Avaya Aura® Messaging Multiserver Single Location Reference Configuration

Release 6.3
Issue 1
March 2014

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on 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: http://support.avaya.com 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 a 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 IF YOU PURCHASE A 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, HTTP://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. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO 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 Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, 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.

Licence 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.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

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

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 Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

Note to Service Provider

The Product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

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, 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.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://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: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document describes network architecture, suggested topologies, system capacities, and product interoperability. This document also describes the functional limitations of certain configurations. With this information, sales design specialists can make decisions about designs that meet the business needs of a customer.

Intended audience

This document is intended for people who determine the best design to meet a customer's business needs.

Related resources

Reference configurations

Reference configuration documents describe the performance, limitations, and capacities of specific configurations of Messaging.

Multiserver configurations

Title	Description	Audience
Avaya Aura® Messaging Multiserver Single Location Reference Configuration	Describes the design, capacities, interoperability, and limitations of multiserver configurations deployed at one location.	Sales and deployment engineers, solution architects, and support personnel

Title	Description	Audience
Avaya Aura® Messaging Multiserver Dual Location Reference Configuration	Describes the design, capacities, interoperability, and limitations of multiserver configurations deployed at two locations.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Aura® Messaging for Multiserver Systems	Describes an end-to-end deployment scenario including all products that must function together in a multiserver configuration, checklists, and initial administration.	Deployment engineers and support personnel
Upgrading Avaya Aura® Messaging for Multiserver Systems	Describes end-to-end upgrade scenarios for this configuration.	Deployment engineers and support personnel

You might find the following Avaya Aura® documents useful:

- *Installing and Configuring Avaya Aura® System Platform*
- *Administering Avaya Aura®System Platform*
- *Secure Access Link Gateway Implementation*

Training

You can get the following Messaging courses at https://www.avaya-learning.com. Enter the course code in the **Search** field and click **Go** to search for the course.

The course titles might differ from the titles shown.

Course code	Course title
2U00230W	Avaya UC Messaging — Overview
2U00231W	Avaya UC Messaging — Heritage
2U00232W	Avaya UC Messaging — Avaya Aura® Messaging
2U00233O	Selling Avaya UC Messaging Learning Bytes
3U00141W	Designing UC Messaging — Avaya Aura® Messaging
5U00140E	Avaya Aura® Messaging Implementation and Support
5U00141E	Avaya Aura® Messaging Administration
ATI01674VEN	Avaya Aura® Messaging — Caller Applications

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.

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

Note:

Videos are not available for all products.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. 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.

Chapter 2: Architecture overview

Multiserver single location

In this reference configuration, the application and storage roles are active on different physical servers and deployed at the same location as the telephony server. This configuration does not provide redundancy for the storage role.

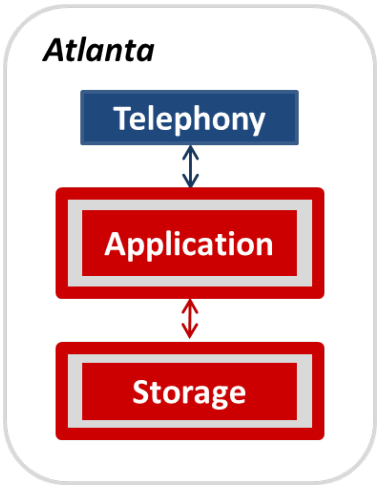
The server types can include any of the following:

- Up to three dedicated application servers for taking calls.
- An optional application server for redundancy, for a total of four clustered application servers.
- One dedicated storage server. You can choose:
  - An Avaya message store running on Avaya-provided hardware, or
  - A Microsoft Exchange Server.
- A dedicated AxC/Directory server. You only need this server when the message store resides on a Microsoft Exchange Server and when your Messaging system must support more than 6000 users.

Topology

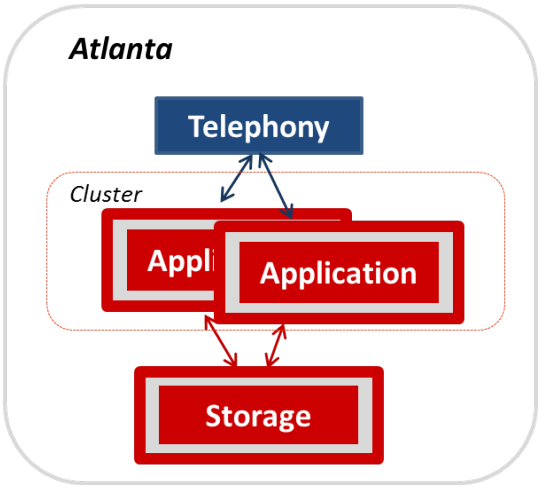
Example A: not clustered

This multiserver, single-location configuration has one dedicated application server and one dedicated storage server and supports up to 6000 users. The dedicated application server communicates with the telephony server and the AxC/Directory that resides on the storage server.



Example C: clustered

This multiserver, single-location configuration has two dedicated application servers and one dedicated storage server and supports up to 12,000 users. You can add a third application server to the cluster to increase the capacity and a fourth server for redundancy. Each application server communicates with the telephony server and the AxC/Directory that resides on the storage server.



Components

The multiserver topology of Avaya Aura® Messaging includes three types of components: Avaya products, third-party products, and Avaya products that provide services to these products.

Avaya Aura® components

Component	Version	Platform	Description
Avaya Aura® Communication Manager	5.2.1 6.3 6.3.2	System Platform	The open, reliable, and scalable IP telephony foundation on which Avaya delivers intelligent communications to large and small enterprises.
Avaya Aura® Messaging	6.3	System Platform	A part of the Avaya Aura® architecture, but you can also Messaging in other environments.
Avaya Aura® Session Manager	6.3.2 6.3.4	System Platform	A SIP routing and integration tool and the core component of the Avaya Aura® solution. Session Manager integrates the SIP entities in the enterprise network.Session Manager offers a new perspective on enterprise communication where Session Managerdoes not manage each location as a separate unit in the enterprise network. You can view and manage each location, branch, and application as a part of the enterprise network.
Avaya Aura® System Manager	6.3.2 6.3.4 6.3.8	System Platform	A product that takes a solution-level approach to network administration. IT departments can use System Manager to

Component	Version	Platform	Description
			incorporate new components and applications under a common management umbrella, managing the Avaya Aura® elements together as a system. System Manager centralizes provisioning, maintenance, and troubleshooting to simplify and reduce management complexity and solution servicing. System Manager provides a common management framework that reduces the complexity of operations for distributed multisite networks with multiple control points inherent in SIP. System Manager also increases the value of convergence by integrating with the enterprise IT infrastructure.
Avaya Aura®System Platform	6.3	System Platform	A server software platform that is generic and virtual and provides a common set of features and services. This set of features and services enables preinstalled and configured virtual applications, called solution

Component	Version	Platform	Description
			templates, to reside on a single physical server. System Platform features include: • Secure Access Link (SAL) to handle alarming and remote access • A consistent upgrade method for all patches and products in the solution template • Security that conforms to Avaya product security standards • WebLM, a web license manager server that manages product licenses • A Network Time Protocol (NTP) clock synchronized to a customer-provided NTP server Avayaoffers product-specific templates that define one or more applications. These templates makes installing different products, such as Messaging, on System Platform easy and efficient.

Avaya products

Component	Version	Platform	Description
Application Server	6.3	System Platform	This component consists of a Linux-

Component	Version	Platform	Description
			based messaging application server. The messaging application provides TUIs which are similar to the following TUIs: • Aria • Audix® • CallPilot®
Avaya Message Store	6.3	System Platform	This component consists of a Linux-based message store. You can deploy Application Server and Avaya Message Store on a single System Platform server. You can also deploy multiple instances of Application Server on a dedicated front-end System Platform server and the multiple instances of Avaya Message Store on a dedicated back-end System Platform server.
Avaya Voice Message Form	6.3	Microsoft Exchange Server	This component provides a toolbar for Microsoft Office Outlook and Exchange Server that supports playback of voice messages on the telephone through the computer. You can deploy this toolbar on Exchange Server.

Component	Version	Platform	Description
Message Networking	5.2	Avaya server with Red Hat Enterprise Linux	This component supports interoperability with legacy voice mail products.
one-X Speech	5.2 6.3	Windows Server 2003 for one-X Speech Release 5.2 Windows Server 2012 for one-X Speech Release 6.3	This component supports the speech-based commands and the text-to-speech functions for voice mail, email, calendar, and telephony functions.

Third-party products

Component	Description
Microsoft Exchange	You can configure Microsoft Exchange as storage destination for your Messaging system.
AudioCodes SIP gateway	Messaging uses SIP for integration with mixed telephony server environments. AudioCodes Mediant 1000 and 1000B gateways allow the Messaging system to connect to third-party telephony servers that Session Manager does not support.
Nuance Loquendo Text to Speech	This components supports conversion of text to speech.
EVM Plus giSTT	This component is a unified messaging application that provides speech-to-text functions for voice mail. Using this application, you can read, listen, and control your voice mail.
Mutare Message Mirror	This component recovers voice messages, greetings, names, passwords, and LDAP data in the event of a catastrophic system failure.

Servers

HP ProLiant DL360p G8 specifications

Component name	Standard server	High capacity server
Chassis	1U	1U

Component name	Standard server	High capacity server
Processor speed	E5-2630 2.3 GHz	E5-2630 2.3 GHz
Number of processors	1	1
Ethernet ports	6	4
RAID type	RAID 1	RAID 5
Disk	2 x 300 GB 10K	3 x 300 GB 15K
Standard power supply	1 x 460 W	2 x 460 W

HP ProLiant DL360 G7 specifications

Component name	Standard server	High capacity server
Chassis	1U	1U
Processor speed	E5620 2.4 GHz 4–core	E5620 2.4 GHz 4–core
Number of processors	1	1
System memory	12 GB	12 GB
Ethernet ports	2	2
RAID type for phase 1 servers	RAID 5	RAID 5
Disk for phase 1 servers	3 x 146 GB 10k	4 x 146 GB 15k
RAID type for phase 2 servers	RAID 1	RAID 5
Disk for phase 2 servers	2 x 300 GB 10k	4 x 146 GB 15k
Standard power supply	1 x 460 W	2 x 460 W

Note:

Phase 1 servers shipped for the first half of the HP ProLiant DL360 G7general availability life cycle. Phase 2 servers shipped for the second half. The disk configuration for the phases are different.

Dell™ PowerEdge™ R620 specifications

Component name	Standard server	High capacity server
Chassis	1U	1U

Component name	Standard server	High capacity server
Processor speed	E5-2630 2.3 GHz 6-core	E5-2630 2.3 GHz 6-core
Number of processors	1	1
Ethernet ports	6	4
RAID type	RAID 1	RAID 5
Disk	2 x 300 GB 10K	3 x 300 GB 15K
Standard power supply	1 x 495 W	2 x 495 W

Dell™ PowerEdge™ R610 specifications

Component name	Standard server	High capacity server
Chassis	1U	1U
Processor speed	E5620 2.4 GHz 4-core	E5620 2.4 GHz 4-core
System memory	12 GB	12 GB
Ethernet ports	2	2
RAID type for phase 1 and 2 servers	RAID 5	RAID 5
Disk for phase 1 servers	3 x 146 GB 10K	4 x 146 GB 15K
Disk for phase 2 servers	3 x 146 GB 15K	4 x 146 GB 15K
Standard power supply	1 x 502 W	2 x 502 W

Note:

Phase 1 servers shipped for the first half of the Dell Power Edge R610 general availability life cycle. Phase 2 servers shipped for the second half. The disk configuration for the phases are different.

S8800 1U specifications

Component name	Standard server	High capacity server
Chassis	1U	1U
Processor speed	E5520 Quad-core 2.26 GHz	E5520 Quad-core 2.26 GHz
Number of processors	1	1
System memory	12 GB	12 GB

Component name	Standard server	High capacity server
Ethernet ports	2	2
RAID type	RAID 5	RAID 5
Disk	3 x 146 GB 10k rpm SAS hard disk drives	4 x 146 GB 15k rpm SAS hard disk drives
Standard power supply	Single power supply	Dual power supplies

Supported hardware

Linux®-based servers

Messaging software runs on the following Avaya-provided servers:

- Dell™ PowerEdge™ R620
- Dell™ PowerEdge™ R610
- HP ProLiant DL360p G8
- HP ProLiant DL360 G7

If you already have the following servers in your network, you can use them with Messaging. However, you must first get an upgrade kit from your Avaya Services representative.

Server	Supporting documentation
S8730	*Maintaining the S8730 server for Modular Messaging*
CallPilot 1006r	*CallPilot 1006r Hardware Upgrade Instructions*
S8800 1U	*Maintaining the AvayaS8800 1U Server for Avaya Aura® Messaging*

You can download these documents from the Avaya Support website at http://support.avaya.com.

VMware®-based servers

Messaging software runs on ESXi host servers.

Avaya does not provide servers for your VMware environment. But you can get compatibility information for servers from the VMware website at: http://www.vmware.com/resources/guides.html. This website also has information about the VMware infrastructure, including I/O, storage/SAN, backups, and interoperability.

Product compatibility

For the latest and most accurate compatibility information go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Test strategy summary

The Messaging system verification team performs multiple tests on the Messaging software to verify the performance, reliability, scalability, and the resource use of Messaging. The tests include verification of the updated functions and features, Messaging upgrade paths, and the migration of external databases to Messaging.

Test	Description
New feature test	Functioning of the new features validated and the performance of the features tested.
Regression test	Manual and automated regression tests to verify the performance of the updated functions and features.
Performance test	Performance tested to verify the responsiveness and the stability of Messaging. The tests include verifying the scalability, reliability, and the resource use of Messaging.
Upgrade test	Upgrade paths tested to verify the supported releases to upgrade Messaging. Messaging supports upgrades from Release 6.0.1 and later releases. For more information, see *Upgrading Avaya Aura® Messaging* at the Avaya Support website: http://support.avaya.com/.
Interoperability testing	Compatibility tested with other products to verify how Messaging interoperates with the products. For more information about the supported products, see *Components*.
Bug fix verification	Debugging of Messaging to resolve bugs that originate during the performance testing verified.
Migration testing	Migration of external databases to Messaging tested.
Solution testing	Multiple features of Messaging tested simultaneously to emulate a customer scenario and verify the performance of Messaging.

Test	Description
Launch readiness testing	The final version of the Messaging software tested, which includes regression testing and testing of selected new features.

Chapter 3: Design considerations

Caveats and limitations

Consider the following limitations when you deploy a multiserver Messaging configuration:

- The smallest multiserver system has one application server and one storage server and supports up to 6000 users. Although this capacity is slightly more than the capacity of the single server configuration, you can increase the capacity by adding application servers.
- Clustering the application servers provides redundancy for the application role because clustered application servers share the traffic load. For full redundancy without the interruption of service or the loss of data, the system capacity must be large enough to carry peak traffic load with one disabled application server.
- The maximum number of ports for an application server is 100, and the maximum number for the system is 300. However, you can cluster four application servers. The fourth server takes calls and provides redundancy. The fourth server does not increase the capacity of your system.

Multiserver capacity and scalability

You can use a maximum of four application servers for each Messaging system. You can use a cluster of up to three application servers for a maximum of 300 ports. You can also add a fourth application server to the cluster for redundancy as long as the active traffic does not exceed 300 ports. Messaging supports 20000 users with an Avaya message store.

The following table shows port and mailbox capacity for the standard server and the high capacity storage server, using the G.711 codec.

Server	Application server	Storage server
Standard server	Ports: 100 Users: 6000	2666 hours for 6000 20–minute mailboxes 2750 hours for 5500 30–minute mailboxes
High capacity storage server	Ports: 100 Users: 6000	6666 hours for 20000 20–minute mailboxes

Server	Application server	Storage server
		6750 hours for 13500 30–minute mailboxes

Migration roadmap and limitations

Migrations

Messaging supports migrations from the following products:

- Intuity Audix , Intuity AudixLX, and Intuity Audix770 using Avaya ProVision or 2nd Nature from Unimax
- Modular Messaging using Avaya ProVision or 2nd Nature from Unimax
- CallPilot® releases 4.0, 5. 0, and 5.1
- Octel Aria using Avaya Professional Services
  - 250 and 350 systems
  - Octel Aria releases 3.10 and 3.11
  - Type “0” mailboxes only

    The first character of the mailbox must be alphabetic.
- A Messaging system that runs on physical servers to a Messaging system that runs on VMware® in a virtualized environment. Your Messaging system must be at release R6.2 or later.

Security considerations

Avaya is responsible for designing and testing its products for security. The customer is responsible for the appropriate security configurations on their data network. Customers have ultimate control over the configuration and use of the product. They are solely responsible for ensuring the security of their systems is adequate for their intended use.

Customers administer their system configuration and can tailor that system to meet their unique needs, but must also ensure to their own satisfaction that the security configuration is aligned with appropriate risk management best practices. Customers are responsible for keeping

themselves informed of the latest information for configuring their systems to prevent unauthorized use.

System managers and administrators are responsible for obtaining and acting on all recommendations, installation instructions, and system administration documents provided with the product. This information can help them understand the features that might introduce risk of toll fraud and the steps they must take to reduce that risk. Responsibilities owned by system managers include (but are not limited to):

- Integration of Messaging servers into existing TCP/IP network(s) according to the corporate networking policies. In most cases, existing firewalls, and corporate security policies and practices can be implemented or adapted for the Messaging system.
- Careful consideration for the security implications when the client access to the Messaging system are enabled.
- Protection of server against unauthorized use with appropriate administrator and user passwords. Use longer and more random passwords to minimize the possibility of compromise. Ensure that you secure the passwords properly.
- Protection of the surrounding network to minimize the threat of denial of service attacks.
- Review of server logs to detect actual and attempted unauthorized use and to identify its source.

System managers are also responsible for: Physical security, password protection, password control, backups, environmental controls.

Neither Avaya nor its suppliers or business partners can guarantee that any product is immune from risk of unauthorized use of IP or telecommunications services or facilities accessed through or connected to this product. Avaya is not responsible for any damages or charges that result either from unauthorized usage or from incorrect installation of the security patches that are made available periodically. See the End-User License Agreement(s) associated with your Messaging product(s) for additional details.

The customer is responsible for using and configuring the following security features available on Messaging software, on firmware, on the Avaya media gateways, and firmware on IP telephones:

Security policy configuration

Security policy is configured for the following:

- Administrator accounts
- Login account
- Change password
- Server access
- Syslog server

- Authentication file
- Firewall

Role-based user access control

Role based access control (RBAC) allows businesses to assign server, gateway, and application access permissions based on job function or role of a user. Avaya implements RBAC on the Messaging server through the use of profiles for the server webpage.

Authentication and encryption

Avaya uses standard X.509 PKI to manage certificates in the enterprise in which the hierarchy of certificates is always a top-down tree, with a root certificate at the top, representing the central Certificate Authority (CA) that is integral to the trusted-party scheme and does not need third-party authentication.

Messaging conforms to the TLS standard to establish a TLS session. Digital certificates authenticate stages of the TLS session establishment to:

- Establish SIP/TLS connections between IP phones and Messaging through the customer installed, trusted third-party certificate.
- Authenticate access to the Messaging web interface.
- Manage SIP/TLS connections
    - Management
    - Signaling

Audit trail logging

Security information is logged in or notified through:

- SNMP trap receiver
- Syslog security log
- Miscellaneous logs that track security-related information

Secure backups

The Messaging server backs up Messaging data over the customer LAN to an external ftp server. The Messaging data can be backed up at the same time as the server data, or independently. In the event of a system failure, the system uses the information stored on the external server to restore the system to an operational state. Messaging supports up to 20,000 mailboxes. Messaging data backup might easily reach 50 Gigabytes or more. Customers might be unable to support transfers of single files of this size. Hence, in Messaging, the system automatically divides large data backups into 500 MB files before transfer. Each file transfer might complete in about 5 minutes. Consequently, the network must support a minimum average transfer rate of 1.6 MBps.

Remote monitoring and maintenance

Messaging uses Secure Access Link (SAL) gateway to manage alarming and remote access. Secure Access Link (SAL) is an Avaya serviceability solution for support and remote management of a variety of devices and products. SAL provides remote access, alarm reception, and inventory capabilities. SAL uses the existing Internet connectivity of the customer to facilitate remote support from Avaya. All communication is outbound from the

customer environment over port 443 using encapsulated Hypertext Transfer Protocol Secure (HTTPS).

For more information about Messaging security features, see *Avaya Aura® Messaging Security Design*.

Additional security information

For security information and documentation about all Avaya products, see the Avaya Security Advisories website at http://support.avaya.com/security. The website includes information about the following topics:

- Avaya Product Security Vulnerability Response Policy
- Avaya Security Vulnerability Classification
- Security advisories for Avaya products
- Software patches for security issues
- Reporting a security vulnerability
- Automatic email notifications of security advisories

For information about Messaging security, see *Avaya Aura® Messaging Security Design*.

For additional information about security practices, see the National Security Agency Security Configuration Guides at http://www.nsa.gov/.

Chapter 4: Configuration details

Customer-provided equipment

The customer must provide the following equipment:

- Standard 19-inch four-post equipment rack that is properly installed and solidly secured. The rack must meet the following standards:
  - American National Standards Institute and Electronic Industries Association standard ANSI/EIA-310–D-92.
  - International Electrotechnical Commission standard IEC 297
  - Deutsche Industrie Norm standard DIN 41494
- Screws that come with the racks for installing the rails
- #2 cross-point (Phillips) screwdriver or 3/8 inch flathead screwdriver
- USB keyboard, USB mouse, and monitor must be available on the site for advanced installation or troubleshooting.
- Power from a nonswitched electrical outlet
- Access to the network

Port utilization

Your IT infrastructure needs to allow network traffic to move freely to and from the Messaging system.

Note:

You must disable multicast while configuring data switch ports.

For System Platform ports, see *Administering Avaya Aura® System Platform* on the Avaya Support website at http://support.avaya.com.

Messaging in a VMware virtualized environment does not require a dedicated VM ethernet port. See your Services representative for information about how to grant Avaya access to virtual machines for implementation and maintenance support.

For complete port matrix information, see Avaya Aura® Messaging Port Matrix available on the Avaya Support website at http://support.avaya.com.

Traffic specification

Messaging generates two types of network traffic:

- Voice traffic between Messaging and your telephony server
- Data traffic between the Messaging servers

Important:

Do not use multicast or network port mirroring to Messaging servers. These network features can generate unnecessary load and, during periods of high-volume traffic, can disrupt the operation and performance of the Messaging system.

Variables for calculating bandwidth

- Include both voice and data traffic. The calculations do not include any other activity in your network.
- Use the G.711 coding rate. If you use G.729, your bandwidth requirements are lower.
- Include the maximum traffic load for a server during peak busy hours. The server has 100 active ports that are simultaneously recording or playing voice data.

The topology of a configuration that supports multiple sites influences how data flows over your network. The placement of the following hardware, relative to each other, can affect this traffic load:

- Messaging servers
- Third-party message stores
- Telephony servers, gateways, and endpoints

These topology variables are not part of the following bandwidth calculations.

Bandwidth recommendations

- Single server system = 25 Mbs
- Multi server system = 25 Mbs for each server

Sample calculation for a multi server system

The number of servers x 25 Mbs = Mbs needed for bandwidth

For example, a fully loaded, 300-port, four-server system requires 100 Mbs: 4 x 25 Mbs = 100 Mbs.

Redundancy and high-availability

Redundancy for application servers

When one application server is sufficient to handle all the voice traffic for a location, adding another application server into a cluster provides redundancy. While both servers are online, the servers share the traffic load. But if one server fails, the other server must handle all the traffic. As long as voice traffic is within the capacity of one server, you have full redundancy without the interruption of service and loss of data.

If the traffic requirements require a cluster of two application servers running at or near capacity and you add a third server, the traffic is spread equally among the three servers. If one of the servers fails, the traffic load is divided between the two remaining servers. As long as the traffic is within the carrying capacity of the remaining two servers, messaging service is not interrupted and data is not lost. The behavior is the same in a cluster of four servers.

Local survivability

Local survivability refers to the continuation of Messaging service if an application server cannot reach the storage server. Therefore, local survivability only applies to locations in which an application server is physically present. Local survivability does not apply to single server configurations.

Local survivability is possible because each application server has a built-in Avaya Distributed Cache Server (ADCS). This rolling cache holds messages for 3 days, that is, 72 hours. You can change this retention period to fewer than 72 hours. Do not increase the retention period.

The AxC/Directory server provides connectivity between the application server and a third-party message store. In these configurations, local survivability applies if any combination of the following connections fail:

- The connection between the application server and the AxC/Directory server
- The connection between the AxC/Directory server and the third-party message store

When an application server cannot reach the storage server, the application server operates in the offline mode. The offline handling of messages and user directory transactions is the mechanism that Messaging uses to achieve local survivability. Offline handling is session based, and an application server only uses offline handling when the application server cannot reach the storage server.

In a distributed topology, all locations have a local application server and therefore, local survivability applies. All application servers use a WAN to connect to the storage server or to the third-party message store through the AxC/Directory server, regardless of their location. If an application server loses this connection, the application server operates in the offline mode and Messaging continues to function.

In a centralized topology with multiple locations, users at locations that do not have an application server do not have local survivability. The network connection between two telephony servers connects users to Messaging. If an outage in this network connection occurs, users at the location that has no application server lose Messaging service. However, if the outage is in the connection between an application server and the storage server, the affected application server operates in the offline mode and service continues for all users.

When an application server operates in the offline mode, Messaging operates as the application server similar to the way the application server interacts with the storage server.

Cache for messages

The system caches messages on the application server and then immediately attempts to deliver the message to the storage destination of the recipient when:

- A caller leaves a message (Call Answer)
- A user plays a message (Message review using a TUI)
- A user sends a message (Voice messaging)

After 72 hours, the system deletes the message from the cache on the application server. If the user plays a message that is older than 72 hours, the system retrieves the message from the message store. Then the system caches the message again on the application server as if the message was a new message.

If your system is a single-server configurations with more than 2500 IMAP4 clients, change the message retention period from 72 hours to 24 hours.

Messaging uses the cache mechanism to avoid delays in message retrieval. Sometimes, Messaging takes longer than 3 seconds to retrieve a message. This time interval depends on the available network bandwidth, the length of the message, and the storage server. To avoid an extended period of silence, Messaging plays a tone after 3 seconds to indicate that the message retrieval is in progress and the call is alive.

Users can use the TUI to address a message to multiple recipients by:

- Creating a Personal Distribution List
- Selecting a predefined personal or system distribution list from the address directory

When the caller sends a message to a distribution list, the application server caches the message in the mailbox of the first person on the list. But after the message reaches the storage server, the system delivers the message to all recipients. After a recipient who is not first on

the list plays the message, the system caches the message on the application server for that user.

When a recipient retrieves a message, the application server goes to the storage destination for the recipient to get a list of the recipient messages and the state of the message (unread, read, or saved.) For the content of the message, the application server first looks locally in its own cache. If the message is not present in the local cache, the application server looks in the other application servers in the cluster. If the message is not on any of the application servers, the application server retrieves the message from the storage destination of the recipient and puts the message into the local cache of the application servers.

Redundancy for Avaya storage servers

Messaging administrators can set up a backup Avaya message store that provides business continuity if the primary storage server fails. Message Mirror software synchronizes the data between these storage servers. For more information about Message Mirror, see http://www.mutare.com.

Message Mirror:

- Monitors the primary storage server and copies messages, names, greetings, passwords, and mailbox and Class of Service changes to the backup server.
- Uses IMAP4 and LDAP ports to connect to the Avaya storage server. You can also use Secure IMAP4 and LDAP ports.

Failover to the backup server is a manual process.

Message Mirror Caveats

You must use a Network Time Protocol (NTP) server within your network to synchronize the time of the System Platform server. The Avaya message store server and the Message Mirror server must synchronize with the NTP server.

While copying Class of Service information, Message Mirror also increases the maximum mailbox and message size on the backup server by 5%. With increase, Message Mirror can copy voice messages of the maximum length on the primary sever to the backup server.

Message Mirror does not replicate the following:

- Broadcast messages at the system level and the site level
- User-entered descriptions for optional greetings
- System lists such as ELAs and PDLs
- Messages stored in a folder other than the Inbox folder
- Future delivery messages stored in a queue
- Sites and topology data

- Telephony domain settings
- Administrative logins
- Nightly backup schedule
- Certificates

Messaging does not support Message Mirror when the:

- Application server and the storage server are active on the same server. For example, a single-server configuration.
- Microsoft Exchange server is the message store.

Glossary

Active Directory	The directory service for a Microsoft Windows 2000, Windows 2003 Server, or Windows 2008 Server. The Active Directory stores information about objects on the network and makes this information available for authorized administrators and users. It provides administrators with an intuitive hierarchical view of the network and a single point of administration for all network objects.
AudioCodes Gateway	A gateway that integrates the Messaging system with customer-provided telephony servers.
Caller	Any person who calls into the Messaging system.
Caller Applications	Extensions to the Messaging telephone user interface (TUI) used to customize how Messaging interacts with callers.
Caller Applications Editor	A tool that customizes the Microsoft Management Console (MMC) user interface to permit the creation, editing, and deployment of Caller Applications.
Cluster	A Messaging topology in which up to three application servers are combined to increase the capacity of the Messaging system.
Codec	A device that encodes or decodes a signal.
Configuration	A way in which application servers, storage servers, and AxC/Directory servers are connected to each other considering single server, multi-server, single site, and multiple site needs.
Console Domain	A virtual machine that is a part of System Platform and has many platform elements, including common logging and alarming, licensing, and remote access.
CoS	Class of Service. A category that determines user access to system options and features.
Dial plan	A set of site-specific properties that are stored on the storage server, and are automatically applied to each application server associated with any given site. Dial plans define the storage server and application servers properties to make the Messaging system.
Dial rule	Rules applied to local and remote users to determine how users can respond to messages from callers. Dial-out rules define the dial strings that are sent to the telephony server for making calls.

DTMF	Dual-Tone Multifrequency. A combination of two tones that uniquely identify each button on a telephone keypad.
EAG	Extended Absence Greeting. A user-recorded greeting that Messaging plays when the user is away from the office.
ELA	Enhanced List Application. A feature that associates one mailbox to a list of members. Instead of sending the same message to individual lists members, you can send the message to the list mailbox.
Enterprise List	Message Networking Enterprise Lists are enterprise-wide mailing lists for users that reside on a Message Networking system. Each Enterprise List represents a specific group of potential recipients for enterprise distribution messages.
ESXi	A virtualization layer that runs directly on the server hardware. Also known as a *bare-metal hypervisor.* Provides processor, memory, storage, and networking resources on multiple virtual machines.
G.711	An audio-encoding format with a coding rate of approximately 64 kilobits per second (kbps) or 8 Kilobytes per second (KBps).
GSM 6.10	An audio-encoding format with a coding rate of approximately 13 kilobits per second (kbps) or 1.6 Kilobytes per second (KBps).
IMAP4	Internet Messaging Access Protocol 4. A method of accessing electronic mail or bulletin board messages that are kept on an email server. Client email applications can use IMAP4 to access remote message stores as if the messages were local.
Info Mailbox	A mailbox that plays greetings and provides information to a caller. A typical informational message includes details about directions, business hours, or weather. Callers cannot leave a message in this mailbox.
LDAP	Lightweight Directory Access Protocol. An Internet Protocol used to retrieve and manage directory information.
Location	Location refers to the physical placement of the server, that is location in building, city, or country. While location refers to the physical destination of the server, site refers to a set of properties that are defined using SMI. See Site on page 38.
Message Mirror	A product of Mutare, Inc. that provides redundancy for the Avaya message store.
MMC	Microsoft Management Console. A presentation service for management applications.
MWI	Message Waiting Indicator. A method of alerting users when messages that meet specified criteria arrive in a mailbox. The indicator is either a

	lamp on the telephone or an audible tone that you hear when you pick up the receiver.
PDL	Personal Distribution List. A labeled collection of addresses that users create and save for later use. Messages that users address to the list are sent to all the list members. Users can only manage and address messages to those PDLs that they create and own.
Personal greeting	A personalized prompt that greets callers when they are transferred to a user mailbox when the extension is busy or not answered.
Personal Operator	A designated extension or mailbox to which the system can transfer callers for assistance when the original call was not answered. Other terms have been used including “personal assistant”, “covering extension”, “operator”, “zero-out destination”, and so on.
PEL	Privacy Enforcement Level. A systemwide privacy parameter that determines the level of privacy the system enforces. The PEL setting determines which clients or interfaces have access to Messaging mailboxes, and the level of restriction imposed on recipients of private messages.
Pilot number	A single number that presents a call to one of the available ports within a hunt group.
PLDS	Product Licensing and Delivery System. A tool for managing asset entitlements and electronic delivery of software and related licenses. You can perform activities such as license activation and deactivation, license re-host, and software downloads.
Rapid prompts	A shortened variation of the standard set of prompts for the experienced Aria TUI user. The optional language pack for rapid prompts is available only in U.S. English.
RBAC	Role-Based Access Control. A tool that defines the administrative roles for your business. You control the administrative privileges on the application and storage servers by assigning a role to a user.
SAL	Secure Access Link. An Avaya serviceability solution for support and remote management of a variety of devices and products. SAL provides remote access and alarm reception capabilities. SAL uses the existing Internet connectivity of a customer to facilitate remote support from Avaya.
SAL Gateway	A customer-installable system that provides remote access, and alarming capabilities for remotely managed devices.
SAN	Storage Area Network. A SAN is a dedicated network that provides access to consolidated data storage. SANs are primarily used to make

	storage devices, such as disk arrays, accessible to servers so that the devices appear as locally attached devices to the operating system.
Site	A set of properties that administrators define in the System Management Interface. Some of the properties are access number, extension length, mailbox length, language choice, and Auto Attendant features.
SMI	System Management Interface. The single point of access to the Messaging system and the license server. You can open the SMI from any standard web browser from anywhere within the firewall of the organization.
SMTP	Simple Mail Transfer Protocol. A TCP/IP protocol that sends and receives email. Most email systems that send mail over the Internet use SMTP to send messages from one server to another and to send messages from an email client to an email server.
Snapshot	Capture a virtual appliance configuration in time. Creating a snapshot can affect service. Some Avaya virtual appliances have limitations and others have specific instructions for creating snapshots.
SNMP	Simple Network Management Protocol. A protocol for managing and monitoring networks.
T.38 codec	A protocol that describes how to send a fax over a computer data network. T.38 is needed because fax data can not be sent over a computer data network in the same way as voice messages.
Template	Avaya offers product-specific templates to install different products on System Platform. A template is a definition of a set of one or more applications to be installed on System Platform.
Topology	The relationship between the Messaging application servers and the sites that the servers support. You define topology properties on the storage server which then applies the properties to the associated application servers.
TTS	Text-to-Speech. Speech synthesis that converts text into speech. TTS converts message envelope information, text names, and email messages and Messaging plays the converted text over the telephone.
TTY (teletypewriter)	A typewriter-style device for communicating alphanumeric information over telephony networks. Typically used by the hearing impaired and sometimes called a telecommunication device for the deaf (TDD).
udom	User applications domain. A virtual machine that runs with a specific type or mode of High Availability protection, according to Avaya Aura® solution template requirements.

User	A person who has an account on the Messaging system.
VM	Virtual Machine. Replica of a physical server from an operational perspective. A VM is a software implementation of a machine (for example, a computer) that executes programs similar to a physical machine.
vMotion	A VMware feature that migrates a running virtual machine from one physical server to another with minimal downtime or impact to end users. vMotion cannot be used to move virtual machines from one data center to another.
VMware HA	VMware High Availability. A VMware feature for supporting virtual application failover by migrating the application from one ESXi host to another. Since the entire host fails over, several applications or virtual machines can be involved. The failover is a reboot recovery level which can take several minutes.
WebLM	Web-based license manager. A licensing solution that facilitates license management of one or more Avaya software products. WebLM also facilitates easy tracking of licenses. WebLM requires a license file. This file contains information about the products that your organization bought, including the major release, the licensed features, and the licensed capacities of each feature.

Index

T

U

V