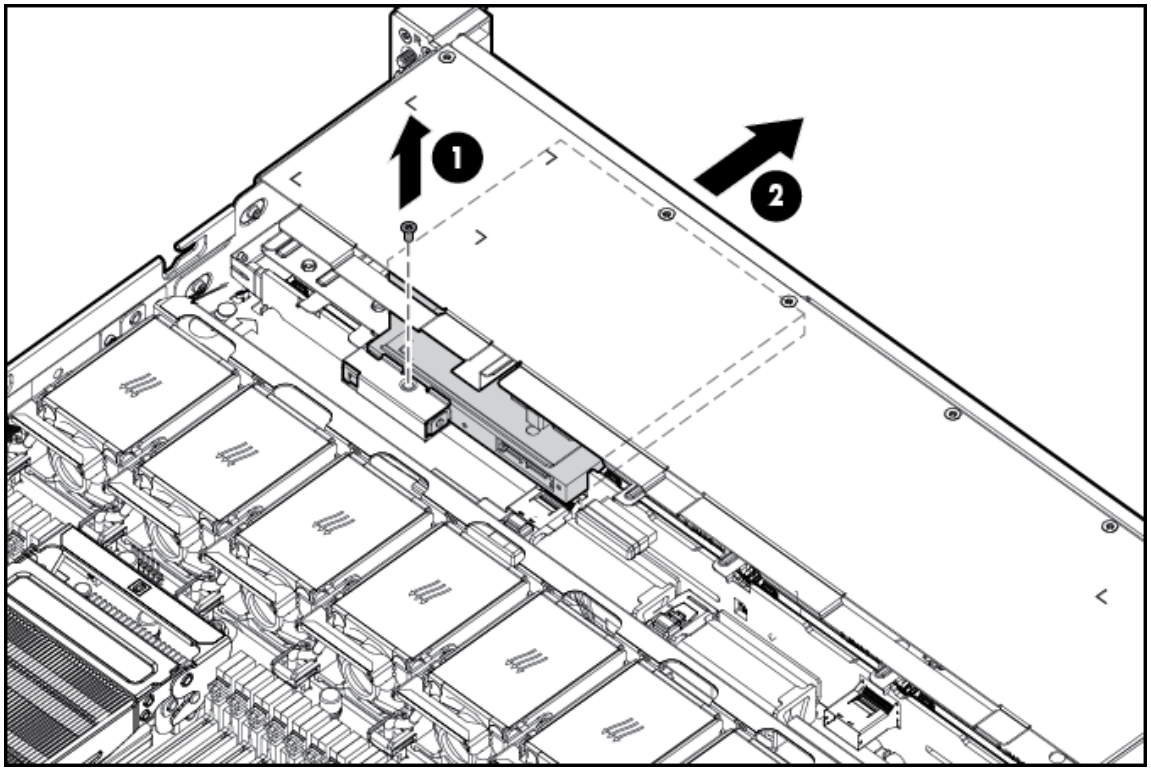


Figure 11: Removing a DVD R/W drive

c. Disconnect the SATA DVD cable from the rear of the DVD drive.

7. Remove the bezel blank from the DVD - ROM bay (refer to appropriate users guide section).

To insert DVD drive:

8. For an SFF DVD drive, do the following:
   a. Install the DVD drive using the screws from this kit and a T - 10/T - 15 Torx screwdriver.
   b. Connect the cable to the rear of the drive and to the SATA DVD - ROM drive connector on the system board.
   c. Clip the cable to the power supply air baffle when routing it along the edge of the system board.
9. Install the access panel
10. Slide the server into the rack.
11. Connect each power cord to the server.
12. Connect each power cord to the power source.
13. Power up the server

NIC problems

Symptoms

- Network controller or FlexibleLOM is installed but not working.
- Network controller or FlexibleLOM has stopped working.
- Network controller or FlexibleLOM stopped working when an expansion board was added

HP documentation reference(s)

Troubleshooting Guide Volume 1: Network controller or FlexibleLOM problems

Server Maintenance and Service Guide: FlexibleLOM

Troubleshooting a NIC

About this task

Follow the steps below to troubleshoot the DL360p G8 SRVR Dual Port PCIe 1GB NIC or DL360p G8 SRVR 1GbE 4-port 331FLR Adapter FIO kit.

Note:

Always follow safe electrostatic discharge practices.

Procedure

1. Check the network controller or FlexibleLOM LEDs to see if any statuses indicate the source of the problem. For NIC LED status information see theSystems insight display LEDs on page 186 or NIC jack LED status.
2. Be sure there are no loose connections.
3. Be sure the correct cable type is used for the network speed or that the correct SFP or DAC cable is used. For dual - port 10GB networking devices, both SFP ports should have the same media (for example, DAC cable or equal SFP+ module). Mixing different types of SFP (SR/LR) on a single device is not supported.
4. Be sure the network cable is working by replacing it with a known functional cable.
5. Be sure a valid IP address is assigned to the controller and that the configuration settings are correct according to Avaya's application documentation.

Next steps

If the part is defective, continue with the following removal and replacement procedures.

Replacing a NIC

About this task

Follow the steps below to replace the DL360p G8 SRVR Dual Port PCIe 1GB NIC or DL360p G8 SRVR 1GbE 4-port 331FLR Adapter FIO kit.

Note:

Always follow safe electrostatic discharge practices.

Procedure

1. Power down the server according to Avaya's application instructions.
2. Remove all power:
   a. Disconnect each power cord from the power source.
   b. Disconnect each power cord from the server.
3. Remove any attached network cables.
4. Extend the server from the rack
5. Remove the access panel
6. Loosen the thumbscrew.
7. Remove the existing FlexibleLOM
   a. Loosen the thumbscrew (1 on the following image).
   b. Remove the Flexible LOM (2 on the following image).

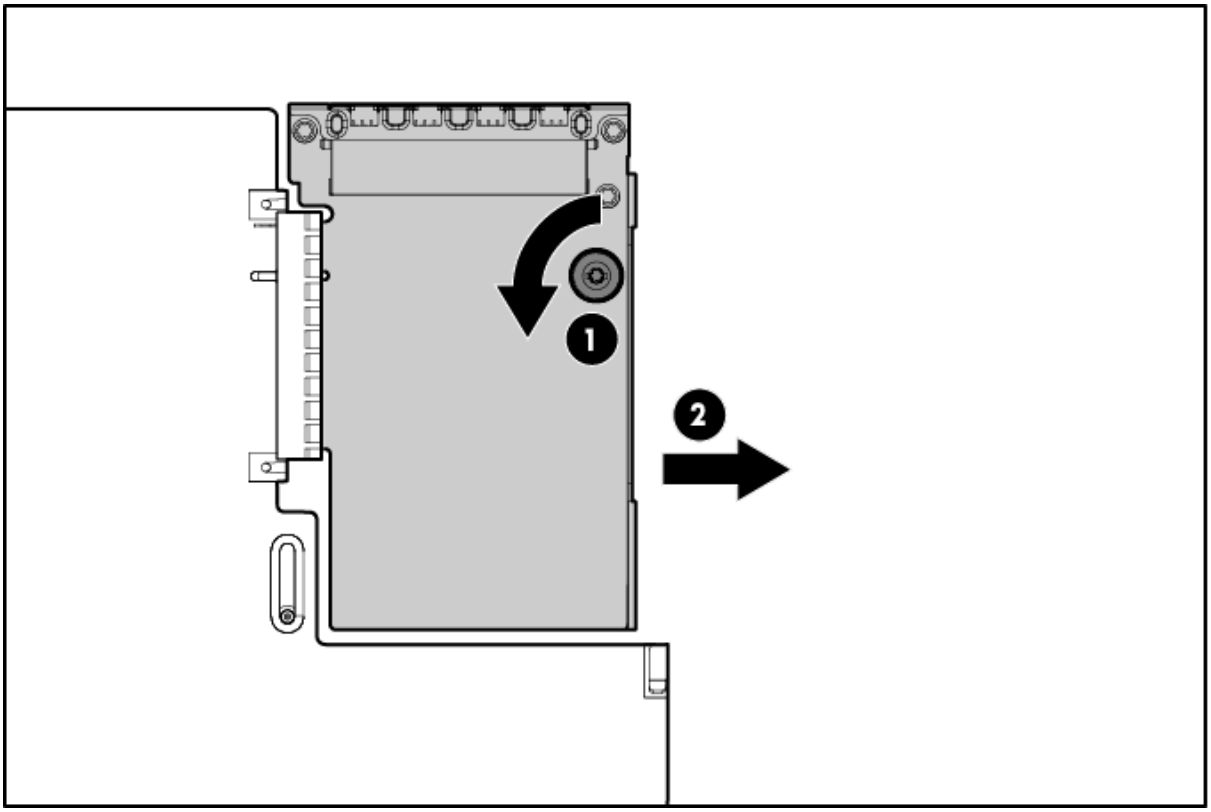


Figure 12: Removing flexible LOM

8. To replace the component, firmly seat the FlexibleLOM in the slot, and then tighten the thumbscrew.
9. To replace the dual port PCIe 1GB NIC follow the expansion board removal instructions. PCIe riser card assembly on page 193

10. Install the access panel
11. Slide the server into the rack.
12. Connect the LAN segment cables.
13. Connect each power cord to the server.
14. Connect each power cord to the power source.
15. Power up the server

Working with a PCIe riser card assembly

About this task

Use this procedure when adding or removing NIC cards.

Note:

Always follow safe electrostatic discharge practices.

Procedure

1. Power down the server according to Avaya's application instructions.
2. Remove all power:
    a. Disconnect each power cord from the power source.
    b. Disconnect each power cord from the server.
3. Extend the server from the rack
4. Remove the access panel
5. Remove the PCIe riser cage.
    a. Flip fasteners up (#1 in following image)
    b. Turn fasteners 180 degrees (#2 in following image)
    c. Lift cage straight up (#3 in following image)

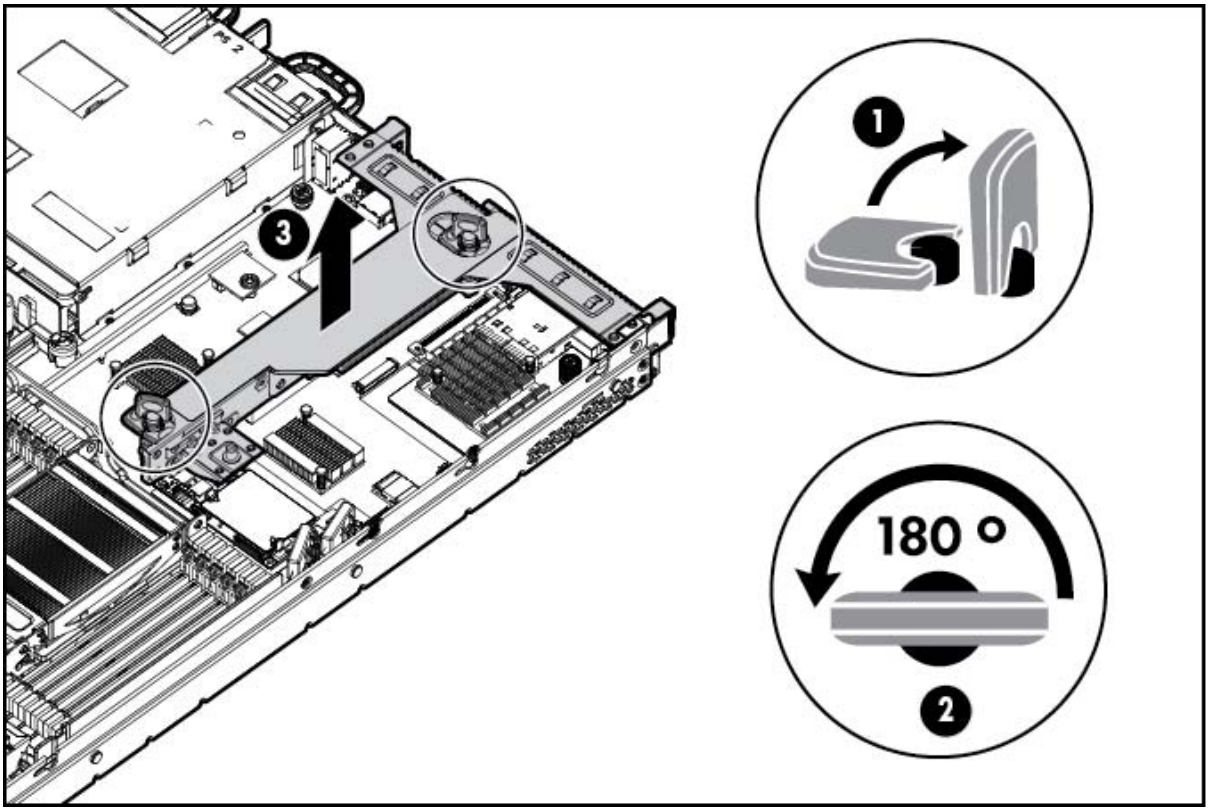


Figure 13: Removing PCIe riser cage

6. Remove any installed expansion boards.

   Note:

   If you are not replacing the expansion board, replace the screw into the PCIe riser cage before installing the PCIe riser cage back into the server.

7. Remove the PCIe riser board.
   a. Remove screws (#1 in following images)
   b. Remove board (#2 in following images)

   Note:

   The x16 PCIe riser board has two screws to remove from the assembly and the x8 PCIe riser board has three screws to remove from the assembly.

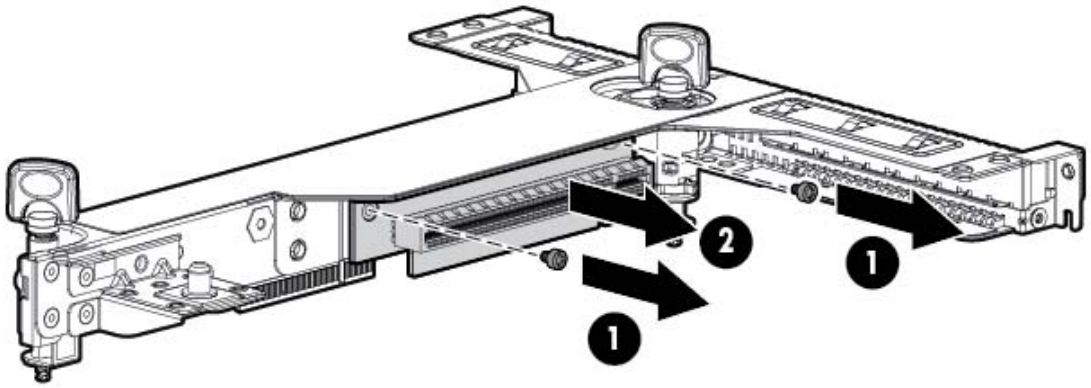


Figure 14: Right side, expansion slot 2 PCIe x16, half-height half-length

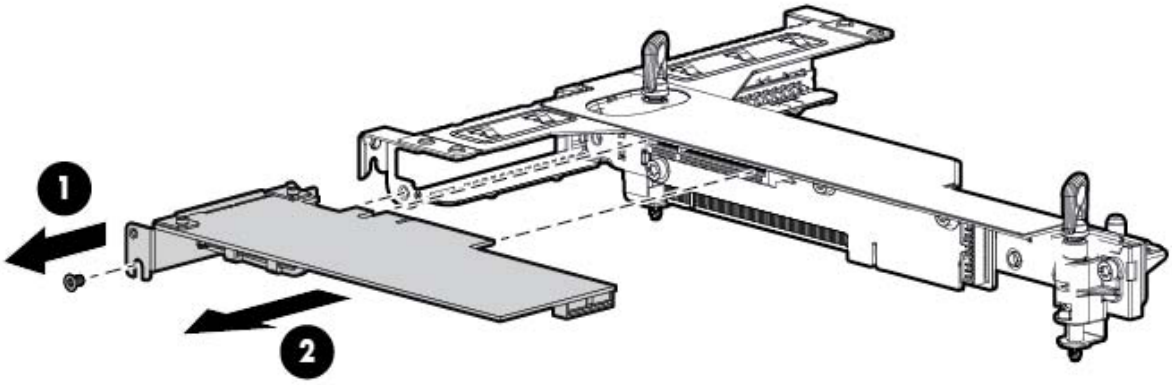


Figure 15: Left side, expansion slot 1 PCIe x8, low profile

8. To replace the component, reverse the removal procedure.

Important:

The server does not power up if the PCI riser cage is not seated properly.

Thermal (fan) problems

Symptoms

- Server powers up but quickly shuts down
- Insight display LEDs indicate a fan failure

- Avaya application alarms fan failure

Note:

For servers with redundant fans, backup fans may spin up periodically to test functionality. This is part of normal redundant fan operation.

HP documentation reference(s)

Troubleshooting Guide Volume 1: Hot - plug fan problems are occurring

Server Maintenance and Service Guide: Fan Module

Troubleshooting thermal fans

About this task

Follow the steps below to troubleshoot the DL360p G8 SRVR FAN FRU.

Note:

Always follow safe electrostatic discharge practices.

Procedure

1. Be sure the fans are properly seated and working.
   a. Follow the procedures and warnings in the server documentation for removing the access panels and accessing and replacing fans.
   b. Unseat, and then reseat, each fan according to the proper procedures.
   c. Replace the access panels, and then attempt to restart the server.
2. Be sure all fan slots have fans or blanks installed.

   Note:

   The server has eight fans. Install fans 1 and 2 only when processor 2 is installed. When only one processor is installed, install the fan blanks in bays 1 and 2.
3. Be sure no ventilation problems exist. If you have been operating the server for an extended period of time with the access panel removed, airflow may have been impeded, causing thermal damage to components.
4. Verify the fan airflow path is not blocked by cables or other material.
5. Be sure no POST error messages are displayed while booting the server that indicate temperature violation or fan failure information.
6. Check the LEDs to be sure the hot - plug fans are working.
7. Be sure hot - plug fan requirements are being met

Next steps

If the part is defective, continue with the following removal and replacement procedures.

Replacing thermal fans

About this task

Follow the steps below to replace the DL360p G8 SRVR FAN FRU.

Note:

Always follow safe electrostatic discharge practices.

Procedure

1. Replace any required non - functioning fans and restart the server if necessary. Fans are hot-swappable.
2. To remove the component:
   a. Extend the server from the rack. If the server is to remain on with application up, ensure power cord does not disconnect when extending server from rack.
   b. Remove the access panel
   c. Remove the fan module.

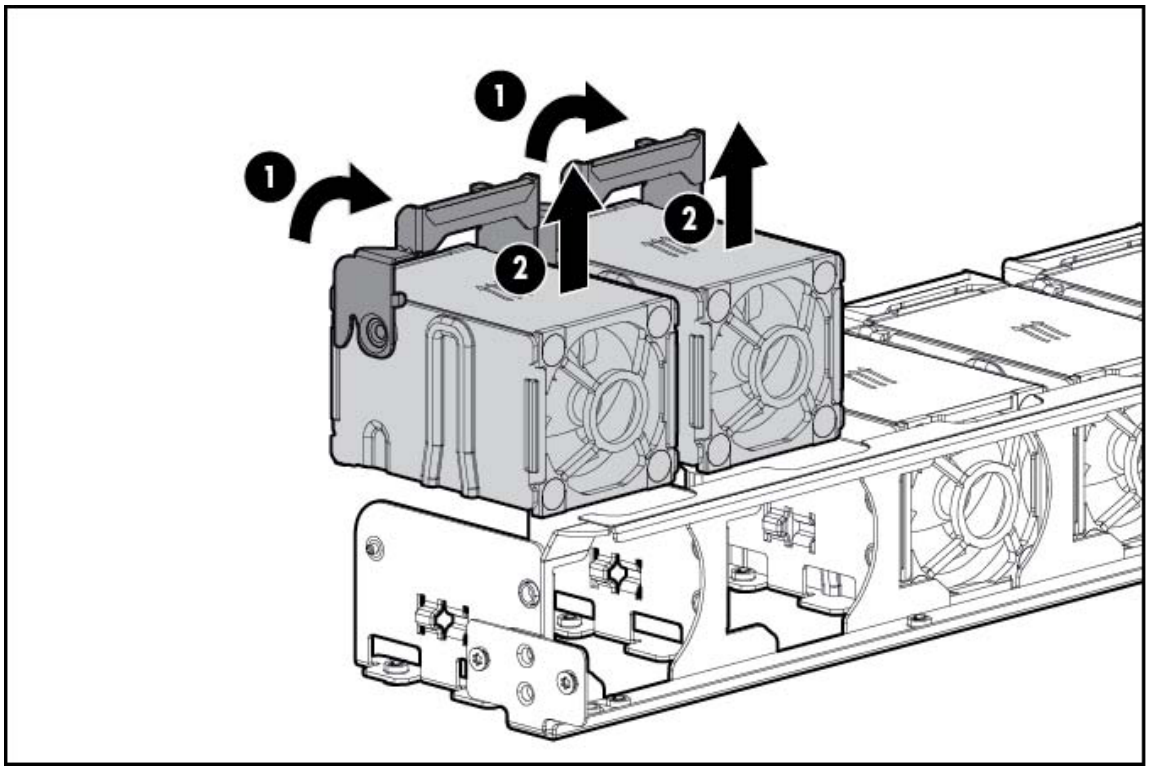


Figure 16: Removing fans

Caution:

To avoid server shutdown, a fan must be replaced within 60 seconds of being removed.

3. To replace the component:
   a. Install the Fan Module

b. Install the access panel

c. Slide the server into the rack.

DIMM problems

Symptoms

- General memory problems are occurring
- Server is out of memory
- Memory count error exists
- Server fails to recognize existing memory
- Server fails to recognize new memory

HP documentation reference(s)

Troubleshooting Guide Volume 1: DIMM Handling Guidelines

Server Maintenance and Service Guide: DIMMS

Helpful Guidelines

- Always follow safe ESD practices
- Avoid electrostatic discharge
- Always hold DIMMs by the side edges only.
- Avoid touching the connectors on the bottom of the DIMM.
- Never wrap your fingers around a DIMM.
- Avoid touching the components on the sides of the DIMM.
- Never bend or flex the DIMM.

Troubleshooting memory DIMMs

About this task

Follow the steps below to troubleshoot a DL360p G8 SRVR 4 GB Memory RDIMM.

Procedure

1. If general memory problems are occurring:
   a. Check system insight display for any memory error LEDs.
   b. Isolate and minimize the memory configuration.
   c. Check any server LEDs that correspond to memory slots.
   d. View power-up screen for any memory errors displayed if monitor is installed.
   e. If you are unsure which DIMM has failed, test each bank of DIMMs by removing all other DIMMs. Then, isolate the failed DIMM by switching each DIMM in a bank with a known working DIMM. Start installing CH1A first and then proceed to install CH2B, second and continue to populate in that order.
   f. Remove any third – party memory.

g. To test the memory, run HP Insight Diagnostics (Troubleshooting Guide Volume 1, pg 68). A keyboard and mouse are required.

2. If the server is out of memory:
   a. Be sure no operating system errors are indicated.
   b. Be sure a memory count error did not occur. Refer to the message displaying memory count during POST. This can only be viewed with monitor and keyboard.
3. If a memory count error exists, a possible cause is that the memory modules are not installed correctly.
   a. Be sure the memory modules are supported by the server.
   b. Be sure the memory modules have been installed correctly in a supported configuration.
   c. Be sure the memory modules are seated properly
   d. Be sure no operating system errors are indicated.
   e. Restart the server and check to see if the error message is still displayed.
   f. Run HP Insight Diagnostics (Troubleshooting Guide Volume 1, pg 68). Then, replace failed components as indicated
4. If the server fails to recognize existing memory:
   a. Reseat the memory.
   b. Be sure the memory is configured properly.
   c. Be sure a memory count error does not occur. See the message displaying memory count during POST. This can only be viewed with monitor and keyboard.
5. If the server fails to recognize new memory:
   a. Be sure the memory is the correct type for the server and is installed according to the server requirements.
   b. Be sure you have not exceeded the memory limits of the server or operating system.
   c. Be sure the memory is seated properly
   d. If possible test the memory by installing the memory into a known working server. Be sure the memory meets the requirements of the new server on which you are testing the memory.

Next steps

If the part is defective, continue with the following removal and replacement procedures.

Replacing memory DIMMs

About this task

Follow the steps below to replace a defective DL360p G8 SRVR 4 GB Memory RDIMM.

Procedure

1. Power down the server

2. Remove all power:
   a. Disconnect each power cord from the power source.
   b. Disconnect each power cord from the server.
3. Extend the server from the rack
4. Remove the access panel
5. Remove the DIMM

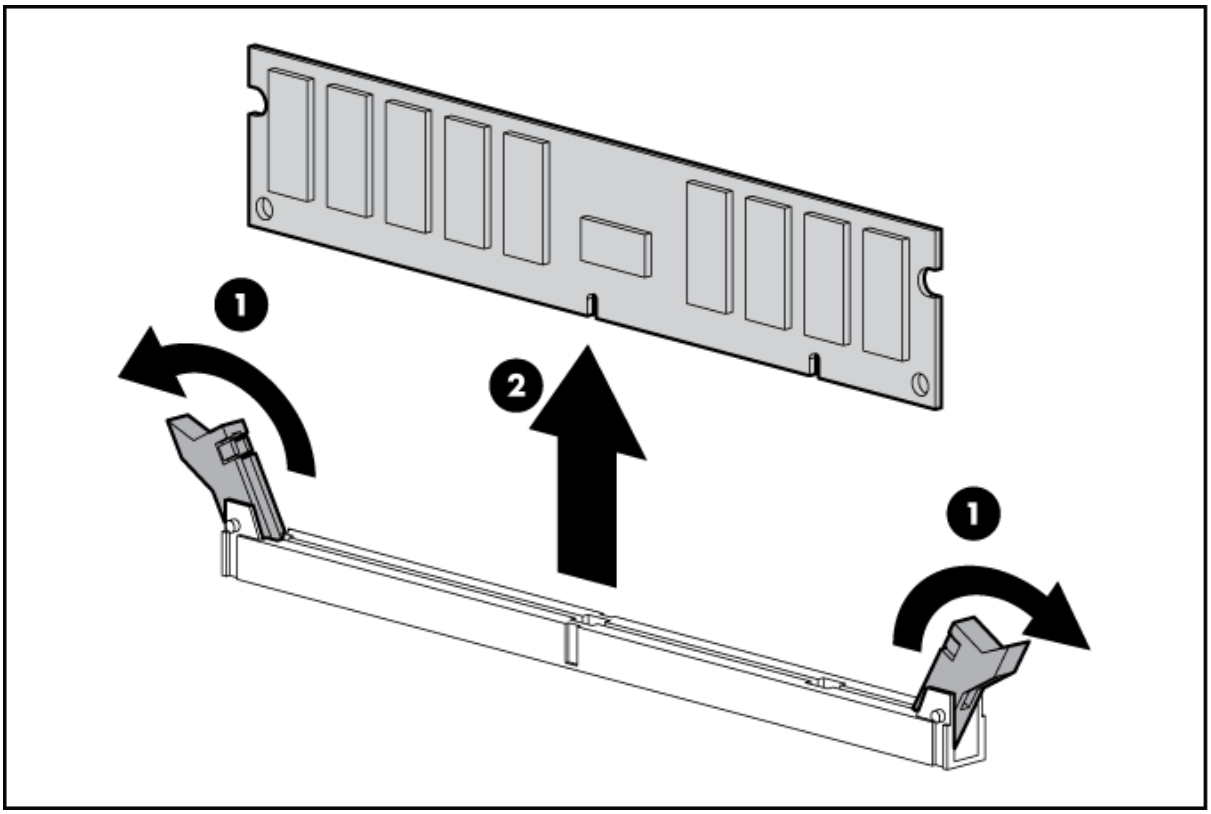


Figure 17: Removing DIMM

6. To replace the component, reverse the removal procedure.

Contacting Avaya Services

Avaya provides a telephone number to report problems or to ask questions about your product:

- The support telephone number is 1–800–242–2121 in the United States.
- For additional support telephone numbers, see the Avaya Website: http://www.avaya.com/support.

Troubleshooting the HP ProLiant DL360 G7 hardware

This section describes how to manage and resolve problems with the HP ProLiant DL360 G7 hardware and provides:

- instructions for how to find the appropriate online server documentation from HP
- references to specific topics in standard HP documentation
- suggested changes, details, and notes to assist you in interpreting the manufacturer's documentation and to clarify Avaya's recommended implementation of the equipment
- additional topics not covered in standard HP documentation but which are necessary for maintaining and troubleshooting the Avaya installation

Warning:

Read the applicable sections in the HP documentation and become familiar with the procedures before replacing hardware components or units. Ensure replacement components or units reference documentation is available prior to starting any replacement procedures. For some hardware, you must stop, start, or reinstall the applications when you replace the hardware. Outages can occur if you do not follow instructions completely.

HP DL360 document set

See the following documents for HP DL360 server information and procedures.

Documents

- HP ProLiant Servers Safety Information
- HP ProLiant DL360 G7 Server Maintenance and Service Guide
- HP ProLiant Servers Troubleshooting Guide
- HP ProLiant DL360 G7 Server User Guide

Documents included in the shipping container

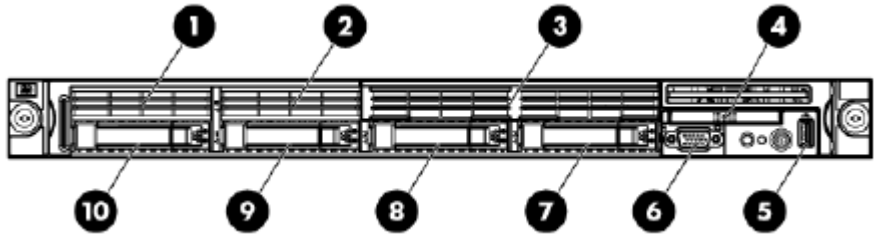
Abbreviation	Title	Part number
1URH	1U Rack Hardware Installation Instructions	365 494–004
PCS	Power Cord Strain Relief Kit	407 454–021

General troubleshooting

The references listed below contain general troubleshooting information.

Topic	Reference	Avaya recommendation
Getting started with server troubleshooting	TG: *Getting started*	
Common problems	TG: *Common problem resolution*	
Diagnostic gflowcharts	TG: *Diagnostic flowcharts*	
HP resources	TG: *HP resources for troubleshooting*	
Error messages:		
• POST error messages and beep codes (separate alphabetical and numeric lists) • Event list error messages • Insight Diagnostics processor error codes		• Review beep codes. If suggested action can be accomplished, replace server. • Memory: ensure that DIMMs are installed correctly. Reseat memory if necessary.

Front-panel troubleshooting indicators



Note:

Servers ship with two or more hard disk drives, depending upon product requirements.

No.	Description
1	Hard disk drive not present.
2	Hard disk drive not present.
3	Activity LED on DVD-RW drive intermittent when DVD is loaded.
4	Systems Insight Display has several LEDs to indicate problems with: • Processor • DIMMs • Fans • Temperature

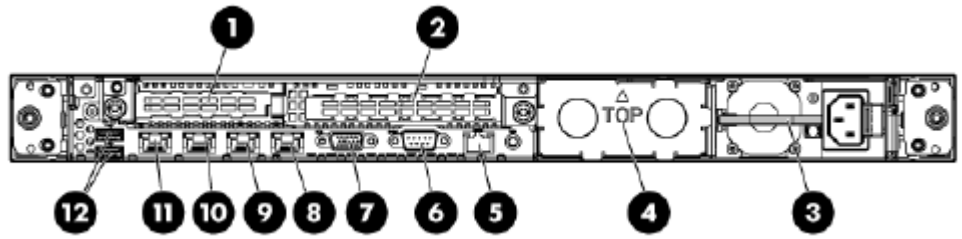
Table continues…

No.	Description
	• Power supply • Power capacity See UG: *Systems Insight Display LEDs*
5	Front USB connector
6	Video connector
7	Hard disk drive LEDs
8	Hard disk drive LEDs
9	Hard disk drive LEDs
10	Hard disk drive LEDs

Note:

In addition to the indicators listed above see also UG: *Front panel LEDs and buttons*.

Rear-panel troubleshooting indicators



No.	Description
1	Slot 1 PCIe2 x8 (8, 4, 2, 1) **Note:** A half HT faceplate is required, and you might need to remove the full faceplate and replace it with a half faceplate (requires a Phillips screwdriver). If adding a NIC, PCI Slot 1 must be used prior to slot 2 (applies to NICs only).
2	Slot 2 PCIe2 x16 (16, 8, 4, 2, 1), 75W +EXT 75W*
3	Power supply LEDs
4	Optional power supply LEDs
5	iLO 3 connector
6	Serial connector
7	Video connector

Table continues…

No.	Description
8	NIC LEDs
9	NIC LEDs
10	NIC LEDs
11	NIC LEDs
12	USB connectors (2)

Note:

In addition to the indicators listed above see also UG: *Rear panel LEDs and buttons*.

Troubleshooting external server components

Use the checklist below to troubleshoot any of the following external server components:

Part number	Description	Hot-swappable?
700501426	DL360G7 SRVR 146GB 10K SAS 2.5” HDD	Y
700501249	DL360G7 SRVR 146GB 15K SAS 2.5” HDD	Y
700501314	DL360G7 SRVR 300GB 10K SAS 2.5” HDD	Y
700501182	DL360G7 SRVR PWR SUP 460W HE	Y, if redundant
700501312	DL360G7 SRVR AC PWR SUP 750W	Y, if redundant
700501313	DL360G7 SRVR DC PWR SUP 1200W	Y, if redundant

No.	Task	Reference	Avaya recommendation	✔
1	Visually check for hardware LED fault indicators:			
	• DL360G7 SRVR 146GB 10K SAS 2.5” HDD • DL360G7 SRVR 146GB 15K SAS 2.5” HDD • DL360G7 SRVR 300GB 10K SAS 2.5” HDD	MSG: *SAS and SATA hard drive LEDs* TG: *Hard drive LED combinations*	If the hardware LED indicates a problem, consult the appropriate troubleshooting information.	
	• DL360G7 SRVR PWR SUP 460W HE • DL360G7 SRVR AC PWR SUP 750W • DL360G7 SRVR DC PWR SUP 1200W	MSG: *Rear panel LEDs and buttons* MSG: *Systems Insight Display LED combinations* TG: *Power supply problems*	If the hardware LED indicates a problem, consult the appropriate troubleshooting information.	

Table continues…

No.	Task	Reference	Avaya recommendation	✔
2	If the hardware LED indicates a problem, consult the appropriate troubleshooting information:			
	• DL360G7 SRVR 146GB 10K SAS 2.5” HDD • DL360G7 SRVR 146GB 15K SAS 2.5” HDD • DL360G7 SRVR 300GB 10K SAS 2.5” HDD	TG: *Drive problems (hard drives and solid state drives)* TG: *Hard drive LED combinations*	If amber LED b links regularly, replace the HDD.	
	• DL360G7 SRVR PWR SUP 460W HE • DL360G7 SRVR AC PWR SUP 750W • DL360G7 SRVR DC PWR SUP 1200W	TG: *Power supply problems*	Check for loose connector.	
3	If the part is defective, see *Replacing external server components*.			

Troubleshooting internal server components

Use the checklist below to troubleshoot any of the following internal server components:

Part number	Description
700501424	DL360G7 DVD-RW DRIVE W/ BRKT
700501322	DL360G7 SRVR DUAL PORT 1GB NIC
700501425	DL360G7 SRVR FAN FRU
700501318	DL360G7 SRVR 2GB MEMORY DIMM
700501319	DL360G7 SRVR 4GB MEMORY DIMM
700501324	DL360G7 SRVR 650 MAH RAID BATTERY

No.	Task	Reference	Avaya recommendation	✔
1	Visually check for LED fault indicators:			

Table continues…

No.	Task	Reference	Avaya recommendation	✔
	• DL360G7 DVD-RW DRIVE W/ BRKT	TG: *CD-ROM and DVD drive problems*	If the hardware LED indicates a problem, consult the appropriate troubleshooting information.	
	• DL360G7 SRVR DUAL PORT 1GB NIC	MSG: *Rear panel LEDs and buttons* MSG: *Systems Insight Display LED combinations*	**Note:** Only refer to Item 2, *NIC LEDs*. If the hardware LED indicates a problem, consult the appropriate troubleshooting information.	
	• DL360G7 SRVR FAN FRU	MSG: *Systems Insight Display LED combinations*	If the hardware LED indicates a problem, consult the appropriate troubleshooting information.	
	• DL360G7 SRVR 2GB MEMORY DIMM • DL360G7 SRVR 4GB MEMORY DIMM	MSG: *Systems Insight Display LED combinations* TG: *Memory problems*	If the hardware LED indicates a problem, consult the appropriate troubleshooting information.	
	• DL360G7 SRVR 650 MAH RAID BATTERY		If the hardware LED indicates a problem, consult the appropriate troubleshooting information.	
2	If the hardware LED indicates a problem, consult the appropriate troubleshooting information:			
	• DL360G7 DVD-RW DRIVE W/ BRKT	TG: *CD-ROM and DVD drive problems*	Perform only Steps 3 and 4 in the *System does not boot from the drive* section. Perform all of the steps in the *Data read from the drive is inconsistent, or drive cannot read data*" and *Drive is not detected* sections.	

Table continues…

No.	Task	Reference	Avaya recommendation	✔
			If problem persists, order replacement drive.	
	• DL360G7 SRVR DUAL PORT 1GB NIC	TG: *Expansion board problems*	Check NIC indicator LEDs. If problem persists, order replacement NIC.	
	• DL360G7 SRVR FAN FRU	TG: *Fan problems*	If problem persists, order replacement fan.	
	• DL360G7 SRVR 2GB MEMORY DIMM • DL360G7 SRVR 4GB MEMORY DIMM	TG: *Memory problems*	If problem persists, order replacement memory.	
	• DL360G7 SRVR 650 MAH RAID BATTERY			
3	If the part is defective, see *Replacing internal server components*.			

Verifying hard drive synchronization—HP ProLiant DL360 G7

About this task

Use this task after you have replaced the HP ProLiant DL360 G7 hard drive to verify data synchronization and drive status.

A replacement hard drive automatically rebuilds the mirror after installation. Use the **`hpacucli`** command to verify the drive as it rebuilds. The Array Configuration Utility CLI (**`hpacucli`**) is a command line based disk configuration program for Smart Array Controllers and RAID Array Controllers.

Note:

For information about troubleshooting and replacing HP ProLiant DL360 G7 hardware, see the HP ProLiant DL360 G7 server documentation CD that is packaged with the server.

Procedure

1. Log in to the Element Manager server as an SSA user (for example, the ntsyadm pre-configured account).
2. At the command line prompt, type `hpacucli controller all show config detail` and press the **ENTER** key.
3. At the password prompt, enter the password and press the **ENTER** key.

The system displays the logical drive status. For example:

```
Array: A
      Interface Type: SAS
      Unused Space: 0 MB
      Status: OK



      Logical Drive: 1
         Size: 136.7 GB
         Fault Tolerance: RAID 1
         Heads: 255
         Sectors Per Track: 32
         Cylinders: 35132
         Stripe Size: 128 KB
         Status: Recovering, 4% complete
```

4. Monitor the logical drive status to ensure that recovery is complete and the status returns to OK. For example:

```
Array: A
      Interface Type: SAS
      Unused Space: 0 MB
      Status: OK



      Logical Drive: 1
         Size: 136.7 GB
         Fault Tolerance: RAID 1
         Heads: 255
         Sectors Per Track: 32
         Cylinders: 35132
         Stripe Size: 128 KB
         Status: OK
```

Verifying hard drive synchronization—HP ProLiant DL360 G7 job aid

About this task

When you run the hpacucli command, the output shows the status of the:

- whole array
- logical drive (which comprises two mirrored physical drives)
- individual physical drives

Example

Healthy system:

The following example shows the output after running the hpacucli command on a healthy system. The status of the array, logical drive, and two physical drives are all OK.

```
Smart Array P410i in Slot 0 (Embedded)
   Bus Interface: PCI
   Slot: 0
   Serial Number: 500143800992E780
   Cache Serial Number: PACCQ0F9VZ502ZQ
   RAID 6 (ADG) Status: Disabled
   Controller Status: OK
   Chassis Slot:
   Hardware Revision: Rev C
```

```
   Firmware Version: 3.00
   Rebuild Priority: Medium
   Expand Priority: Medium
   Surface Scan Delay: 15 secs
   Queue Depth: Automatic
   Monitor and Performance Delay: 60 min
   Elevator Sort: Enabled
   Degraded Performance Optimization: Disabled
   Inconsistency Repair Policy: Disabled
   Wait for Cache Room: Disabled
   Surface Analysis Inconsistency Notification: Disabled
   Post Prompt Timeout: 0 secs
   Cache Board Present: True
   Cache Status: OK
   Accelerator Ratio: 25% Read / 75% Write
   Drive Write Cache: Disabled
   Total Cache Size: 256 MB
   No-Battery Write Cache: Disabled
   Cache Backup Power Source: Batteries
   Battery/Capacitor Count: 1
   Battery/Capacitor Status: OK
   SATA NCQ Supported: True

   Array: A
      Interface Type: SAS
      Unused Space: 0 MB
      Status: OK



      Logical Drive: 1
         Size: 136.7 GB
         Fault Tolerance: RAID 1
         Heads: 255
         Sectors Per Track: 32
         Cylinders: 35132
         Stripe Size: 128 KB
         Status: OK
         Array Accelerator: Enabled
         Unique Identifier: 600508B1001030393932453738300B00
         Disk Name: /dev/cciss/c0d0
         Mount Points: /admin 94 MB, /boot 101 MB, swap 4.0 GB, swap 4.0 GB, / 2.0 GB, /
var 2.0 GB, /var/log 2.0 GB, /var/log/audit 3.0 GB, /opt 6.0 GB, /var/mcp 112.4 GB, /tmp
502 MB, /home 502 MB
         OS Status: LOCKED
         Logical Drive Label: A00B92015001438009 92E7800DF3
         Mirror Group 0:
            physicaldrive 1I:1:1 (port 1I:box 1:bay 1, SAS, 146 GB, OK)
         Mirror Group 1:
            physicaldrive 1I:1:2 (port 1I:box 1:bay 2, SAS, 146 GB, OK)

      physicaldrive 1I:1:1
         Port: 1I
         Box: 1
         Bay: 1
         Status: OK
         Drive Type: Data Drive
         Interface Type: SAS
         Size: 146 GB
         Rotational Speed: 10000
         Firmware Revision: HPD6
         Serial Number:          PCY18MVE
         Model: HP      DG0146FARVU
         PHY Count: 2
         PHY Transfer Rate: 6.0GBPS, Unknown
```

```
      physicaldrive 1I:1:2
         Port: 1I
         Box: 1
         Bay: 2
         Status: OK
         Drive Type: Data Drive
         Interface Type: SAS
         Size: 146 GB
         Rotational Speed: 10000
         Firmware Revision: HPD6
         Serial Number:          PCY195VE
         Model: HP       DG0146FARVU
         PHY Count: 2
         PHY Transfer Rate: 6.0GBPS, Unknown


   SEP (Vendor ID PMCSIERA, Model  SRC 8x6G) 250
      Device Number: 250
      Firmware Version: RevC
      WWID: 500143800992E78F
      Vendor ID: PMCSIERA
      Model:  SRC 8x6G
```

Failed system:

The following example shows the output after running the hpacucli command on a system where the first physical drive has been removed. The system displays the status as follows:

- array: Failed
- logical drive: Interim Recovery Mode
- first physical drive: Failed
- second physical drive: OK

```
Array: A
      Interface Type: SAS
      Unused Space: 0 MB
      Status: Failed

      One of the drives on this array have failed or has been removed.




      Logical Drive: 1
         Size: 136.7 GB
         Fault Tolerance: RAID 1
         Heads: 255
         Sectors Per Track: 32
         Cylinders: 35132
         Stripe Size: 128 KB
         Status: Interim Recovery Mode
         Array Accelerator: Enabled
         Unique Identifier: 600508B1001030393932453738300B00
         Disk Name: /dev/cciss/c0d0
         Mount Points: /admin 94 MB, /boot 101 MB, swap 4.0 GB, swap 4.0 GB, / 2.0 GB, /
var 2.0 GB, /var/log 2.0 GB, /var/log/audit 3.0 GB, /opt 6.0 GB, /var/mcp 112.4 GB, /tmp
502 MB, /home 502 MB
         OS Status: LOCKED
         Logical Drive Label: A00B9201500143800992E7800DF3
         Mirror Group 0:
            physicaldrive 1I:1:1 (port 1I:box 1:bay 1, SAS, 146 GB, Failed)
         Mirror Group 1:
```

```
            physicaldrive 1I:1:2 (port 1I:box 1:bay 2, SAS, 146 GB, OK)

      physicaldrive 1I:1:1
         Port: 1I
         Box: 1
         Bay: 1
         Status: Failed
         Drive Type: Data Drive
         Interface Type: SAS
         Size: 146 GB
         Rotational Speed: 10000
         Firmware Revision: HPD6
         Serial Number:          PCY18MVE
         Model: HP      DG0146FARVU
         PHY Count: 2
         PHY Transfer Rate: Unknown, Unknown

      physicaldrive 1I:1:2
         Port: 1I
         Box: 1
         Bay: 2
         Status: OK
         Drive Type: Data Drive
         Interface Type: SAS
         Size: 146 GB
         Rotational Speed: 10000
         Firmware Revision: HPD6
         Serial Number:          PCY195VE
         Model: HP      DG0146FARVU
         PHY Count: 2
         PHY Transfer Rate: 6.0GBPS, Unknown


   SEP (Vendor ID PMCSIERA, Model  SRC 8x6G) 250
      Device Number: 250
      Firmware Version: RevC
      WWID: 500143800992E78F
      Vendor ID: PMCSIERA
      Model:  SRC 8x6G
```

Recovering system:

The following example shows the output after running the hpacucli command on a system where the first physical drive has been replaced and is recovering. The system displays the status as follows:

- array: OK
- logical drive: Recovering. When in recovery mode, the system displays the percent complete of recovery for the logical drive.
- first physical drive: Rebuilding
- second physical drive: OK

```
Array: A
      Interface Type: SAS
      Unused Space: 0 MB
      Status: OK



      Logical Drive: 1
         Size: 136.7 GB
         Fault Tolerance: RAID 1
         Heads: 255
         Sectors Per Track: 32
```

```
         Cylinders: 35132
         Stripe Size: 128 KB
         Status: Recovering, 4% complete
         Array Accelerator: Enabled
         Unique Identifier: 600508B1001030393932453738300B00
         Disk Name: /dev/cciss/c0d0
         Mount Points: /admin 94 MB, /boot 101 MB, swap 4.0 GB, swap 4.0 GB, / 2.0 GB, /
var 2.0 GB, /var/log 2.0 GB, /var/log/audit 3.0 GB, /opt 6.0 GB, /var/mcp 112.4 GB, /tmp
502 MB, /home 502 MB
         OS Status: LOCKED
         Logical Drive Label: A00B9201500143800992E7800DF3
         Mirror Group 0:
            physicaldrive 1I:1:1 (port 1I:box 1:bay 1, SAS, 146 GB, Rebuilding)
         Mirror Group 1:
            physicaldrive 1I:1:2 (port 1I:box 1:bay 2, SAS, 146 GB, OK)

      physicaldrive 1I:1:1
         Port: 1I
         Box: 1
         Bay: 1
         Status: Rebuilding
         Drive Type: Data Drive
         Interface Type: SAS
         Size: 146 GB
         Rotational Speed: 10000
         Firmware Revision: HPD6
         Serial Number:         PCY18MVE
         Model: HP      DG0146FARVU
         PHY Count: 2
         PHY Transfer Rate: 6.0GBPS, Unknown

      physicaldrive 1I:1:2
         Port: 1I
         Box: 1
         Bay: 2
         Status: OK
         Drive Type: Data Drive
         Interface Type: SAS
         Size: 146 GB
         Rotational Speed: 10000
         Firmware Revision: HPD6
         Serial Number:         PCY195VE
         Model: HP      DG0146FARVU
         PHY Count: 2
         PHY Transfer Rate: 6.0GBPS, Unknown


   SEP (Vendor ID PMCSIERA, Model  SRC 8x6G) 250
      Device Number: 250
      Firmware Version: RevC
      WWID: 500143800992E78F
      Vendor ID: PMCSIERA
      Model:  SRC 8x6G
```

Replacing external components

Use the checklist below to replace any of the following external server components:

Part number	Description	Hot-swappable?
700501426	DL360G7 SRVR 146GB 10K SAS 2.5” HDD drive	Y
700501249	DL360G7 SRVR 146GB 15K SAS 2.5” HDD	Y
700501314	DL360G7 SRVR 300GB 10K SAS 2.5” HDD	Y
700501182	DL360G7 SRVR PWR SUP 460W HE	Y, if redundant
700501312	DL360G7 SRVR AC PWR SUP 750W	Y, if redundant
700501313	DL360G7 SRVR DC PWR SUP 1200W	Y, if redundant

Note:

Hard disk drives and redundant power supplies are hot-swappable; you do not have to power down the server. Replacing a power supply usually does not require removing the server from the rack unless cables or other obstructions prevent removing and replacing the power supply.

No.	Task	Reference	Avaya recommendation	✔
1	Power down server if the part being replaced is not hot-swappable.	MSG: *Power down the server*	Determine whether the replaceable component is hot-swappable.	
2	Slide the server out of the rack if required to access the part being replaced.	MSG: *Extend the server from the rack* MSG: Remove the server from the rack	Check that the Cable Management Arm (if present) moves freely out of the way of rear panel components.	
3	Replace the component:			
	• DL360G7 SRVR 146GB 10K SAS 2.5” HDD • DL360G7 SRVR 146GB 15K SAS 2.5” HDD • DL360G7 SRVR 300GB 10K SAS 2.5” HDD	MSG: Removal and replacement procedures > *SAS and SATA hard drive* MSG: Removal and replacement procedures > *Hard drive blank*		
	• DL360G7 SRVR PWR SUP 460W HE • DL360G7 SRVR AC PWR SUP 750W	MSG: Removal and replacement procedures > *Hotplug power supply*	Ensure that the replacement power supply matches the specifications of the defective power supply.	

Table continues…

No.	Task	Reference	Avaya recommendation	✔
	• DL360G7 SRVR DC PWR SUP 1200W	MSG: Removal and replacement procedures > *Power supply blank*		
4	Slide the server into the rack (if slid out)	UG: *Installing the server into the rack*	Check that the Cable Management Arm (if present) moves freely out of the way of rear panel components.	
5	Connect the power cable(s) to the power supply (if disconnected)	UG: *Powering up and configuring the server*		
6	Power up the server (if powered down)	UG: *Power up the server*		

Replacing internal components

Use the checklist below to replace any of these internal server components:

Part number	Description
700501424	DL360G7 DVD-RW DRIVE W/ BRKT
700501322	DL360G7 SRVR DUAL PORT 1GB NIC
700501425	DL360G7 SRVR FAN FRU
700501318	DL360G7 SRVR 2GB MEMORY DIMM
700501319	DL360G7 SRVR 4GB MEMORY DIMM
700501324	DL360G7 SRVR 650 MAH RAID BATTERY

Note:

Although not used frequently, Avaya customers are required to have a monitor, keyboard, and mouse available for use by installation and/or servicing technicians.

No.	Task	Reference	Avaya recommendation	✔
1	Have the proper tools	MSG: *Required tools*		
2	Observe safety warnings	TG:"*Important safety information* MSG: *Safety considerations*		
3	Power down the server	MSG: Removal and replacement procedures > *Power down the server*		

Table continues…

No.	Task	Reference	Avaya recommendation	✔
4	Slide the server out of the rack	MSG: Removal and replacement procedures > *Extend the server from the rack* MSG: Removal and replacement procedures > *Remove the server from the rack*		
5	Remove the cover	MSG: Removal and replacement procedures > *Access panel*	**Electrostatic alert:** Ensure that you are properly grounded before handling internal components.	
6	Replace the component:			
	• DL360G7 DVD-RW DRIVE W/ BRKT	MSG: Removal and replacement procedures: • *DVD tray* • *DVD-ROM or DVD-RW drive*	Omit Steps 4 and 5 from both procedures. You do not need to remove the air baffle or the BBWC battery pack.	
	• DL360G7 SRVR DUAL PORT 1GB NIC	MSG: Removal and replacement procedures: • PCI riser board assembly • *Expansion boards* • *PCIe riser board*	Mark any cables connected to the NIC and reconnect to the same ports after the NIC is replaced. The NIC requires a half-HT faceplate. You might need to remove the full faceplate and replace it with the half faceplate, which requires a crosshatch (Phillips) screwdriver. **Note:** If adding a NICs: populate PCI Slot 1 first, followed by Slot 2.	
	• DL360G7 SRVR FAN FRU	MSG: Removal and replacement procedures > *Fan module*	Refer to the Systems Insight Display LEDs to identify the defective fan.	
	• DL360G7 SRVR 2GB MEMORY DIMM • DL360G7 SRVR 4GB MEMORY DIMM	MSG: Removal and replacement procedures > *DIMMs*	Refer to the Systems Insight Display LEDs to identify the defective DIMM.	

Table continues…

No.	Task	Reference	Avaya recommendation	✔
			Caution: When removing the air baffle, ensure that the RAID battery does not fall out of its compartment in the baffle. **Caution:** Refer to the information on the top of the air baffle and inside cover for correct DIMM placement.	
	• DL360G7 SRVR 650 MAH RAID BATTERY	MSG: Removal and replacement procedures > *BBWC battery pack or FBWC capacitor pack*	**Caution:** Consult the internal label with directions for removing the air baffle. Be careful that the RAID battery does not fall out of its compartment in the baffle. To remove the cable from the battery, gently rock the connector back and forth and free of the alignment slots. **Caution:** When replacing the air baffle and facing the front of the server, insert the left side into the alignment slots, then gently flex the baffle so that the right side slides into its alignment slot easily. DO NOT attempt to force or pound the baffle into place. **Caution:** DO NOT pinch the battery cable when replacing the air baffle.	

Table continues…

No.	Task	Reference	Avaya recommendation	✔
7	Replace the cover	MSG: Removal and replacement procedures > *Access panel*		
8	Slide the server into the rack	RI-SR	Check that the Cable Management Arm (if present) moves freely out of the way of rear panel components.	
9	Connect and secure the power cords	GS: *Connecting the Power Cables* GS: *Securing the Power Cord*		
10	Power up the server	GS: *Turning on the System*		

Upgrading memory for the HP DL360 G7 server

In a standalone deployment, perform this task on the Element Manager server. In the case of a standalone with redundancy deployment, perform this task on both Element Manager servers. This task adds memory to an existing AAC installation. Perform this task if your system has been experiencing any memory shortages.

Note:

This procedure does not apply to the co-resident model.

Before you begin

- You have backed up the AAC system.
- You have the AAC Memory Upgrade Kit.
- You have the HP DL360 document set.

About this task

Use this procedure to replace the existing 2 GB DIMM RAM memory with new 4 GB DIMM RAM memory.

If using mixed sized DIMMs, insert the larger sized DIMMs in the primary DRAM channels, then move onto the smaller sizes in the correct sequential order. The primary DRAM channels are marked with white tabs.

Install RDIMMs in alphabetical order (slots A through I).

Procedure

1. Observe safety warnings.
2. Observe all ESD safety precautions.
3. Handle the DIMMs with care:
   - Hold DIMMs by the side edges only.
   - Avoid touching the connectors on the bottom of the DIMM.

- Never wrap your fingers around a DIMM.
- Avoid touching the components on the sides of the DIMM.
- Never bend or flex the DIMM.

4. Power off the HP DL360 G7 server.
5. Extend the server from the rack.
6. Remove the access panel.
   a. Open the latch

      If it is locked, use a T-15 Torx screwdriver to unlock the latch.
   b. Slide the access panel to the rear of the chassis.
   c. Remove the panel.
7. If installed, remove the BBWC battery pack from air baffle and set it aside.

   Keep the wires connected.
8. Remove the air baffle.

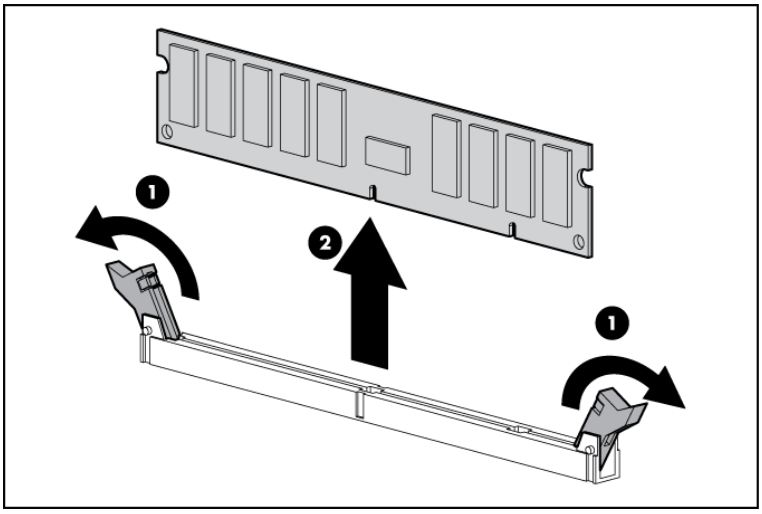


Figure 18: DIMM Removal

9. Open the DIMM slot latches.
10. Remove all existing 2 GB DIMM memory.
11. Install new 4 GB DIMM memory in the Primary DRAM channels, (white colored, slots A, B, C).
12. Reinstall the used 2 GB DIMM memory in the Secondary DRAM channels, (black colored, slots D-I).
13. Reinstall the Air Baffle.

Warning:

Be careful not to damage DIMMS or cables.

14. If removed, reinstall the BBWC battery pack.
15. Install the access panel.
16. Power up the HP DL360 G7 server.

Result

When you successfully install the memory, the server will automatically run a diagnostic on the new memory to test for failures.

Troubleshooting the Dell R610 hardware

This section provides tasks to troubleshoot and/or replace some Dell R610 components.

This section describes how to manage and resolve problems with the Dell R610 hardware and provides:

- instructions for how to find the appropriate online server documentation from Dell
- references to specific topics in standard Dell documentation
- suggested changes, details, and notes to assist you in interpreting the manufacturer's documentation and to clarify Avaya's recommended implementation of the equipment
- additional topics not covered in standard Dell documentation but which are necessary for maintaining and troubleshooting the Avaya installation

Warning:

Read the applicable sections in the Dell documentation and become familiar with the procedures before replacing hardware components or units. Ensure replacement components or units reference documentation is available prior to starting any replacement procedures. For some hardware, you must stop, start, or reinstall the applications when you replace the hardware. Outages can occur if you do not follow instructions completely.

Downloading Dell documentation

Use this procedure to find and download the Dell™ PowerEdge™ R610 documentation from Dell.

Procedure

1. Open a browser and to go http://www.support.dell.com/.
2. On the Welcome to Dell Support page click on the `Start Here` button in the Support for Enterprise IT section.

3. On the Welcome to Enterprise IT Support click on `Select a product` in the Product Support section.
4. On the next page click on `Select Model` in the Choose a Model section.
5. On the Select Product by Model page, click on `Servers, Storage, Networking`.
6. On the Select Product by Model > Server, Storage, Networking page use the scroll bar in the Select Your Product Line column and click on `PowerEdge Server`.
7. On the Select Product by Model > Server, Storage, Networking > PowerEdge Server page, use the scroll bar in the Select Your Product Model column and click on `R610`.
8. On the Select Product by Model > Server, Storage, Networking > PowerEdge Server > R610 page, click on the `Confirm` button in the Confirm your selection section.
9. On the Product Support for PowerEdge R610 page click on Manuals and Documentation.
10. On the Dell™ PowerEdge™ R610 System page, click the `Download` link that corresponds to the document that you want to download.
11. Download the documents in the *Dell R610 document set* > *Documents to download* section below.

Dell R610 documentation set

Refer to the documents listed below for Dell R610 server installation information and procedures.

Note:

Download the documents listed in the *Documents to download* section below. Printed copies of the documents listed in the *Documents included in the shipping container* section below ship with the server.

Documents to download

Abbreviation	Title	Part number
CMAI	Cable Management Arm Installation	0F880KA00
GS	Getting Started With Your System	R465D
HOM	Hardware Owner's Manual	No number
RI-SR	Rack Installation (Sliding Rails)	0J171KA00

Note:

If you want to locate and download an individual document:

- Go to http://www.dell.com/.
- Type `R610` plus the keywords of the document title in the Search field in the upper-right corner and press `Enter`.

Examples:

- Type `R610 Technical Guidebook` to search for the *Technical Guidebook* document.
- Type `R610 Getting Started` to search for the *Getting Started with your System* document.

Documents included in the shipping container

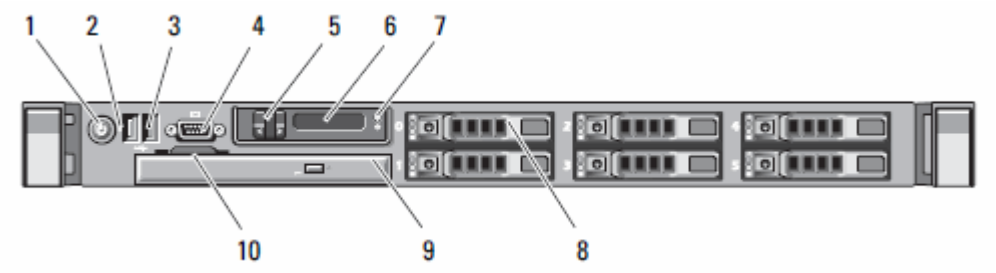
Abbreviation	Title	Part number
PS	Product Safety, EMC & Environmental Datasheet	No number
TG	Technical Guidebook	No number

General troubleshooting

The references listed below contain general troubleshooting information.

Topic	Reference	Avaya recommendation
System features and diagnostics that are accessible during startup	HOM: *Access System Features During Startup*	**Caution:** Only performed when requested by Avaya Support personnel. **Note:** Keyboard, monitor, and mouse are required.
LCD panel	HOM: *LCD Panel Features*	
LCD status messages	HOM: *LCD Status Messages*	See *LCD status message explanations* in this document for recommended resolutions.
System messages	HOM: *System Messages*	**Caution:** For advanced troubleshooting only—consult Avaya Services. **Note:** Keyboard, monitor, and mouse are required.

Front panel troubleshooting indicators



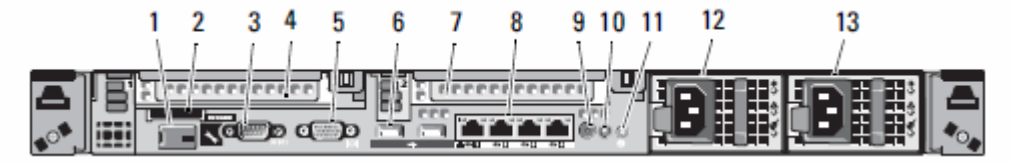
Use the front panel indicators listed to troubleshoot server components:

No.	Description	Avaya recommendation
1	Power-on indicator, power button	Indicates when the system power is on. The power button controls the DC power supply output to the system. **Note:** Consult individual application/solution documentation for detailed shutdown procedures. **Note:** To force an ungraceful shutdown, press and hold the power button for five (5) seconds. **Caution:** Not recommended for products/solutions that use System Platform.
2	NMI button	Used to troubleshoot software and device driver errors when using certain operating system. This button can be pressed using the end of a paper clip. **Caution:** Not recommended for products/solutions that use System Platform. Use this button only if directed to do so by qualified support personnel.
3	USB connectors (2)	
4	Video connector	
5	LCD menu buttons	Allows you to navigate to the control panel LCD menu.

Table continues…

No.	Description	Avaya recommendation
6	LCD Panel	Provides system ID, status information, and system error messages. LCD background color indicates these conditions: • **Blue:** normal system operation • **Amber:** system needs attention LCD panel displays errors codes and descriptive tests.
7	System identification button	Turns the system ID modes on and off. The identification buttons on the front and back panels can be used to locate a particular system within a rack. When one of these buttons is pushed, the LCD panel on the front and the system status indicator on the chassis back panel flash blue until one of the buttons is pushed again. **Note:** Some applications/solutions use this light for additional functionality.
8	Hard drives	Servers ship with two or more hard disk drives, depending upon product requirements.
9	Optical drive	
10	System identification panel	A slide-out panel for system information including the Express Service tag, embedded NIC MAC address, and iDRAC6 Express card MAC address. Space is provided for an additional label.

Rear panel troubleshooting indicators



Use the rear panel indicators listed to troubleshoot server components:

No.	Description	Avaya recommendation
1	iDRAC6 Enterprise/Express port (optional)	Dedicated management port for the optical iDRAC6 Enterprise/Express card.
2	VFlash media slot (optional)	Connects an external SD memory card for the optional iDRAC6 Enterprise/Express card.

Table continues…

No.	Description	Avaya recommendation
3	Serial connector	
4	PCIe slot 1	Consult application/solution documentation for specific behavior of the optional card in this slot.
5	Video connector	
6	USB connectors (2)	
7	PCIe slot 2	Consult application/solution documentation for specific behavior of the optional card in this slot.
8	Ethernet connectors (4)	
9	System status indicator connector	
10	System status indicator	Provides a power on indicator for the back of the system.
11	System identification button	Turns the system ID modes on and off. The identification buttons on the front and back panels can be used to locate a particular system within a rack. When one of these buttons is pushed, the LCD panel on the front and the system status indicator on the chassis back panel flash blue until one of the buttons is pushed again. **Note:** Some applications/solutions use this light for additional functionality.
12	Power supply 1 (PS1)	
13	Poser supply 2 (PS2)	

Troubleshooting external server components

Use the checklist below to troubleshoot any of the following external server components:

Part number	Description	Hot-swappable?
700501316	R610 SRVR 146GB 10K SAS 2.5” HDD	Y
700501317	R610 SRVR 146GB 15K SAS 2.5” HDD	Y
700501315	R610 SRVR 300GB 10K SAS 2.5” HDD	Y
700501421	R610 SRVR 600GB 10K SAS 2.5" HDD	Y
700501183	R610 SRVR AC PWR SUP 502W ES	Y, if redundant
700501311	R610 SRVR AC PWR SUP 717W	Y, if redundant

No.	Task	Reference	Avaya recommendation	✔
1	Visually check for hardware LED fault indicators:			
	• R610 SRVR 146GB 10K SAS 2.5” HDD • R610 SRVR 146GB 15K SAS 2.5” HDD • R610 SRVR 300GB 10K SAS 2.5” HDD • R610 SRVR 600GB 10K SAS 2.5" HDD	HOM: *Hard Drive Indicator Patterns for RAID* TG: *Storage*	If the HDD LED indicates a problem, consult the appropriate troubleshooting information.	
	• R610 SRVR AC PWR SUP 502W ES • R610 SRVR AC PWR SUP 717W	HOM: *Power Indicator Codes* TG: *Power Supply Indicators*	If the LEDs indicate a problem, consult the appropriate troubleshooting information.	
2	If the hardware LED indicates a problem, consult the appropriate troubleshooting information:			
	• R610 SRVR 146GB 10K SAS 2.5” HDD • R610 SRVR 146GB 15K SAS 2.5” HDD • R610 SRVR 300GB 10K SAS 2.5” HDD • R610 SRVR 600GB 10K SAS 2.5" HDD	HOM: *Troubleshooting Hard Drives*	• Inspect LEDs and LCD display output. • If the LED flashes green, then amber, then off (in that order), replace the HDD. • If the LED blinks amber, replace the HDD.	
	• R610 SRVR AC PWR SUP 502W ES • R610 SRVR AC PWR SUP 717W	HOM: *Troubleshooting Power Supplies*		
3	If the part is defective, see *Replacing external server components*.			

Troubleshooting internal server components

Use the checklist below to troubleshoot any of the following internal server components:

Part number	Description
700501323	R610 SRVR DUAL PORT 1GB NIC
700501422	R610 SRVR DVD-RW DRIVE W/ BRKT
700501423	R610 SRVR FAN FRU
700501320	R610 SRVR 2GB MEMORY DIMM
700501320	R610 SRVR 4GB MEMORY DIMM
700501325	R610 SRVR RAID BATTERY

No.	Task	Reference	Avaya recommendation	✔
1	Visually check for hardware LED fault indicators:			
	• R610 SRVR DUAL PORT 1GB NIC	TG: *NIC Indicators*	If the hardware LED indicates a problem, consult the appropriate troubleshooting information.	
	• R610 SRVR DVD-RW DRIVE W/ BRK	HOM: *Optical Drive*		
	• R610 SRVR FAN FRU	HOM: *Cooling Fans*		
	• R610 SRVR 2GB MEMORY DIMM • R610 SRVR 4GB MEMORY DIMM	HOM: *System Memory*		
	• R610 SRVR RAID BATTERY	HOM: *RAID Battery*		
2	If the hardware LED indicates a problem, consult the appropriate troubleshooting information:			
	• R610 SRVR DUAL PORT 1GB NIC	HOM: *Troubleshooting a NIC*	Check NIC indicator LEDs. If problem persists, order replacement NIC.	
	• R610 SRVR DVD-RW DRIVE W/ BRK	HOM: *Troubleshooting an Optical Drive*	If problem persists, order replacement drive.	
	• R610 SRVR FAN FRU	HOM: *Troubleshooting a Fan*	If problem persists, order replacement fan.	
	• R610 SRVR 2GB MEMORY DIMM • R610 SRVR 4GB MEMORY DIMM	HOM: *Troubleshooting System Memory*	If problem persists, order replacement memory.	

Table continues…

No.	Task	Reference	Avaya recommendation	✔
	• R610 SRVR RAID BATTERY	HOM: *RAID Battery*	Keyboard, monitor, and mouse required for advanced troubleshooting.	
3	If the part is defective, see *Replacing internal server components*.			

Troubleshooting the Dell R610 power supply

Procedure

1. Using the power supply's status indicator, identify the faulty power supply.
2. Reseat the power supply by removing and reinstalling it as follows:
   a. Disconnect the power cable from the power source and the power supply you intend to remove and remove the cables from the Velcro strap.
   b. Press the lever release latch and slide the power supply out of the chassis.
   c. On a system with redundant power supplies, verify that both power supplies are the same type and have the same maximum output power.
   d. Slide the new power supply into the chassis until the power supply is fully seated and the release latch snaps into place.
   e. Connect the power cable to the power supply and plug the cable into a power outlet.
3. If the problem persists, replace the faulty power supply with another power supply of the same type.
4. If the problem persists, contact Dell for support.

Replacing external components

Use the checklist below to replace any of the following external server components:

Part number	Description	Hot-swappable?
700501316	R610 SRVR 146GB 10K SAS 2.5" HDD	Y
700501317	R610 SRVR 146GB 15K SAS 2.5" HDD	Y
700501315	R610 SRVR 300GB 10K SAS 2.5" HDD	Y
700501421	R610 SRVR 600GB 10K SAS 2.5" HDD	Y
700501183	R610 SRVR AC PWR SUP 502W ES	Y, if redundant
700501311	R610 SRVR AC PWR SUP 717W	Y, if redundant

Note:

Hard disk drives and redundant power supplies are hot-swappable; you do not have to power down the server. Replacing a power supply usually does not require removing the server from the rack unless cables or other obstructions prevent removing and replacing the power supply.

No.	Task	Reference	Avaya recommendation	✔
1	Power down server (if necessary)		Determine whether the replaceable component is hot-swappable.	
2	Slide the server out of the rack (if necessary)	RI-SR CMAI: *Moving the CMA Away from the CMA Tray*	Ensure that the Cable Management Arm (if present) moves freely out of the way of rear panel components.	
3	Replace the component:			
	• R610 SRVR 146GB 10K SAS 2.5” HDD • R610 SRVR 146GB 15K SAS 2.5” HDD • R610 SRVR 300GB 10K SAS 2.5” HDD • R610 SRVR 600GB 10K SAS 2.5" HDD	HOM: *Hard drives*		
	• R610 SRVR AC PWR SUP 502W ES • R610 SRVR AC PWR SUP 717W	HOM: *Power supplies*	Ensure that the replacement power supply matches the specifications of the defective power supply.	
4	Slide the server into the rack (if necessary)	RI-SR	Ensure that the Cable Management Arm (if present) moves freely out of the way of rear panel components.	
5	Connect the power cable(s) to the power supply (if necessary)	GS: *Connecting the Power Cables* GS: *Securing the Power Cord*		
6	Power up the server (if necessary)	GS: *Turning on the System*		

Replacing internal components

Use the checklist below to replace any of these internal server components:

Part number	Description
700501323	R610 SRVR DUAL PORT 1GB NIC
700501422	R610 SRVR DVD-RW DRIVE W/ BRKT
700501423	R610 SRVR FAN FRU
700501320	R610 SRVR 2GB MEMORY DIMM
700501320	R610 SRVR 4GB MEMORY DIMM
700501325	R610 SRVR RAID BATTERY

Note:

Although not used frequently, Avaya customers are required to have a monitor, keyboard, and mouse available for use by installation and/or servicing technicians.

No.	Task	Reference	Avaya recommendation	✔
1	Have the proper tools	HOM: *Recommended Tools*		
2	Observe safety warnings	HOM: *Safety First—For You and Your System*		
3	Power down server			
4	Slide the server out of the rack	RI-SR		
5	Remove the cover	HOM: *Opening and Closing the System*	**Electrostatic alert:** Ensure that you are properly grounded before handling internal components.	
6	Replace the component:			
	• R610 SRVR DUAL PORT 1GB NIC	HOM: *Expansion Cards*	Mark any external cables connected to the NIC and reconnect to the same ports after the NIC is replaced.	
	• R610 SRVR DVD-RW DRIVE W/ BRKT	HOM: *Optical Drive*	In the *Removing an Optical Drive* section perform steps 2–5 only. In the *Installing an Optical Drive* section perform steps 2–6, 8, and 10 only.	

Table continues…

No.	Task	Reference	Avaya recommendation	✔
	• R610 SRVR FAN FRU	HOM: *Cooling Fans*	**Caution:** Do not attempt to hot-swap a fan.	
	• R610 SRVR 2GB MEMORY DIMM • R610 SRVR 4GB MEMORY DIMM	HOM: *System Memory*	Consult server cover label for memory placement. Consult application/ solution documentation for specific procedures.	
	• R610 SRVR RAID BATTERY	HOM: *RAID Battery*	Remove the battery from the cable. Do not replace the battery cable unless it is defective. **Note:** Monitor, keyboard, and mouse might be necessary for server reboot.	
7	Replace the cover	HOM: *Opening and Closing the System*		
8	Slide the server into the rack	RI-SR	Ensure that the Cable Management Arm (if present) moves freely out of the way of rear panel components.	
9	Connect and secure the power cords	GS: *Connecting the Power Cables* GS: *Securing the Power Cord*		
10	Power up the server	GS: *Turning on the System*		

LCD status message explanations

LCD status codes, the associated text, the likely cause(s) for the error code, and the corrective action are listed below. When escalation is the corrective action, contact Avaya if you have a maintenance contract with Avaya or contact the Avaya business partner from whom you purchased the server. If the escalation requires replacing a field replaceable unit (FRU), see:

- *Replacing external server components*
- *Replacing internal server components*

Code	Text	Causes	Corrective action
N/A	AVAYA	AVAYA displays when: • The system is powered on. • The power is off and active POST errors are displayed.	This message is for information only.
E1000	FAILSAFE, Call Support		Escalate for possible server replacement.
E1114	Temp Ambient	Ambient system temperature is out of acceptable range.	Check room temperature and external air flow. If both are within acceptable limits, then escalate for possible server replacement.
E1116	Temp Memory	Memory has exceeded acceptable temperature and has been disabled to prevent damage to the components.	Check room temperature and external air flow. If both are within acceptable limits, then escalate for possible server replacement.
E12nn	xx PwrGd	Specified voltage regulator has failed.	Escalate for possible server replacement.
E1210	CMOS Batt	CMOS battery is missing, or the voltage is out of acceptable range.	Shut down server for 1 hour and disconnect the power supply. If problem continues, escalate for possible server replacement.
E1211	ROMB Batt	RAID battery is either missing, bad, or unable to recharge due to thermal issues.	Check room temperature and external air flow. If both are within acceptable limits, then escalate for possible server replacement.
E1216	3.3V Regulator failure	3.3V voltage regulator has failed.	See HOM: *Troubleshooting Expansion Cards*. Turn off the system and attached peripherals. Power down system and unplug power cord. Open system and ensure that expansion card riser and expansion card are firmly seated. Close system, power up. If trouble persists, replace card.
E1229	CPU # VCORE	Processor # VCORE voltage regulator has failed.	Escalate for possible server replacement.
E122A	CPU # VTT Regulator failure	Specified processor VTT voltage regulator has failed	Replace the server.
E122C	CPU Power Fault	A power fault was detected when powering up the processor(s).	Remove AC power to the system for 10 seconds and restart the system.
E122D	Memory Regulator # Failed	One of the memory regulators has failed.	Reseat the memory modules.

Table continues…

Code	Text	Causes	Corrective action
E122E	On-board regulator failed.	One of the on-board voltage regulators failed.	Remove AC power to the system for 10 seconds and restart the system.
E1310	RPM Fan ##	RPM of specified cooling fan is out of acceptable operating range.	Check room temperature and external air flow. If both are within acceptable limits, then escalate for possible server replacement.
E1311	RPM Fan Mod #x	RPM of fan x in the # module is out of acceptable operating range.	Check room temperature and external air flow. If both are within acceptable limits, then escalate for possible server replacement.
E1313	Fan Redundancy	The system is no longer fan-redundant. Another fan failure will put the system at risk of over-heating.	Check room temperature and external air flow. If both are within acceptable limits, then escalate for possible server replacement. Check control panel LCD for additional scrolling messages.
E1410	CPU # IERR	Specified microprocessor is reporting an internal error.	Escalate for possible server replacement.
E1414	CPU # Thermtrip	Specified microprocessor is out of acceptable temperature range and has halted operation.	Check room temperature and external air flow. If both are within acceptable limits, then escalate for possible server replacement. **Note:** The LCD continues to display this message until the system's power cord is disconnected and reconnected to the AC power source.
E1418	CPU # Presence	Specified processor is missing or bad, and the system is in an unsupported configuration.	Escalate for possible server replacement.
E141C	CPU Mismatch	Processors are in an unsupported configuration.	Run server diagnostics. This requires a keyboard and monitor.
E141F	CPU Protocol	The system BIOS has reported a processor protocol error.	Escalate for possible server replacement.
E1420	CPU Bus PERR	The system BIOS has reported a processor bus parity error.	Escalate for possible server replacement.
E1422	CPU Machine Chk	The system BIOS has reported a machine check error.	Escalate for possible server replacement.

Table continues…

Code	Text	Causes	Corrective action
E1610	PS # Missing	No power is available from the specified power supply; specified power supply is improperly installed or faulty.	Escalate for possible power supply replacement.
E1614	PS # Status	No power is available from the specified power supply; specified power supply is improperly installed or faulty.	Escalate for possible power supply replacement.
E1618	PS # Predictive	Power supply voltage is out of acceptable range; specified power supply is improperly installed or faulty.	Escalate for possible power supply replacement.
E161C	PS # Input Lost	Power source for specified power supply is unavailable, or out of acceptable range.	Check the AC power source for the specified power supply. Escalate for possible power supply replacement.
E1620	PS # Input Range	Power source for specified power supply is unavailable, or out of acceptable range.	Escalate for possible power supply replacement.
E1624	PS Redundancy	The power supply subsystem is no longer redundant. If the last supply fails, the system will go down.	Escalate for possible power supply replacement.
E1626	Power Supply Mismatch	The power supplies in the system are not the same wattage.	Ensure that power supplies with matching wattage are installed.
E1629	Power required > PSU wattage.	The system configuration requires more power than the power supplies can provide, even with throttling.	Turn off power to the system, reduce the hardware configuration or install higher-wattage power supplies, and then restart the system.
E1710	I/O Channel Chk	The system BIOS has reported an I/O channel check.	Escalate for possible server replacement.
E1711	PCI PERR B## D## F##	reported a PCI parity error on a component that resides in PCI configuration space at bus ##, device ##, function ##.	Escalate for possible server replacement.
	PCI PERR Slot #	The system BIOS has reported a PCI parity error on a component that resides in the specified PCI slot.	
E1712	PCI SERR B## D## F##	The system BIOS has reported a PCI system error	Escalate for possible server replacement.

Table continues…

Code	Text	Causes	Corrective action
		on a component that resides in PCI configuration space at bus ##, device ##, function ##.	
	PCI SERR Slot #	The system BIOS has reported a PCI system error on a component that resides in the specified slot.	
E1714	Unknown Err	The system BIOS has determined that there has been an error in the system, but is unable to determine its origin.	Escalate for possible server replacement.
E1715	Fatal I/O error.	The system BIOS has determined there has been an error in the system.	Call Avaya Services.
E1716	Chipset IERR Bus ## Dev ## Function ##.	The system BIOS has reported a chipset internal error that resides in bus ##, device ##, function ##.	Call Avaya Services.
E1717	CPU ## internal error.	The system BIOS has determined that the specified processor has had an internal error.	Call Avaya Services.
E171F	PCIE Fatal Err B## D## F##	The system BIOS has reported a PCIe fatal error on a component that resides in PCI configuration space at bus ##, device ##, function ##.	Reseat all PCIe cards, then reboot the system. If the problem persists, escalate for possible server replacement.
	PCIE Fatal Err Slot #	The system BIOS has reported a PCIe fatal error on a component that resides in the specified slot.	
E1810	HDD ## Fault	The SAS subsystem has determined that hard drive ## has experienced a fault.	Remove the front bezel and check the top LED on the hard drives. If LED is off or flashing green, then amber, then off or flashing amber 4 times per second, the hard drive is probably failing. Escalate for possible hard drive replacement.
E1811	HDD ## Rbld Abrt	The specified hard drive has experienced a rebuild abort.	
E1812	HDD ## Removed	The specified hard drive has been removed from the system.	Information only.

Table continues…

Code	Text	Causes	Corrective action
E1A11	PCI Riser hardware & configuration mismatch	PCIe risers are not configured correctly. Some invalid configurations prevent the system from powering on.	Reinstall the expansion-card riser. Reseat the NIC. If problem persists, replace the server.
E1A12	PCI Riser not detected	One or all of the PCIe risers is missing. The prevents the system from powering on.	Reinstall the missing riser card(s).
E1A14	SAS Cable A	SAS cable A is missing or bad.	Escalate for possible server replacement.
E1A15	SAS Cable B	SAS cable B is missing or bad.	Escalate for possible server replacement.
E1A1D	Control panel USB cable not detected.	USB cable to the control panel is missing or bad.	Reseat the cable. If the problem persists, escalate for possible server replacement.
E2010	No Memory	No memory is installed in the system.	Escalate for possible memory or server replacement.
E2011	Mem Config Err	Memory detected, but is not configurable. Error detected during memory configuration.	Escalate for possible server replacement.
E2012	Unusable Memory	Memory is configured, but not usable. Memory subsystem failure.	Escalate for possible memory or server replacement.
E2013	Shadow BIOS Fail	The system BIOS failed to copy its flash image into memory.	Escalate for possible memory or server replacement.
E2014	CMOS Fail	CMOS failure. CMOS RAM not functioning properly.	Escalate for possible server replacement.
E2015	DMA Controller	DMA controller failure.	Escalate for possible server replacement.
E2016	Int Controller	Interrupt controller failure.	Escalate for possible server replacement.
E2017	Timer Fail	Timer refresh failure.	Escalate for possible server replacement.
E2018	Prog Timer	Programmable interval timer error.	Escalate for possible server replacement.
E2019	Parity Error	Parity error.	Escalate for possible server replacement.
E201A	SIO Err	SIO failure.	Escalate for possible server replacement.
E201B	Kybd Controller	Keyboard controller failure.	Escalate for possible server replacement.

Table continues…

Code	Text	Causes	Corrective action
E201C	SMI Init	System management interrupt (SMI) initialization failure.	Escalate for possible server replacement.
E201D	Shutdown Test	BIOS shutdown test failure.	Escalate for possible server replacement.
E201E	POST Mem Test	BIOS POST memory test failure.	Escalate for possible server replacement.
E2020	CPU Config	CPU configuration failure.	Check for specific error messages.
E2021	Memory Population	Incorrect memory configuration. Memory population order incorrect.	Check for specific error messages. Escalate for possible memory or server replacement.
E2022	POST Fail	General failure after video.	Check for specific error messages.
E2110	MBE Crd # DIMM ## & ##	One of the DIMMs in the set implicated by "## & ##" has had a memory multi-bit error (MBE). If no memory card is present, the "Crd #" string is left out of the message.	Escalate for possible memory or server replacement.
E2111	SBE Log Disable Crd # DIMM ##	The system BIOS has disabled memory single-bit error (SBE) logging, and will not resume logging further SBEs until the system is rebooted. "##" represents the DIMM implicated by the BIOS. If no memory riser card is present, the "Crd #" string is left out of the message.	Escalate for possible server replacement.
E2113	Mem Mirror Crd # DIMM ## & ##	The system BIOS has disabled memory mirroring because it has determined that one half of the mirror has had too many errors. "## & ##" represents the DIMM pair implicated by the BIOS. If no memory card is present, the "Crd #" string is left out of the message.	Escalate for possible memory or server replacement.
I1910	Intrusion	System cover removed.	Information only.
I1911	>3 ERRs Chk Log	LCD overflow message. A maximum of three error messages can display sequentially on the LCD. The	Information only.

Table continues…

Code	Text	Causes	Corrective action
		fourth message displays as the standard overflow message.	
I1912	SEL Full	System Event Log is full of events, and is unable to log any more events.	Clear the log by deleting event entries.
W1228	ROMB Batt < 24hr	Warns predictively that the RAID battery has less than 24 hours of charge left.	Information only.
W1627	Power required > PSU wattage.	The system configuration requires more power than what the power supply can provide.	Turn off power to the system, reduce the hardware configuration or install higher-wattage power supplies, and then restart the system.
W1628	Performance degraded.	The system configuration requires more power than what the power supply can provide, but it can boot if throttled.	Turn off power to the system, reduce the hardware configuration or install higher-wattage power supplies, and then restart the system.

Replacing the Dell R610 hard drive

Procedure

1. Identify the faulty hard drive.
2. Remove the front bezel.
3. Using the RAID management software, prepare the drive for removal.

   Wait until the hard-drive indicators on the drive carrier signal that the drive can be removed safely. See your storage controller documentation for information about hot-swap drive removal. If the drive has been online, the green activity/fault indicator will flash as the drive is powered down. When the drive indicators are off, the drive is ready for removal.
4. Press the release button and open the drive carrier release handle to release the drive.
5. Slide the hard drive out of the drive bay.
6. Insert a drive blank in the vacated drive bay.

Replacing the Dell R610 DVD-ROM drive

About this task

Warning:

You cannot hot swap the Dell R610 DVD-ROM. You must power down the server to replace the DVD-ROM. See the Dell documentation to determine if the DVD-ROM is faulty before replacing any hardware.

Procedure

1. Remove the bezel.
2. Turn off the system, including any attached peripherals, and disconnect the system from its electrical outlet.
3. Open the system.
4. Disconnect the cable connector labeled OPTICAL from the back of the drive.
5. To remove the drive carrier, press the release latch, then slide the carrier out of the chassis.
6. Align the replacement optical drive with its opening in the front panel.
7. Slide in the optical drive until the latch snaps into place.
8. Connect the cable connector labeled OPTICAL to the back of the drive.
9. Connect the power cable to DVD_PWR and the interface cable to SATA_A on the system board.
10. Replace the front bezel, if applicable.
11. Reconnect the system and peripherals to their electrical outlets.

Replacing the Dell R610 server

About this task

Warning:

If a catastrophic failure occurs and the entire server needs to be replaced, the software backup of the server can be used to restore to the new server. If a backup of the server is not available, data loss occurs.

Procedure

1. Remove the failed server from the rack.

   Caution:

   Use caution removing power from the server. Personal injury and equipment damage can result. Use safe lifting practices.

2. Install the replacement server into the rack.
3. Restore the software from a backup if available.
4. Install and configure the software if a backup is not available.

Troubleshooting the S8800 hardware

This section describes how to manage and resolve problems with the S8800 hardware.

Light path diagnostics

About light path diagnostics

Light path diagnostics is a system of LEDs on various external and internal components of the server. When an error occurs, LEDs light up throughout the server. By viewing the LEDs in a particular order, you can often identify the source of the error.

When LEDs light up to indicate an error, they remain lit when the server is turned off, provided that the server is still connected to a power source and the power supply is operating correctly.

Using light path diagnostics to identify system errors

About this task

If an error occurs, view the light path diagnostics LEDs in the following order:

Procedure

1. Look at the operator information panel on the front of the server. Check if the information LED or system error LED lights up.
2. View the light path diagnostics panel. Lit LEDs on this panel indicate the type of error that has occurred.

   Important:

   The checkpoint code display does not provide error codes or suggest components to be replaced. The checkpoint code is an internal code used for IBM development only and is subject to change over time. Ignore this code unless you have a specific request from Avaya to note it.
3. Remove the server cover while the server is connected to power and look inside the server for lit LEDs.

Important:

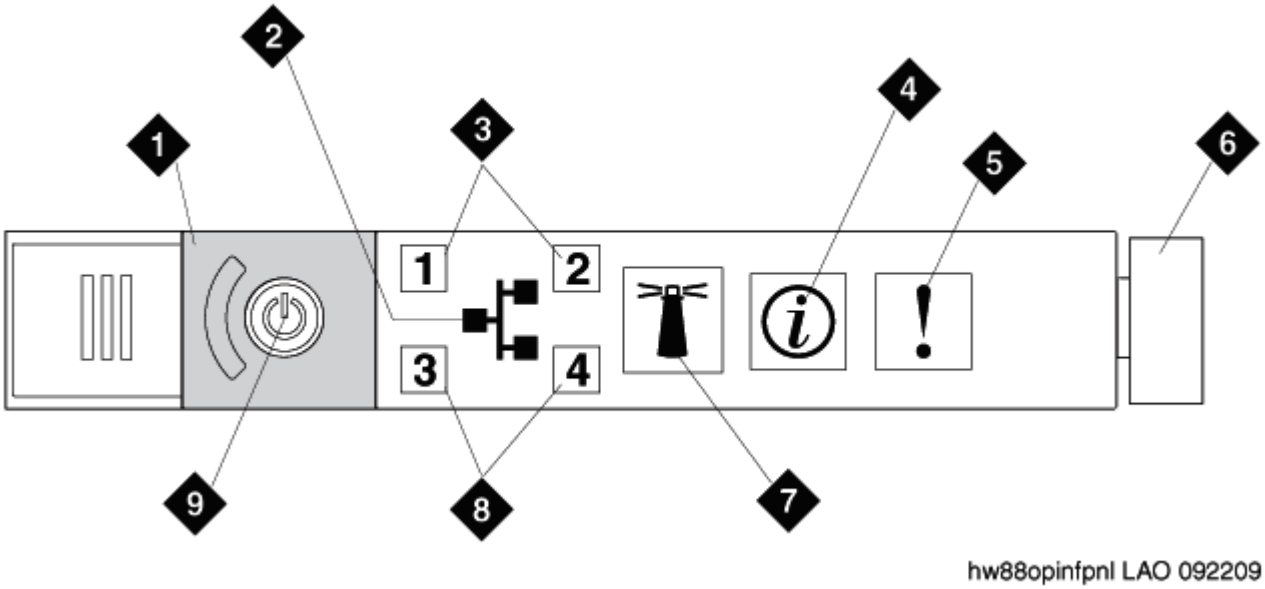
Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 258.

Certain components inside the server have LEDs that light up to indicate the location of a problem. For some components, such as dual inline memory modules (DIMMs) and fans, these LEDs can help you identify the problem. For other components, these LEDs are not useful.

Orange on a component or an orange label on or near a component indicates that the component can be hot-swapped, which means that you can remove or install the component while the server is running. Orange can also indicate touch points on hot-swap components. See the instructions for removing or installing a specific hot-swap component for any additional procedures that you might have to perform before you remove or install the component.

Operator information panel

The operator information panel is located on the front of the server.



hw88opinfpnl LAO 092209

1	Power control button cover
2	Ethernet icon LED
3	Ethernet activity LEDs These LEDs indicate that the server is transmitting or receiving signals on the Ethernet port that corresponds to the lit LED.
4	Information LED

Table continues…

	This LED indicates that a noncritical event has occurred. An LED on the light path diagnostics panel also lights up to help isolate the error.
5	System error LED This LED indicates that a system error has occurred. An LED on the light path diagnostics panel also lights up to help isolate the error.
6	Release latch Slide this latch to the left to access the light path diagnostics panel, which is behind the operator information panel.
7	Locator button and LED Use this LED to visually locate the server among other servers. It is also used as the physical presence for Trusted Platform Module (TPM). Press this button to turn on or turn off this LED locally. You can use IBM Systems Director to light this LED remotely. A system locator LED on the back of the server also lights up when this LED lights up.
8	Ethernet activity LEDs These LEDs indicate that the server is transmitting or receiving signals on the Ethernet port that corresponds to the lit LED.
9	Power control button and power-on LED Press this button to turn the server on and off. The states of the power-on LED are: • Off: AC power is not present, or the power supply or the LED itself has failed. • Flashing rapidly (4 times per second): the server is turned off and is not ready to be turned on. The power-control button is disabled. The power-control button becomes active approximately three minutes after the server is connected to AC power. • Flashing slowly (once per second): the server is turned off and is ready to be turned on. You can press the power-control button to turn on the server. • Lit: The server is turned on. **Note:** If this LED is off, do not assume that electrical power is absent in the server. The LED might be burned out. To remove all electrical power from the server, you must disconnect the power cord from the electrical outlet.

Accessing the light path diagnostics panel

The light path diagnostics panel is on the top of the operator information panel.

Procedure

1. Slide the blue release button on the operator information panel to the left. Pull forward on the unit until the hinge of the operator panel is free of the server chassis.
2. Pull down on the unit, so that you can view the light path diagnostics panel information.

1	Operator information panel

Table continues…

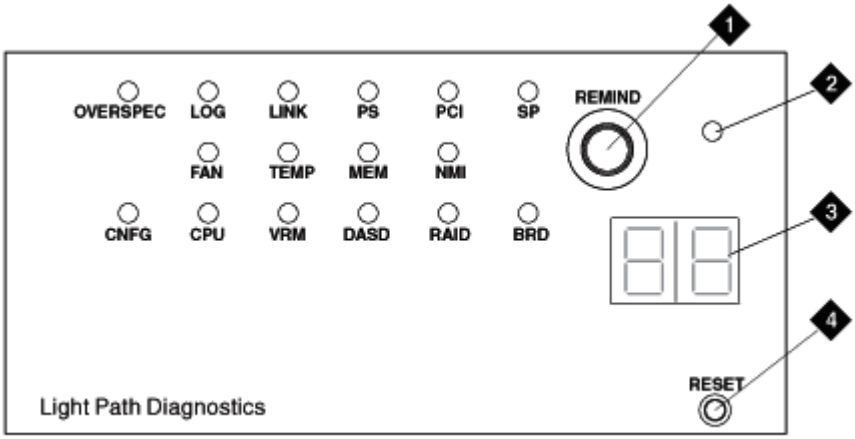
2	Light path diagnostics LEDs
3	Release latch

3. Note any LEDs that light up, and then reinstall the light path diagnostics panel in the server.

Important:

When you slide the light path diagnostics panel out of the server to check the LEDs, do not run the server continuously with light path diagnostics panel outside of the server. The panel should be outside of the server for only a short time. The light path diagnostics panel must remain in the server when the server is running to ensure proper cooling.

Light path diagnostics panel



hw88lpdpnl LAO 092309

1	Remind button Pressing this button places the system-error LED on the front panel into Remind mode. In Remind mode, the system-error LED flashes once every 2 seconds until the problem is corrected, the server is restarted, or a new problem occurs. By placing the system-error LED indicator in Remind mode, you acknowledge that you are aware of the last failure but will not take immediate action to correct the problem. The Integrated Management Module (IMM) controls the remind function.
2	NMI button Pressing this button forces a nonmaskable interruption to the microprocessor. You might have to use a pen or the end of a straightened paper clip to press the button. Use this button only when directed by your service provider.
3	Checkpoint code display The checkpoint code is an internal code used for IBM development only and is subject to change over time. The checkpoint code does not provide error codes or suggest components to be replaced. Ignore this code unless you have a specific request from Avaya to note it .

Table continues…

4	Reset button Pressing this button resets the server and runs the power-on self-test (POST). You might have to use a pen or the end of a straightened paper clip to press the button. The Reset button is in the lower-right corner of the light path diagnostics panel.

Troubleshooting light path diagnostic LEDs

OVERSPEC LED lights up

The OVERSPEC LED on the light path diagnostics panel lights up when the power supplies are using more power than their maximum rating.

Troubleshooting steps

Procedure

1. Check the power-supply LEDs for an error indication. For example, AC LED and DC LED do not both light up, or the information LED lights up. Replace a failed power supply.
2. Replace the server.

LOG LED lights up

The LOG LED on the light path diagnostics panel lights up when an error occurs.

Troubleshooting steps

Procedure

1. If any replaceable components need to be replaced, replace them.
2. If a faulty component is not replaceable, replace the server.

LINK LED lights up

The LINK LED on the light path diagnostics panel is not used.

Troubleshooting steps

Procedure

Ignore unless directed otherwise by Avaya.

PS LED lights up

The PS LED on the light path diagnostics panel lights up when power supply 1 or power supply 2 fails.

Troubleshooting steps

Procedure

1. Check the power supply LEDs for an error indication. For example, AC LED and DC LED do not both light up.
2. Make sure that the power supplies are seated correctly.
3. Remove one of the power supplies to isolate the failed power supply.
4. Replace the failed power supply.

PCI LED lights up

The PCI LED on the light path diagnostics panel lights up when an error occurs on a PCI bus or on the system board. An additional LED lights up next to a failing PCI slot.

Troubleshooting steps

Procedure

1. Check the LEDs on the PCI slots to identify the component that caused the error.
2. If you have a monitor, check the system error log for information about the error.
3. If you cannot isolate the failing PCIe card by using the LEDs and the information in the system error log, remove one card at a time from the failing PCI bus. Restart the server after each card is removed.
4. Reseat the failing PCIe card.
5. Replace the server.

SP LED lights up

The SP LED on the light path diagnostics panel lights up when an error occurs on the service processor.

Troubleshooting steps

Procedure

1. Disconnect the server from the power source, and then reconnect the server to the power source and restart the server.
2. Report this error to your service provider for possible server replacement.

FAN LED lights up

The FAN LED on the light path diagnostics panel lights up when a fan fails, is operating too slowly, or has been removed. The TEMP LED might also light up.

Troubleshooting steps

Procedure

1. Reseat the failing fan, which is indicated by a lit LED near the fan connector on the system board.
2. Replace the server.

TEMP LED lights up

The TEMP LED on the light path diagnostics panel lights up when the system temperature exceeds a threshold level. A failing fan can cause the TEMP LED to light up.

Troubleshooting steps

Procedure

1. Make sure that the room temperature is not too high.
2. Make sure that the air vents are not blocked.

3. Determine whether a fan has failed. If it has, replace the server.

MEM LED lights up

The MEM LED on the light path diagnostics panel lights up when a memory configuration is invalid or a memory error occurs (both the MEM LED and CNFG LED might light up).

Troubleshooting steps when both MEM LED and CNFG LED light up

Procedure

1. Make sure that the DIMM configuration is supported.
2. Replace the DIMMs with a supported configuration.

Troubleshooting steps when only MEM LED lights up

Procedure

- If the server did not boot and a failing DIMM LED lights up:
  1. If you have a monitor, check for a PFA log event in the system event log .
  2. Reseat the DIMM.
  3. If the problem still exists, move the DIMM to a different slot.
  4. Look at the DIMM LEDs on the system board:
     - If the DIMM LED that corresponds to the new DIMM socket lights up, replace the DIMM.
     - If the DIMM LED that corresponds to the original DIMM socket lights up, replace the server.
- If the server booted, the failing DIMM is disabled, and the DIMM LED lights up:
  1. If the LEDs light up by two DIMMs and you have a monitor, check the system event log for a PFA event for one of the DIMMs, and then replace that DIMM. Otherwise, replace both DIMMs
  2. If the LED lights up by only one DIMM, replace that DIMM.

NMI LED lights up

The NMI LED on the light path diagnostics panel lights up when a nonmaskable interruption occurs, or you press the NMI button.

Troubleshooting steps

Procedure

1. If you have a monitor, check the system event log for information about the error.
2. Shut down the server and remove the power cord.
3. Check that all plug-in cards and devices are firmly installed.
4. Turn on the server.
5. If the server does not boot, replace the server.

CNFG LED lights up

The CNFG LED on the light path diagnostics panel lights up when a hardware configuration error occurs. This LED is used with the MEM and CPU LEDs.

Troubleshooting steps

Procedure

1. Check that the memory modules are installed in the correct sequence.
2. Check that the memory modules are properly seated.
3. Replace the server.

CPU LED lights up

When only the CPU LED lights up, a microprocessor has failed.

When the CPU and CNFG LEDs light up, an invalid microprocessor configuration has occurred.

Troubleshooting steps

Procedure

1. Determine whether the CNFG LED also lights up.
   - If the CNFG LED does not light up, a microprocessor has failed.
   - If the CNFG LED lights up, then an invalid microprocessor configuration has occurred.
2. Replace the server if the microprocessor has failed.
3. Make sure that the microprocessors are compatible with each other if the microprocessor configuration is invalid.

   The microprocessors must match in speed and cache size. To compare the microprocessor information, run the Setup utility and select **System Information** > **System Summary** > **Processor Details**.

VRM LED lights up

The VRM LED on the light path diagnostics panel is not used.

Troubleshooting steps

Procedure

Ignore unless directed otherwise by Avaya.

DASD LED lights up

The DASD LED on the light path diagnostics panel lights up when a hard disk drive fails or is missing.

Troubleshooting steps

Procedure

1. Check the LEDs on the hard disk drives for the drive with a lit up status LED and reseat the hard disk drive.

2. If the error remains, replace the hard disk drive and then restart the server.

RAID LED lights up

The RAID LED on the light path diagnostics panel is not used.

Troubleshooting steps

Procedure

Ignore unless directed otherwise by Avaya.

BRD LED lights up

The BRD LED on the light path diagnostics panel lights up when an error occurs on the system board.

Troubleshooting steps

Procedure

Replace the server.

System board LEDs

The following figure shows the LEDs on the system board. A lit LED on or beside a component identifies the component as the cause of an error.

Power supply LEDs

Power supply LEDs

1	AC LED (green)
2	DC LED (green)
3	Power supply error LED (amber)

Identifying power supply problems

Power supply LEDs			Description
AC	**DC**	**Error**	
Off	Off	Off	No AC power to the server or a problem with the AC power source. This is a normal condition when no AC power is present. See Server has no AC power on page 248
Off	Off	On	No AC power to the power supply, a problem with the AC power source, or a failed power supply. This condition occurs only when a second power supply is providing power to the server.

Table continues…

Power supply LEDs			Description
AC	DC	Error	
			See Error LED lights up for one power supply on page 248
Off	On	Off	Faulty power supply. See Faulty power supply on page 249
Off	On	On	Faulty power supply. See Faulty power supply on page 249
On	Off	Off	Power supply not fully seated (most typical), faulty power supply, or faulty system board. See Power supply AC LED lights up on page 249
On	Off or flashing	On	Faulty power supply. See Faulty power supply on page 249
On	On	Off	Normal operation
On	On	On	Power supply is faulty but still operational See Faulty power supply on page 249

Troubleshooting power supply problems

Server has no AC power

All power supply LEDs are off when the server has no AC power.

Troubleshooting steps

Procedure

1. Check the AC power to the server.
2. Make sure that the power cord is connected to a functioning power source.
3. Turn the server off and then turn the server back on.
4. Replace the power supply.

Error LED lights up for one power supply

If the power supply Error LED lights up and all other power supply LEDs are off, either the power supply has no AC power, a problem exists with the AC power source, or the power supply failed.

This condition occurs only when a second power supply is providing power to the server.

Troubleshooting steps

Procedure

1. Check the AC power to the server.

2. Make sure that the power cord is connected to a functioning power source.
3. Replace the power supply.

Power supply AC LED lights up

If the power supply AC LED lights up and all other power supply LEDs are off, one of three possible problems exists:

- The power supply is not fully seated (most typical).
- The power supply is faulty.
- The system board is faulty.

Troubleshooting steps

Procedure

1. Reseat the power supply.
2. If the 240 V failure LED on the system board does not light up, replace the power supply.
3. If the 240 V failure LED on the system board lights up, replace the server.

Faulty power supply

Several LEDs and combinations of LEDs can indicate that a power supply is faulty. The following table describes these LEDs and LED combinations.

AC	DC	Error
Off	On	Off
Off	On	On
On	Off or flashing	On
On	On	On

Troubleshooting steps

Procedure

Replace the power supply.

Troubleshooting hard disk drive, power, or memory problems

Customer-provided equipment

The customer must provide the services personnel with the following equipment for the troubleshooting procedures that are described in this section:

- USB keyboard
- USB mouse
- Monitor

Diagnosing server problems

About this task

Use this sequence of tasks to diagnose a problem in the server.

Procedure

1. Check the system-error LED on the operator information panel. If this LED lights up or flashes, check the light diagnostic panel.

   Important:

   When you slide the light path diagnostics panel out of the server to check the LEDs, do not run the server continuously with the light path diagnostics panel outside of the server. The panel should be outside of the server for only a short time. The light path diagnostics panel must remain in the server when the server is running to ensure proper cooling.

2. Check the power supply LEDs and hard disk drive LEDs.
3. If the LED lights up for a component that can be hot swapped, such as a hard disk drive or power supply, reseat the component and see if the alarm clears. If the alarm does not clear, replace the component.

   Orange on a component or an orange label on or near a component indicates that the component can be hot-swapped. (Orange can also indicate touch points on hot-swap components.) See the instructions for removing or installing a specific hot-swap component for any additional procedures that you might have to perform before you remove or install the component.

   Important:

   Do not remove a component with blue touch points while the server is running. Blue touch points indicate that the component cannot be hot swapped.

4. Check all cables and power cords.
5. If the LED lights up for a component that cannot be hot swapped or if the sever is already turned off, connect a customer-provided keyboard, mouse, and monitor to the server.
6. Perform the appropriate shut down procedure for the application that is running on the server.
7. If the LED was lit for a component that cannot be hot swapped, reseat or replace the component. See the procedure for replacing the component. Replaceable components that cannot be hot swapped are:

   - DIMMs
   - RAID battery

8. Check for successful completion of power-on self-test (POST). POST error messages are displayed on the system monitor.

Hard disk drive LEDs

Troubleshooting hard disk drives

Failed hard disk drive

A hard disk drive has failed, and the associated amber hard disk drive status LED lights up.

Troubleshooting steps

Procedure

Replace the hard disk drive.

Important:

Before replacing the hard disk drive, check the documentation for the application that is running on the server. You may need to execute specific commands before replacing a hard disk drive.

After you replace a hard disk drive, the rebuild process takes a minimum of 30 minutes.

A newly installed hard disk drive is not recognized

Troubleshooting steps

Procedure

1. Check the amber status LED for the hard disk drive.
2. If the LED lights up, remove the drive from the bay, wait 45 seconds, and reinsert the drive. Make sure that the drive assembly connects to the hard disk drive backplane.
3. Check the green activity LED and the amber status LED for the hard disk drive:
   - If the green activity LED flashes and the amber status LED does not light up, the drive is recognized by the RAID controller and is working correctly.
   - If the green activity LED flashes and the amber status LED flashes slowly, the drive is recognized by the RAID controller and is rebuilding.
   - If neither LED lights up or flashes, check the hard disk drive backplane (go to next step).
   - If the green activity LED flashes and the amber status LED lights up, replace the drive. If the activity of the LEDs remains the same, go to the next step. If the activity of the LEDs changes, return to step 1.
4. If the application provides information about the RAID status, access that information.
5. Connect a customer-provided keyboard, mouse, and monitor to the server and check the application syslog for errors.

Multiple hard disk drives fail

Troubleshooting steps

Procedure

Replace the server.

Multiple hard disk drives are offline

Troubleshooting steps

Procedure

Replace the server.

A replacement hard disk drive does not rebuild

Troubleshooting steps

Procedure

1. Make sure that the hard disk drive is recognized by the RAID controller card (the green hard disk drive activity LED is flashing).
2. Check the amber status LED for the hard disk drive.
3. If the LED lights up, remove the drive from the bay, wait 45 seconds, and reinsert the drive. Make sure that the drive assembly connects to the hard disk drive backplane.
4. Check the green activity LED and the amber status LED for the hard disk drive:
   - If the green activity LED flashes and the amber status LED does not light up, the drive is recognized by the RAID controller and is working correctly.
   - If the green activity LED flashes and the amber status LED flashes slowly, the drive is recognized by the RAID controller and is rebuilding.
   - If neither LED lights up or flashes, check the hard disk drive backplane (go to next step).
   - If the green activity LED flashes and the amber status LED lights up, replace the drive. If the activity of the LEDs remains the same, go to the next step. If the activity of the LEDs changes, return to step 1.
5. Connect a customer-provided keyboard, mouse, and monitor to the server and check the application syslog for errors.

Troubleshooting power problems

Power control button does not work

The power-control button does not work, and the reset button does work (the server does not start).

Note:

The power control button does not function until approximately three minutes after the server has been connected to AC power.

Approximately five seconds after the server is connected to power, the power-on LED will blink quickly (three flashes per second). Approximately three minutes after the server is connected to power, the power-on LED will blink slowly (one flash per second)

You must wait for the power-on LED to blink slowly (one flash per second) before pressing the power button. If you press the power button while the power-on LED is blinking quickly (three flashes per second), the server will not turn on.

Troubleshooting steps

Procedure

1. Disconnect the server power cords.
2. Connect a customer-provided keyboard, mouse, and monitor to the server.
3. Reconnect the power cords.
4. Check the LEDs on the system board. For some components, such as DIMMs and fans, these LEDs can help you identify the problem. For other components, these LEDs are not useful.
5. Make sure that:
   - The power cords are correctly connected to the server and to a working electrical outlet.
   - The type of memory that is installed is correct.
   - The DIMMs are fully seated and in the correct sequence for the application that is running on the server.
   - The LEDs on the power supply do not indicate a problem.
6. Reseat the DIMMs.
7. Reseat the power supplies.
8. Replace the DIMMs as needed. Restart the server after replacement.
9. Replace the power supplies, one at a time. Restart the server after each replacement.
10. If you just installed an optional device, remove it, and restart the server. If the server now starts, you might have installed more devices than the power supply supports.
11. Replace the server.

Server does not start

Troubleshooting steps

Procedure

1. Check the four 12-volt power LEDs (A, B, C, and D) on the system board.
2. If the Channel A power LED lights up:
   a. Remove all PCIe cards and riser cards.
   b. Try restarting the server.
   c. If the server starts, reinstall the PCIe cards and riser cards, one at a time, to isolate the defective card. Restart the server after reinstalling each PCI riser card.
3. If the Channel D power LED lights up:
   a. Remove all DIMMs and restart the server.
   b. If the server restarts, reinstall the DIMMs, one pair at a time, to isolate the defective DIMM. Restart the server after installing each DIMM.

Server does not turn off

Troubleshooting steps

Procedure

1. Connect a customer-provided keyboard, mouse, and monitor to the server.
2. Press Ctrl+Alt+Delete.
3. Turn off the server by pressing the power-control button and hold it down for 5 seconds.
4. Restart the server.
5. If the server fails POST and the power control button does not work, disconnect the power cord for 20 seconds, and then reconnect the power cord and restart the server.
6. If the problem still exists, replace the server.

Troubleshooting memory problems

Memory displayed is less than memory installed

The amount of system memory that is displayed is less than the amount of installed physical memory.

Troubleshooting steps

Procedure

1. Make sure that:
   - No error LEDs light up on the operator information panel.
   - The DIMMs are seated correctly.
   - If you changed the memory, you updated the memory configuration in the Setup utility.
2. Shut down the server and remove the power cords.
3. Reseat the DIMMs.
4. Reconnect the power cords, and restart the server.
5. Check the amount of system memory.
6. If the problem still exists, replace the server.

Multiple rows of DIMMs in a branch are identified as failing

Troubleshooting steps

About this task

Procedure

1. Reseat the DIMMs.
2. Restart the server.
3. Remove the lowest numbered DIMM pair of those that are identified and replace it with an identical pair of known good DIMMs. Then, restart the server.

4. Repeat Step 3 as necessary. If the failures continue after all identified pairs are replaced, go to step 8.
5. Return the removed DIMMs, one pair at a time, to their original connectors. Restart the server after each pair, until a pair fails.
6. Replace each DIMM in the failed pair with an identical known good DIMM. Restart the server after each DIMM.
7. Replace the failed DIMM. Repeat steps 5 and 6 until you have tested all removed DIMMs.
8. Replace the lowest numbered DIMM pair of those identified. Then, restart the server.
9. Repeat Step 8 as necessary.

Replacing components in the Avaya S8800 Server

Safety information

General safety information

Follow these rules to ensure general safety:

- Observe good housekeeping in the area of the system units during and after maintenance.
  - Place removed covers and other parts in a safe place, away from all personnel, while you service the system unit.
  - Keep your tool case away from walk areas so that people do not trip over the tool case.
- When lifting any heavy object:
  1. Verify that you can stand safely without slipping.
  2. Distribute the weight of the object equally between your feet.
  3. Use a slow lifting force. Never move suddenly or twist when you attempt to lift.
  4. Lift by standing or by pushing up with your leg muscles. This action removes the strain from the muscles in your back. Do not attempt to lift any objects that weigh more than 16 kg (35 lb.) or objects that you think are too heavy for you.
- Do not perform any action that causes hazards to the customer or that makes the equipment unsafe.
- Before you start the system unit, ensure that other technical support staff and customer personnel are not in a hazardous position.
- Do not wear loose clothing that can be trapped in moving parts. Ensure that your sleeves are fastened or rolled up above your elbows. If your hair is long, fasten it.
- Insert the ends of your necktie or scarf inside clothing or fasten the necktie or scarf with a nonconductive clip, approximately 8 cm (3 inches) from the end.
- Do not wear jewelry, chains, metal-frame eyeglasses, or metal fasteners for your clothing. Metal objects are good electrical conductors.
- Remove items from your shirt pocket, such as pens and pencils, that could fall into the server as you lean over it.

- Wear safety glasses when you are working in any conditions that might be hazardous to your eyes.
- Avoid dropping any metallic objects, such as paper clips, hairpins, and screws into the server.
- After service, reinstall all safety shields, guards, labels, and ground wires. Replace any safety device that is worn or defective.
- Reinstall all covers correctly before returning the server to service.

Warning:

To prevent access to electrical hazards by unauthorized personnel and to ensure continued compliance with international radiated emissions requirements, tighten all captive screws securely so they cannot be loosened without the use of a tool.

Safety Inspection

Use this list to identify potentially unsafe conditions related to the server. When the server was designed and built, the required safety items were installed on each server to protect users and technical support staff from injury. If any unsafe conditions are present, determine how serious the apparent hazard is and whether you can safely continue without first correcting the problem.

Consider these conditions and the safety hazards they present:

- Electrical hazards, especially primary power. Primary voltage on the frame can cause serious or fatal electrical shock.
- Explosive hazards, such as a damaged monitor face or bulging capacitor.
- Mechanical hazards, such as loose or missing hardware.

Perform the following safety checks when servicing this unit:

1. Check exterior covers for damage such as loose, broken, or sharp edges.
2. Shutdown the system and unplug the AC power cords.
3. Check the power cord:
   - Verify that the third-ground connector is in good condition. Use an ohmmeter to measure third-wire ground continuity for 0.1 ohm or less between the external ground pin and frame ground.
   - Verify that the power cord is the appropriate type.
   - Verify that insulation is not frayed or worn.
4. Check inside the server for any obvious unsafe conditions, such as metal filings, contamination, water or other liquids, or signs of fire or smoke damage.
5. Check for worn, frayed, or pinched cables.
6. Verify that the power-supply cover fasteners, such as screws or rivets, have not been removed or tampered with.
7. If you notice any damage, replace the appropriate system components.

Electrical safety rules

Electrical current from power, telephone, and communication cables can be hazardous. To avoid any shock hazard, you must disconnect all power cords and cables.

Observe the following rules when working on electrical equipment.

- Find the room emergency power-off (EPO) switch, disconnecting switch, or electrical outlet. If an electrical accident occurs, you can then operate the switch or unplug the power cord quickly.
- Do not work alone under hazardous conditions or near equipment that has hazardous voltages.
- Disconnect all power before:
  - Doing a mechanical inspection
  - Working near power supplies
  - Removing or installing servers
- Before you start to work on the server, unplug the power cord. If you cannot unplug it, ask the customer to switch off the wall box that supplies power to the server. Afterwards, lock the wall box in the off position.
- If you must work on a server that has exposed electrical circuits, observe the following precautions:
  - Ensure that another person, familiar with the power-off controls, is near you. Another person must be there to switch off the power if necessary.
  - Stand on suitable rubber mats to insulate you from grounds such as metal floor strips and system unit frames. Obtain the mats locally, if necessary.
  - When using testers, set the controls correctly and use the approved probe leads and accessories for the tester.
  - Use only one hand when working with powered-on electrical equipment. Keep the other hand in your pocket or behind your back. This precaution can prevent current from passing through your body.
- Regularly inspect and maintain your electrical hand tools for safe operational condition. Do not use worn or broken tools and testers.
- Never assume that power was disconnected from a circuit. First, verify that the unit is turned off.
- Always look carefully for possible hazards in your work area. Examples of hazards are moist floors, non-grounded power extension cables, and missing safety grounds.
- Do not touch live electrical circuits with the reflective surface of a plastic dental mirror. The surface is conductive. Touching a live circuit can cause personal injury and damage to the server.
- Use only approved tools and test equipment. Some hand tools have handles covered with a soft material that does not insulate you when working with live electrical currents.
- Many customers place rubber floor mats that contain small conductive fibers to decrease electrostatic discharges near the equipment. Do *not* use this type of mat to protect yourself from electrical shock.

If an electrical accident occurs:

- Use caution. Do not become a victim yourself.
- Turn off power.
- Send another person to get medical aid.

Protecting against ESD damage

Any system component that contains transistors or integrated circuits is sensitive to electrostatic discharge (ESD). ESD damage can occur when there is a difference in charge between objects. Protect against ESD damage by equalizing the charge. The server, the part, the work mat, and the person handling the part must all be at the same charge.

Packaging materials that contain ESD-sensitive components are usually marked with a yellow and black warning symbol.

⚠ Caution:

You must observe proper grounding techniques to prevent the discharge of static electricity from your body into ESD-sensitive components.

To avoid damaging ESD-sensitive components:

- Limit your movement. Movement can cause static electricity to build up around you.
- Keep the parts in protective packages until you are ready to install them into the server. If it is necessary to set down a part, put it back into its static-protective package. Do not place the part on the server cover or on a metal surface.
- Place parts on a grounded surface before removing them from their containers.
- Handle the components only after attaching a wrist strap to your bare wrist. Attach the other end of the wrist strap to a ground that terminates at the system ground, such as any unpainted metallic chassis surface.
- Handle a circuit board by the faceplate or side edges only. Avoid touching pins, leads, or circuitry. Hold devices such as a hard disk drive in the same manner. The ESD-sensitive area of these components is located on the bottom surface.

  ⚠ Caution:

  Make sure that the unprotected part of your hand is not in contact with the non-component side of the board.
- Keep components away from plastics and other synthetic materials such as polyester clothing. Most clothing is insulative and retains a charge even when you wear a wrist strap.
- Do not hand components to another person unless that person is grounded at the same potential level. In general, avoid contact with other people.
- Use the black side of a grounded work mat to provide a static-free work surface. The mat is especially useful when handling ESD-sensitive devices.
- Take additional care when handling devices during cold weather. Heating reduces indoor humidity and increases static electricity.
- Verify that the ESD protective devices you use are ISO 9000 certified as fully effective.

Material codes for replaceable components

Component	Material code
2GB DIMMs 1333 Mhz	700478274

Table continues…

Component	Material code
146 GB SAS 2.5” 10K RPM hard disk drive	700478316
146 GB SAS 2.5” 15K RPM hard disk drive	700478324
2-port Ethernet card (PCIe card)	700478290
675 watt power supply	700478308
RAID battery	700478753
Replacement server	

Returning defective equipment

Procedure

1. Place the defective equipment in the protective packaging that accompanied the replacement equipment.
2. Return the defective equipment to Avaya using the procedures established for your region.

Removing and installing the server cover

Removing the server cover

Before you begin

Before you disconnect the server from the power source, make a note of which LEDs light up, including the LEDs that light up on the operation information panel, on the light path diagnostics panel, and LEDs inside the server on the system board. Once you disconnect the server from the power source, you lose the ability to view the LEDs because the LEDs do not light up when the power source is removed.

About this task

Remove the server cover to access the server's internal components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 258.

Procedure

1. If you are planning to view the error LEDs that are on the system board and components, leave the server connected to power.
2. If you are planning to install or remove a DIMM, PCI card, battery, or other non-hot swap device:
   a. Turn off the server and all attached devices.
   b. Label and disconnect all power cords and external cables.
3. If the server has been installed in a rack, slide the server out from the rack enclosure.
4. Lift the server cover off the server and set it aside.

Important:

For proper cooling and airflow, replace the cover before you turn on the server. Operating the server for extended periods of time (over 30 minutes) with the cover removed might damage server components.

Installing the server cover

About this task

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 258.

Procedure

1. Make sure that all internal cables, PCIe cards, and other components are installed and seated correctly and that you have not left loose tools or parts inside the server. Also, make sure that all internal cables are correctly routed.
2. Slide the server all the way into the rack until it latches.
3. Reconnect the external cables and power cords.

Replacing memory modules

Sequence for populating DIMM connectors

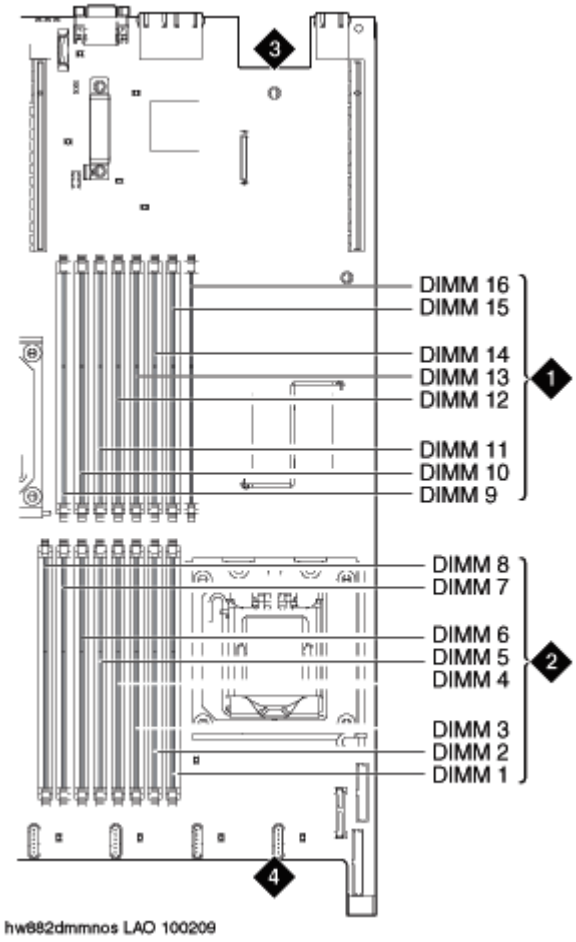
To optimize system performance, install dual in-line memory modules (DIMMs) in the sequence that is shown in the following table.

Installed microprocessors	DIMM connector population sequence
Microprocessor 1	3, 6, 8, 2, 5, 7, 1, 4
Microprocessor 2	11, 14, 16, 10, 13, 15, 9, 12

Note:

Dual microprocessors require equal distribution of DIMMs between the processors. For example, a 12GB DIMM would have connectors 3,6,8 and 11,14,16 populated.

The following figure shows the numbering sequence of the DIMMs.



1	DIMMs for microprocessor 2
2	DIMMs for microprocessor 1
3	Back of server
4	Front of server

Removing the DIMM air baffle

About this task

You must remove the DIMM air baffle to replace or install a memory module.

Caution:

For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with a missing air baffle might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 258.

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Remove the cover.

Removing a memory module

Before you begin

Remove the DIMM air baffle.

About this task

Important:

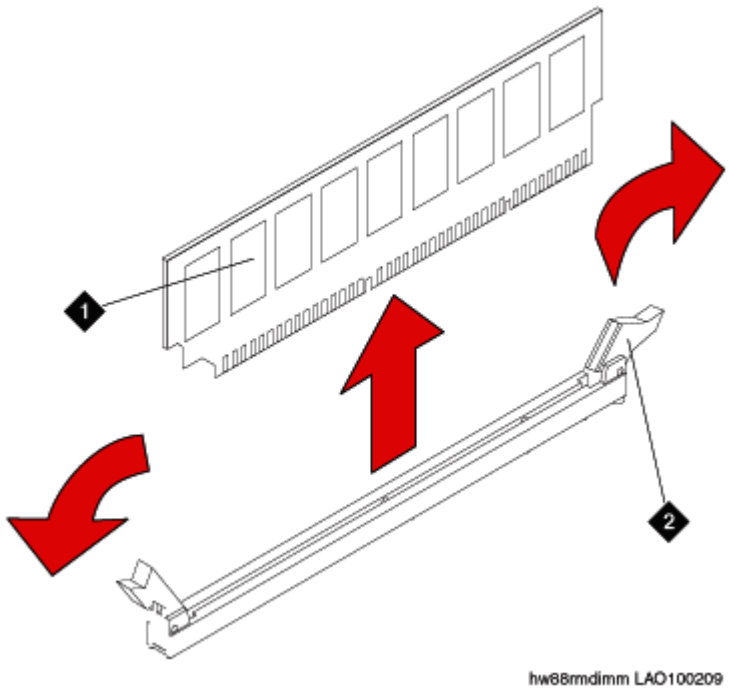
Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 258.

Procedure

Carefully open the retaining clips on each end of the memory module connector and remove the memory module. See the following figure.

Important:

Open and close the clips gently to avoid breaking the retaining clips or damaging the memory module connectors.



1	Memory module
2	Retaining clip

When you install or remove memory modules, the server configuration information changes. When you restart the server, the system displays a message that indicates that the memory configuration has changed.

Next steps

Install a memory module.

Installing a memory module

Before you begin

Remove the DIMM air baffle.

About this task

Important:

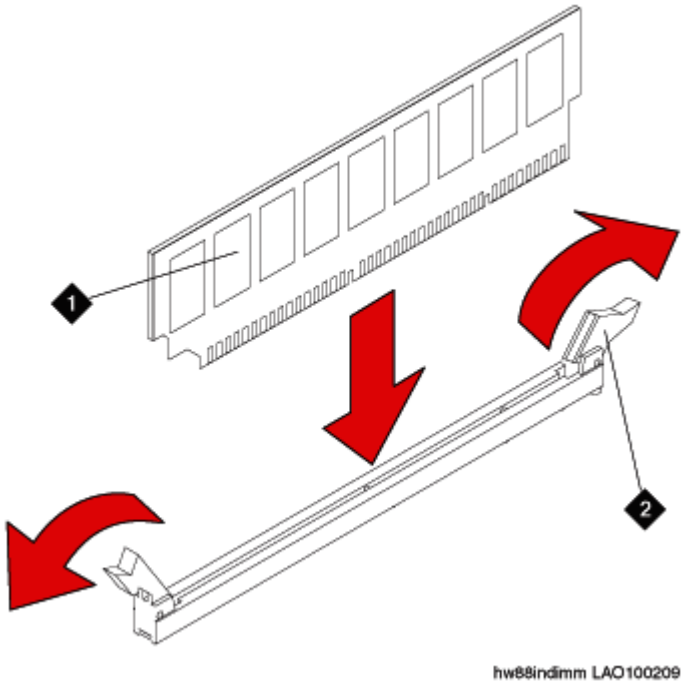
Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 258.

Procedure

1. Carefully open the retaining clips on each end of the memory module connector. See the following figure.

   Important:

   Open and close the clips gently to avoid breaking the retaining clips or damaging the memory module connectors.



1	Memory module
2	Retaining clip

2. Touch the static-protective package that contains the memory module to any unpainted metal surface on the server.
3. Remove the memory module from the package.
4. Turn the memory module so that the memory module keys align correctly with the connector.
5. Insert the memory module into the connector by aligning the edges of the memory module with the slots at the ends of the memory module connector.
6. Firmly press the memory module straight down into the connector by applying pressure on both ends of the memory module simultaneously.

   The retaining clips snap into the locked position when the memory module is firmly seated in the connector.

   Important:

   If there is a gap between the memory module and the retaining clips, the memory module has not been correctly inserted. Open the retaining clips, remove the memory module, and then reinsert it.
7. Replace the air baffle over the memory modules. Make sure all cables are out of the way.
8. Install the cover.
9. Reconnect the external cables and power cords.
10. Turn on the attached devices and the server.

    When you install or remove memory modules, the server configuration information changes. When you restart the server, if a monitor and keyboard are connected, the system displays a message that indicates that the memory configuration has changed.

Installing the DIMM air baffle

About this task

You must install the DIMM air baffle after you install a memory module.

Caution:

For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with a missing air baffle might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 258.

Procedure

1. Lower the air baffle into place. Make sure that all cables are out of the way.
2. Install the cover.

3. Reconnect the external cables and power cords.
4. Turn on the attached devices and the server.

Removing and installing a PCI riser-card assembly

Removing a PCI riser-card assembly

About this task

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 258.

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Remove the cover.
4. If a card is installed in the PCI riser-card assembly, disconnect any cables that are connected to the card.
5. Place the riser-card assembly on a flat, static-protective surface.

Next steps

Installing a PCI riser-card assembly

Before you begin

Reinstall any PCIe cards and reconnect any internal cables that you removed.

About this task

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 258.

Procedure

1. Press down on the riser-card assembly. Make sure that the assembly is fully seated in the riser-card connector on the system board.
2. Install the cover.
3. Reconnect the external cables and power cords.
4. Turn on the attached devices and the server.

Replacing a PCIe card

Removing a PCIe card

Before you begin

Remove the PCI riser-card assembly.

About this task

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 258.

Procedure

Carefully grasp the card by its top edge or upper corners, and pull the card from the PCI expansion slot. See the following figure.

Next steps

Install a PCIe card.

Installing a PCIe card

Before you begin

Remove the PCIe card.

About this task

Caution:

When you install a PCIe card, make sure that the card is correctly seated in the riser-card assembly and that the riser-card assembly is securely seated in the riser-card connector on the system board before you turn on the server. An incorrectly seated PCIe card might cause damage to the system board, the riser-card assembly, or the PCIe card.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 258.

Procedure

1. Install the riser-card assembly in the server.
2. Perform any configuration tasks that are required for the PCIe card.
3. Install the cover.
4. Reconnect the external cables and power cords.
5. Turn on the attached devices and the server.

Replacing a hard disk drive

Removing a hard disk drive

About this task

Important:

To ensure adequate system cooling, do not operate the server for more than 2 minutes without either a hard disk drive or a filler panel installed in each bay.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 258.

Procedure

Grasp the handle and slide the drive out of the drive bay approximately 25 mm (1 inch). Wait until the drive stops spinning before you remove the drive completely from the bay.

Next steps

Install a hard disk drive.

Installing a hard disk drive

Before you begin

If replacing an existing hard drive, remove the hard drive that you want to replace.

About this task

Important:

To ensure adequate system cooling, do not operate the server for more than 2 minutes without either a hard disk drive or a filler panel installed in each bay.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 258.

Procedure

1. Touch the static-protective package that contains the drive to any unpainted metal surface on the server.
2. Remove the drive from the package and place it on a static-protective surface.
3. Make sure that the tray handle is in the open (unlocked) position.
4. Align the drive assembly with the guide rails in the bay. See the following figure.
5. Gently push the drive assembly into the bay until the drive stops.
6. Push the tray handle to the closed (locked) position.
7. If the drive was hot-swapped, check the hard disk drive status LED to verify that the hard disk drive is operating correctly.

   After you replace a failed hard disk drive, the green activity LED flashes as the disk is accessed. When the new drive starts to rebuild, the amber LED flashes slowly, and the green activity LED remains lit during the rebuild process. The rebuild process takes approximately 30 minutes. An amber LED that remains lit indicates a faulty drive that you must replace.

Replacing a power supply

Removing a power supply

About this task

Caution:

To remove all electrical current from the server, ensure that all power cords are disconnected from the power source. The power control button on the server does not turn off the electrical current supplied to the server. The server also might have more than one power cord.

Caution:

Never remove the cover on a power supply or any part that has the following label attached.

hw88vltwrn LAO100209

Hazardous voltage, current, and energy levels are present inside any component that has this label attached. These components do not contain any serviceable parts. If you suspect a problem with one of these parts, replace the power supply.

Important:

During normal operation, each power supply bay must contain either a power supply or power supply filler for proper cooling.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 258.

Procedure

1. If the server has only one power supply, turn off the server and peripheral devices and disconnect all power cords. If the server has two power supplies, you can replace one power supply while the server is running.
2. If the server is in a rack, at the back of the server, pull back the cable management arm to gain access to the rear of the server and the power supply.
3. Press and hold the orange release tab to the left. See the following figure.
4. Pull the power supply part of the way out of the bay, and then release the latch and support the power supply as you pull the power supply the rest of the way out of the bay.

Next steps

Install a power supply.

Installing a power supply

About this task

Caution:

To remove all electrical current from the server, ensure that all power cords are disconnected from the power source. The power control button on the server does not turn off the electrical current supplied to the server. The server also might have more than one power cord.

Caution:

Never remove the cover on a power supply or any part that has the following label attached.

hw88vltwrn LAO100209

Hazardous voltage, current, and energy levels are present inside any component that has this label attached. These components do not contain any serviceable parts. If you suspect a problem with one of these parts, replace the power supply.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 258.

Procedure

1. Touch the static-protective package that contains the power supply to any unpainted metal surface on the server.
2. Remove the power supply from the package and place the power supply on a static-protective surface.
3. If you are installing a power supply into an empty bay, remove the power-supply filler panel from the power-supply bay.
4. Grasp the handle on the back of the power supply and slide the power supply into the power-supply bay until it clicks. Make sure that the power supply connects firmly into the power supply connector. See the following figure.
5. Route the power cord through the handle so that the power cord does not accidentally become unplugged.
6. Connect the power cord for the new power supply to the power-cord connector on the power supply.
7. Connect the other end of the power cord to a properly grounded electrical outlet.

8. Make sure that both the AC LED and the DC LED on the power supply light up.

   Both LEDs light up when the power supply is operating correctly.

Replacing the RAID battery

Removing the RAID battery

Before you begin

The RAID battery is located on top of the RAID controller card.

The RAID configuration data is preserved when you replace the battery.

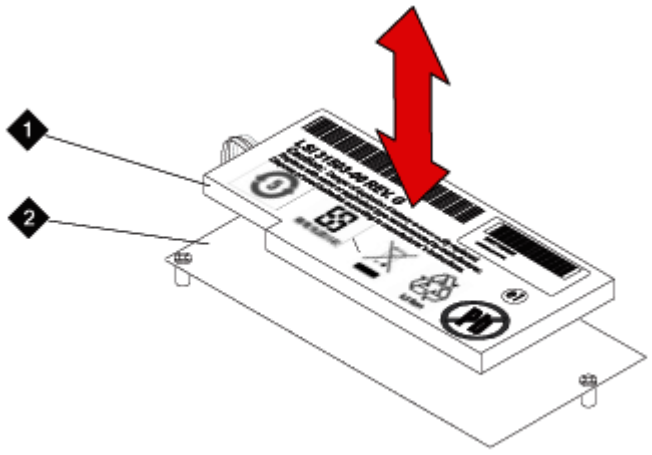
About this task

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 258.

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Remove the cover.
4. Disconnect the cable from the connector on the battery. Leave the other end of the cable connected to the battery carrier.
5. Squeeze the clip on the side of the battery to remove the battery from the battery carrier. See the following figure.



hw881rmrdbt1 LAO100209

1	Battery
2	Battery carrier

6. Put the old battery aside.

Next steps

Install a new RAID battery.

Installing the RAID battery

Before you begin

Remove the existing RAID battery.

About this task

The RAID battery is located on top of the RAID controller card.

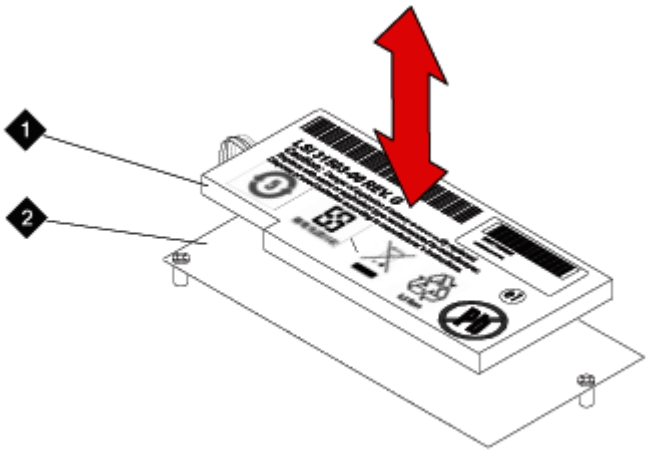
The RAID configuration data is preserved when you replace the battery.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage on page 258.

Procedure

1. Connect the battery cable to the connector on the battery.
2. Press the new battery onto the battery carrier until the clip on the side of the battery snaps into place. See the following figure.



hw881rmrdbt1 LAO100209

1	Battery
2	Battery carrier

3. Install the cover.
4. Reconnect the external cables and power cords.
5. Turn on the attached devices and the server.

Replacing an Avaya S8800 Server

Reuse of hardware components in replacement servers

When you replace the Avaya S8800 Server, you must reuse the following components:

- DIMMs if more than two (4 GB capacity)
- Redundant power supply if used
- Any PCIe cards
- Hard disk drives if more than two.

You must remove these components from the defective server and install them in the replacement server.

Required equipment and tools

- Replacement Avaya S8800 Server
- #2 cross-point (Phillips) screwdriver or 3/8 inch flathead screwdriver
- USB keyboard, USB mouse, and monitor
- Electrostatic wrist ground strap and mat

Tasks to replace an Avaya S8800 Server

#	Task	Description	Notes	✔
1	Shut down the server.	If you can shut down the server from the software, do so. Otherwise, press the power button for several seconds to shut down the server.		
2	Disconnect all power cords and external cables.	**Important:** Be sure to label the cables for easy reconnection.		
3	Remove the server from the rack.	See Removing the server from the rack on page 273.		
4	Remove the reusable components from the failed server.	See Reusing hardware components on page 272.		
5	Install the reusable components in the new server.	See Reusing hardware components on page 272.		

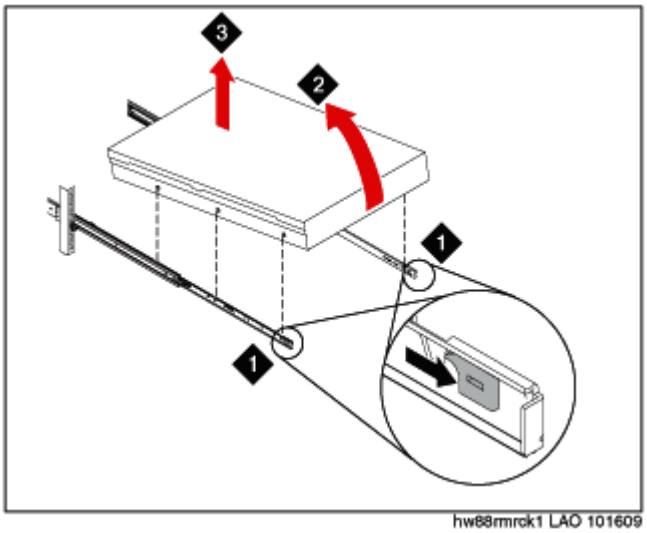
Table continues…

#	Task	Description	Notes	✔
6	Install the new server in the rack.	See Installing the server in the rack on page 273.		
7	Reconnect the external cables and power cords.			
8	Turn on the server.	See Turning on the server on page 275.		

Removing the server from the rack

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Push the locking levers (1) forward. See the following figure.



4. Lift up the front of the server (2). See the preceding figure.
5. Pull the server out of the rack (3). See the preceding figure.

Installing the server in the rack

Before you begin

Attach rails to the rack.

Procedure

1. Pull the slide rails forward until they click, two times, into place. See 1 in Figure 19: Attaching server to slide rails on page 274.
2. Carefully lift the server and tilt it into position over the slide rails so that the rear nail heads on the server line up with the rear slots on the slide rails. See 2 and 3 in Figure 19: Attaching server to slide rails on page 274.

3. Slide the server down until the rear nail heads slip into the two rear slots.
4. Slowly lower the front of the server until the other nail heads slip into the other slots on the slide rails. See 4 in Figure 19: Attaching server to slide rails on page 274.
5. Make sure that the front latch slides over the nail heads. See 5 in Figure 19: Attaching server to slide rails on page 274.

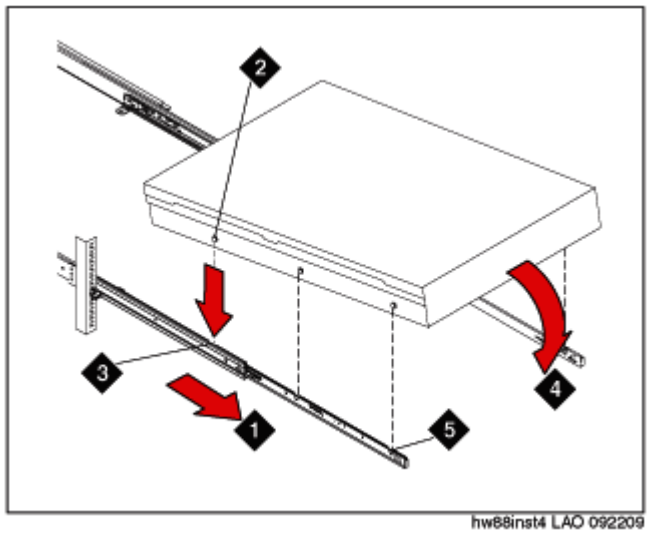


Figure 19: Attaching server to slide rails

6. Lift the locking levers on the slide rails. See 6 in Figure 20: Locking server to slide rails on page 274.
7. Push the server all the way into the rack until it clicks into place. See 7 in Figure 20: Locking server to slide rails on page 274.

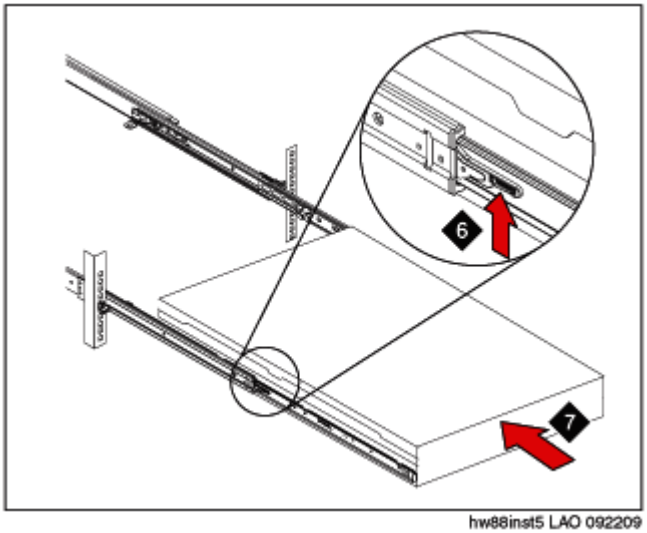


Figure 20: Locking server to slide rails

8. Insert the optional M6 screws in the front of the server when you move the rack cabinet or if you install the rack cabinet in a vibration-prone area. See Figure 21: Installing M6 screws on page 275.

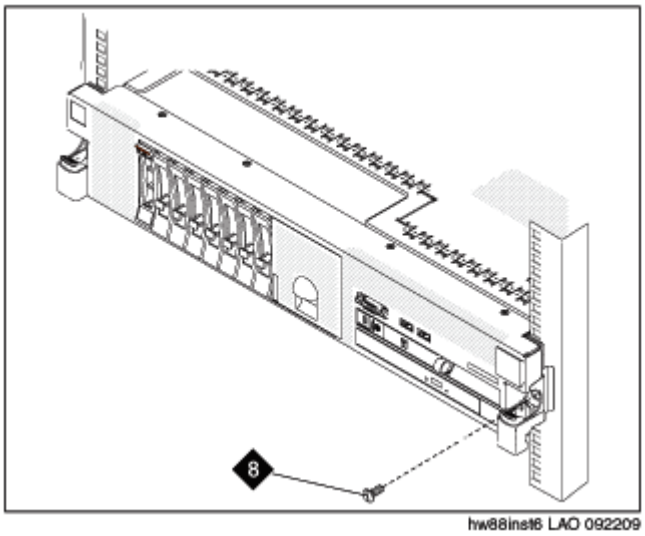


Figure 21: Installing M6 screws

Next steps

Install the cable management arm if desired.

Turning on the server

About this task

After the server is installed in the rack, turn on the server to make sure that it powers up properly. Once you determine that it powers up properly, turn it off before you start any software installation procedure.

Important:

You must wait for the power-on LED to blink slowly (one flash per second) before pressing the power button. If you press the power button while the power-on LED is blinking quickly (three flashes per second), the server will not turn on.

Procedure

1. Plug one end of the power cord into the server power supply and the other end into a UPS or nonswitched outlet.

   Approximately 5 seconds after the server is connected to power, one or more fans might start running to provide cooling, and the power-on LED will blink quickly (three flashes per second). Approximately 3 minutes after the server is connected to power, the power-on LED will blink slowly (one flash per second), and one or more fans might start running.

2. Once the power-on LED begins to blink slowly, press the power button on the front of the server.

The power-on LED will stop blinking and stay lit. After you press the power button, the server takes approximately 5 minutes to initialize.

Next steps

See the specific product documentation for information on installing the operating system and software.

Chapter 12: Troubleshooting software faults

This chapter describes how to identify and correct problems with the Avaya Aura® Conferencing software.

Denial of Service troubleshooting

Denial of Service (DoS) attacks cause excessive SIP messaging or HTTP messaging, which can degrade system performance. To check your DoS configuration, see Configuration errors on page 140.

Important:

If you experience performance degradation in the system with a valid DoS configuration, contact Avaya Support for further assistance.

Patch troubleshooting

Problems upgrading the software can occur either during the command line patch, or during upgrades of the database schema, Avaya Aura® Conferencing Element Manager, Network Elements, or any other components upgraded through the Element Manager Console. If an error occurs during an upgrade or patch, the system attempts to rollback to the previous Maintenance Release or patch load.

Important:

The system does not attempt to rollback any modifications to the database data. You can resolve errors in database data by applying an Maintenance Release or patch to fix the issue, or with a database restore from backups. For information on patching, see *Deploying Business Collaboration Solution 1.0*.

Patching faults

Patching faults may occur in any of the scenarios described below.

Scenario	Where to check for fault information
An error occurs during an Element Manager and database schema Maintenance Release upgrade or patch upgrade.	• Check the command line output after you run `mcpUpgradeMR.pl` or `mcpPatch.pl` scripts. • Check the install script log files. Errors appear as command line output, and the system attempts to rollback to the previous Maintenance Release or patch if an error occurs.

Table continues…

Scenario	Where to check for fault information
An error occurs during a Network Element Maintenance Release upgrade or patch run from the Element Manager Console.	Check the Element Manager Console logs after you run the Maintenance Release upgrade or patch upgrade. The logs indicate a success or failure. The system attempts to rollback to the previous Maintenance Release or patch if an error occurs.
An error occurs during an Maintenance Release upgrade or patch upgrade.	Check the Element Manager Console logs in the stdout, or view the log files in /var/mcp/install. The log files contain entries which indicate the rollback status: • NEMTC 804 INFO Rollback of Upgrade Transaction Initiated • NEMTC 805 INFO Rollback of Patch Transaction Initiated • NEMTC 806 INFO Rollback of Upgrade Transaction Successful • NEMTC 807 INFO Rollback of Patch Transaction Successful • NEMTC 808 INFO Rollback of Upgrade Transaction Failed • NEMTC 809 INFO Rollback of Patch Transaction Failed

Patching fault resolution

You can manually downgrade the system software with the previous Maintenance Release or patch if an error occurred during patching. Reverting to a previous load consists of downgrading the Network Elements to the previous Maintenance Release or patch load. All Network Elements except the database are downgraded. The database stays at the newer software load. The database is not restored from a database backup of the previous Maintenance Release or patch load. Maintenance Releases and patch upgrades of the database are typically backwards compatible. If the database is corrupted or the database upgrade failed, you can only downgrade the database to a previous Maintenance Release or patch. For most database upgrade failures, a database downgrade is not required. Typically you can fix the database upgrade failure by checking the error logs, resolve any issues, and then execute the upgrade again.

Important:

Do not downgrade the system or database unless you understand the impacts associated with downgrading. A database downgrade is a last resort solution to a database problem. Downgrading the database from a backup causes data loss. All database changes, including provisioning and configuration since the last database backup, are lost after a database downgrade.

Performing a manual failover

About this task

The Element Manager supports Hot Standby. If the active Element Manager process fails or there is a network isolation, the secondary Element Manager takes over activity. You can perform a manual failover if the secondary Element Manager is active and you wish to make the primary Element Manager active instead.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements**, **Element Manager** ,**Element Manager**, **NE Maintenance**.
2. In the Element Manager Maintenance window, verify that the Instance 0 is in the Hot Standby state and Instance 1 is in the Active state.
3. In the Element Manager Maintenance window, select **Instance 1**.
4. Click **Stop**.

   The connection to the Element Manager is lost, and the primary Element Manager takes over activity.
5. In the navigation panel of Element Manager Console, select **Feature Server Elements**, **Element Manager**,**Element Manager** , **NE Maintenance**.
6. In the Element Manager Maintenance window, select the **Offline Instance 1**.
7. Click **Start**.

   The system will show the primary Element Manager is in the Active state and the secondary Element Manager is in the Hot Standby state.

Power outage recovery

Use the tasks in this section to recover after a power outage. Perform the tasks in the order provided below. Note, however, that this order is not the way the system comes up if all servers are powered on at the same time.

1. Start and stop the database.
2. Verify that the Element Manager processes are running.
3. Start and stop Element Manager.
4. Verify the status of other server and components.

Starting and stopping the database

About this task

If the database fails to come up after the power outage recovery, perform this task to start and stop the database.

Caution:

The commands in this task severely affect service.

Procedure

1. Use SSH to connect to the database server and log on as user with DBA role.
2. To start the database, perform the following steps:
   a. Type `startDB` and press the **ENTER** key.
   b. Enter the sudo password and press the **ENTER** key.
3. To stop the database, perform the following steps:
   a. Type `stopDB` and press the **ENTER** key.
   b. Enter the sudo password and press the **ENTER** key.

Verifying Element Manager processes are running

About this task

The Element Manager processes on the Element Manager server must be running to control the components from the Element Manager Console.

Procedure

1. Use SSH to connect to the server on which Element Manager is running, and log on as a user with AA role.
2. Type `neinit -p` and press the **ENTER** key.

   If the processes are running, you see output similar to the following:

```
[ntappadm@zngdy0y9 ~]$ neinit -p
Release Name Pid
------- ---- ----
MCP_17.0 EM_0 1638
```

Starting and stopping Element Manager

About this task

Use this task to start and stop Element Manager only if Element Manager failed to come up after the power outage recovery.

Procedure

1. Log on to the Element Manager server as a user with AA role.
2. Type `cd /var/mcp/install` and press the **ENTER** key to change directories.
3. To start Element Manager, type `./emStart.pl` and press the **ENTER** key.
4. To stop Element Manager, type `./emStop.pl` and press the **ENTER** key.

5. To view the Element Manager startup logs, do the following:
   a. Type `cd /var/mcp/oss/log/EM/all/MCP/EM_0` and press the **ENTER** key to change directories.
   b. Type `tail -f *.active` and press the **ENTER** key.

Verifying the status of other servers and components

Procedure

1. In the navigation pane of Element Manager Console, expand each network element.
2. To view the status of a network element, select **NE Maintenance**.
3. To view the network element startup logs, do the following:
   a. Use KVM or SSH to connect to the Element Manager server.
   b. Log on as a user with AA role.
   c. Type `cd /var/mcp/oss/log/EM/all/MCP/<NE Name>` and press the **ENTER** key to change directories.
   d. Type `tail -f *.active` and press the **ENTER** key.
4. To verify whether Provisioning Manager is operating properly, do the following:
   a. Log on to Provisioning Client.
   b. In the Provisioning Client window, select **User Management > Search Users**.
   c. From the Search by box, select **Last Name**.
   d. In the Search for box, enter the last name of a user.
   e. Click **Search**.
   f. If the browser does not respond properly, restart Provisioning Manager.

Element Manager Console troubleshooting

This section provides tasks for troubleshooting Element Manager Console.

Adjusting font display in Element Manager Console

About this task

The Java Runtime Environment (JRE) can conflict with Post Script fonts installed on the management PC. The conflict causes spacing problems with the text displayed in the Element Manager Console window. The text generates an extra space, which cuts off part of the text.

Procedure

1. On the workstation, navigate to to **C:\WINNT\Fonts**.
2. Delete the font files with the extensions **.PFM** or **.PFB**.
3. Restart Element Manager Console.
4. If the Element Manager Console still displays the problem, repeat steps 1 through 3 to check the fonts directory again for files with the **.PFM** or **.PFB** extension.

Resolving a lost connection between the Element Manager and Element Manager Console

About this task

If the connection between the Element Manager and Element Manager Console is lost, a dialog box and a logon prompt appear on your workstation screen.

Procedure

1. Perform basic troubleshooting to determine if the fault is a network or connection-related problem.
2. If the connection is lost because of an Element Manager failover or because of the hosting server, Element Manager Console can be reestablished after the secondary Element Manager takes over activity.

Chapter 13: Troubleshooting Avaya media server faults

Use the tasks in this chapter to identify and correct problems with an Avaya media server.

Avaya media server logs

From Element Management Console, you can:

- enable and disable debug trace on an Avaya media server. See Configuring logs for a media server on page 283.
- change the number of debug trace logs stored in history on an Avaya media server. See Configuring logs for a media server on page 283.
- download logs from an Avaya media server. See Downloading logs for a media server on page 284.

Configuring logs for a media server

About this task

Use this procedure to

- enable or disable debugtrace for a media server. When debugtrace is enabled, the Avaya media server writes logs in the files *Debug.txt in the directory /var/mcp/ma/MAS/common/logs.
- enable or disable system diagnostic mode for a media server. When system diagnostic mode is enabled, the Avaya media server writes logs in the files *Debug.txt in the directory /var/mcp/ma/MAS/common/logs.

Note:

Enabling system diagnostic mode can reduce system performance.

Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > Log Processing > Log Configuration**.

2. In the Media Server Log Configuration dialog box, select the **Enable debugtrace** check box if you want to enable debug traces.
3. Select the **Enable system diagnostic mode** check box if you want to enable system diagnostic mode.
4. Click **Apply**.

Downloading logs for a media server

About this task

Use this procedure to download the logs for a media server to a file. You can also download the debug trace logs for a media server.

Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > Log Processing > Log Download**.
2. In the Media Server Log Download dialog box, select the **Include debug trace logs** check box if you want to download trace logs also.
3. Click **Download**.
4. In the Save dialog box, specify the location and file to which you want to download the media server log(s).
5. Click **Save**.

Monitoring active sessions on a media server

About this task

Use this procedure to monitor active sessions on a media server.

Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > Monitoring > Active Sessions**.
2. In the Active Sessions window, specify the settings you want to use.

Monitoring the performance of a media server

About this task

Use this procedure to monitor the performance of a media server.

Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > Monitoring > Performance Monitor**.
2. In the Performance window, review the performance information for the media server.

Accessing the session detail record browser for a media server

About this task

Use this procedure to access the session detail record browser for a media server.

Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > Session Detail Record Browser**.
2. In the Session Detail Record Browser window, enter your query settings.
3. Click **Execute**.

Rejection of incoming SIP calls

An Avaya media server may reject the incoming SIP calls in any of the following conditions:

- The Avaya media server rejects incoming SIP calls for one or more service types. In this case, use the Log Viewer to identify attempts to launch an uninstalled or unlicensed service.
- The Avaya media server rejects incoming SIP calls using SIP failure responses, such as 403 Forbidden, in the message traces or logs.

To resolve this problem, see Checking Pending Lock state on page 286.

Checking Pending Lock state

About this task

An Avaya media server in the Pending Lock state rejects new service requests, but allows all active sessions to complete. Use this task to determine if the Avaya media server is in Pending Lock state and unlock the server, if required.

Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > Service Maintenance**.
2. In the Media Server Maintenance dialog box, check if the **Admin State** column indicates **Pending Locked**.
3. Click **Unlock** to unlock the server.

Chapter 14: SIP messages and associated treatment causes

Understanding SIP messages and associated treatment causes helps in understanding the call scenarios that generate the SIP messages and how it maps to the treatment cause.

Treatment causes

The following table lists the common treatment causes for SIP messages. The treatment cause number and description is also provided.

Reason	Treatment cause	Description
ADDRESS_INCOMPLETE	484	The server received a request with a Request-URI that was incomplete.
AGCF_CWT_ANNOUNCEMENT	1201	AGCF Call Waiting occurs.
AGCF_HELD_ANNOUNCEMENT	1202	AGCF Hold occurs.
ALL_INCOMING_CALLS_NOT_ALLOWED	1050	Terminating party has Call Screening feature turned on and forbids all incoming calls.
ALL_OUTGOING_CALLS_NOT_ALLOWED	1051	All outgoing calls not allowed due to call screening.
AMBIGUOUS	485	The Request-URI was ambiguous. The response MAY contain a listing of possible unambiguous addresses in Contact header fields. Revealing alternatives can infringe on privacy of the user or the organization.
BAD_EXSTENSION	420	The server did not understand the protocol extension specified in a Proxy-Require or Require header field. The server must include a list of the unsupported extensions in an Unsupported header field in the response.

Table continues…

Reason	Treatment cause	Description
BAD_GATEWAY	502	The server, while acting as a gateway or proxy, received an invalid response from the downstream server it accessed in attempting to fulfill the request.
BAD_REQUEST	400	The request could not be understood due to malformed syntax. The Reason-Phrase should identify the syntax problem in more detail, for example, "Missing Call-ID header field".
BUSY_EVERYWHERE	600	The callee's end system was contacted successfully but the callee is busy and does not wish to take the call at this time. The response may indicate a better time to call in the Retry-After header field.
CALL_LEG_TRANSACTION_DOES_NOT_EXIST	481	This status indicates that the UAS received a request that does not match any existing dialog or transaction.
CALL_PICKUP_FORBIDDEN	1090	CPU VSC Call are closed due to Forbidden message.
CONFLICT	409	User tried to join the call, but dialog is private to him.
CONTENT_NOT_ACCEPTABLE	406	The resource identified by the request is only capable of generating response entities that have content characteristics not acceptable according to the Accept header field sent in the request.
DIGIT_TIMEOUT	1200	Handle case where AGCF sends an incoming INVITE for digit timeout.
DOES_NOT_EXIT_ANYWHERE	604	The server has authoritative information that the user indicated in the Request-URI does not exist anywhere.
EVENT_NOT_SUPPORTED	489	The event package is not registered as the one that Avaya supports.
FORBIDDEN	403	The server understood the request but is refusing to fulfill it.
GATEWAY_TIMEOUT	504	The only reason of GATEWAY_TIMEOUT is DATABASE_FAILURE_ERROR (corresponding code).
GONE	410	The requested resource is no longer available at the server and no forwarding address is known. This condition is expected to be considered permanent.
HOTLINE_VCA	1020	403 Forbidden was received for Hotline call map to HOTLINE_VCA.
HUNT_OVERFLOW	1150	If hunting to next route group member is selected and all hunt group members are unavailable.
INTERNATIONAL_CALLS_NOT_ALLOWED	1054	International calls not allowed due to call screening.
INTERNATIONAL_CARRIER_OVERRIDE_NOT_ALLOWED	1102	User not allowed to override international carrier. User is not allowed to dial-around for international calls and it is not casual dial his pre-subscribed carrier.

Table continues…

Reason	Treatment cause	Description
INTER_RATEAREA_CARRIER_OVERRIDE_NOT_ALLOWED	1101	User not allowed to override inter-rate carrier. User is not allowed to dial-around for inter-rate area calls and it is not casual dial his pre-subscribed carrier.
INTRA_RATEAREA_CARRIER_OVERRIDE_NOT_ALLOWED	1100	User not allowed to override intra-rate carrier. User is not allowed to dial-around for intra-rate area calls and it is not casual dial his pre-subscribed carrier.
LENGTH_REQUIRED	411	Content-Length field is malformed.
LOCAL_CALLS_NOT_ALLOWED	1052	Local calls not allowed due to call screening.
LONG_DISTANCE_CALLS_NOT_ALLOWED	1053	Long distance calls not allowed due to call screening.
LOOP_DETECTED	482	The server has detected a loop.
MCT_FAILURE	499	Malicious Call Trace failed.
MCT_SUCCESS	498	Malicious Call Trace success.
MEDIA_NOT_ACCEPTABLE	606	The user's agent was contacted successfully but some aspects of the session description such as the requested media, bandwidth, or addressing style were not acceptable. A 606 (Not Acceptable) response means that the user wishes to communicate but cannot adequately support the session described.
METHOD_NOT_ALLOWED	405	The method specified in the Request-Line is understood, but not allowed for the address identified by the Request-URI.
NOT_ACCEPTABLE_HERE	488	The response has the same meaning as 606 (Not Acceptable), but only applies to the specific resource addressed by the Request-URI and the request may succeed elsewhere.
NOT_IMPLEMENTED	501	The server does not support the functionality required to fulfill the request. This is the appropriate response when a UAS does not recognize the request method and is not capable of supporting it for any user. (Proxies forward all requests regardless of method.)
NO_CALL_AVAILABLE_FOR_PICKUP	1091	No call available for pickup because call leg transaction does not exist.
PAYMENT_REQUIRED	402	Reserved for future use.
PRECONDITION_FAILED	412	Publish failure because there is problems with entity tag: (no entity tag, Multiple SIP-If-Match headers).
PREMIUM_CALLS_NOT_ALLOWED	1055	Premium calls not allowed due to call screening.
REQUEST_PENDING	491	The request was received by a UAS that had a pending request within the same dialog.

Table continues…

Reason	Treatment cause	Description
QUEUE_CLOSURE	1082	UCD Group is closed/cannot service.
QUEUE_MAXIMUM_SIZE	1081	Maximum queue size of UCD exceeded.
QUEUE_TIMEOUT	1080	Call to UCD group expired.
REQUEST_ENTITY_TOO_LARGE	413	The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.
REQUEST_URI_TOO_LONG	414	The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.
SELECTIVE_REJECT_INCOMING	1056	The originator is being banned by the user directly.
SERVER_INTERNAL_ERROR	500	The server encountered an unexpected condition that prevented it from fulfilling the request. The client may display the specific error condition and may retry the request after several seconds. If the condition is temporary, the server may indicate when the client may retry the request using the Retry-After header field.
SERVICE_UNAVAILABLE	503	The server is temporarily unable to process the request due to a temporary overloading or maintenance of the server. The server may indicate when the client should retry the request in a Retry-After header field. This message is observed when the location of the user is not served by any media server clusters on PROV.
SIPLINES_NOREGDESTS	900	The terminating party is a SIPLines subscriber who is homed to this appsvr and does not have any registered destinations.
STARCODE_SUCCESS	1001	Star code feature used successful.
STARCODE_FAILURE	1002	Using Star code failed.
STARCODE_STATUS_ENABLE	1003	Star code status: enable.
STARCODE_STATUS_DISABLE	1004	Star code status: disable.
STARCODE_CLIR_PER_CALL_SUCCESS	1005	CLIR per call based activation successful.
STARCODE_CLIP_PER_CALL_SUCCESS	1006	CLIP per call based activation successful.
STARCODE_NCWD_PER_CALL_SUCCESS	1007	Call Waiting Disable state is updated for the signal.
STARCODE_CLI_SUCCESS	1008	CLI Notification service successful.

Table continues…

Reason	Treatment cause	Description
STARCODE_CLI_FAILURE	1009	Star code CLI failed because last caller is anonymous or there is no info about last caller.
TOO_MANY_HOPS	483	The server received a request that contains a Max-Forwards header field with the value zero.
UCD_DELAY_ANNOUNCEMENT	1084	UCD Grouped did not answer the call during configured delay time.
UCD_RINGBACK	1083	UCD Group is active. Connect to ringback.
VERSION_NOT_SUPPORTED	505	The server does not support, or refuses to support, the SIP protocol version that was used in the request. The server is indicating that it is unable or unwilling to complete the request using the same major version as the client, other than with this error message.

Index

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W