Administering Avaya Multimedia Messaging

Release 3.2
Issue 2
August 2017

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 as set forth below in the Designated System(s) License (DS) section as applicable. 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 set of Designated Processors that hosts (physically or virtually) 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: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. 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.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on

Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use 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.

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

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software 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, unless otherwise stated, 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

Contents

Chapter 1: Introduction

Purpose

This document describes ongoing administration, management, and maintenance tasks for Avaya Multimedia Messaging. Use this document after deploying Avaya Multimedia Messaging. For more information about deployment, see *Deploying Avaya Multimedia Messaging*.

Change history

The following table summarizes major changes in this document.

Issue	Release date	Summary of changes
Release 3.2, Issue 1	June 2017	This is a new document. Administration information from *Deploying Avaya Multimedia Messaging* has been moved into this document and reorganized. The following key changes have been made to the existing administration information: • Added a brief summary of key administrator responsibilities. • Updated the list of management tools and added information about system layer commands. • Added Managing application sessions on page 28. • Moved client device certificate information into a new section called Managing client device certificates on page 30and added a note about the client certificate policy. • Updated Avaya Multimedia Messaging multisite adapter administration and management on page 43 to indicate that allowable media sizes on each site must be the same. • Updated Making a backup for an Avaya Multimedia Messaging node on page 65. • Updated the restore steps for a cluster and a single node. • Added new Gluster restoration information. • Indicated that you need to migrate to Release 3.0 and then upgrade to Release 3.2. Information about migrating to Release 3.0 has been removed from this document.

Issue	Release date	Summary of changes
		• Updated the steps in Upgrading the Avaya Multimedia Messaging server on page 75. • Added information about system layer updates. • Reorganized and edited troubleshooting information. • Updated Managing logs on page 36. • Removed “CollectNodes” references from the document.
Release 3.2, Issue 2	August 2017	• Updated the virtual machine requirements in Virtual machine and physical server deployment specifications on page 14. • Updated the **`collectlogs`** command syntax information in the chapter Management tools and commands on page 15. • Updated the information about disk volumes in Increasing the size of a disk volume on a virtual machine on page 48. • Minor rephrasing and terminology changes throughout the document.

Chapter 2: Avaya Multimedia Messaging overview

Avaya Multimedia Messaging provides advanced multiparty instant messaging (IM) and rich media exchange capabilities to Avaya Unified Communications (UC) applications. Avaya Multimedia Messaging functionality is available on Avaya Equinox™ for Mac, Windows, Android, and iOS.

When Avaya Multimedia Messaging is enabled on a supported application, you can

- Exchange text-based instant messages with users of Avaya Multimedia Messaging, Avaya Aura® Presence Services, Microsoft Lync, and Skype for Business.
- Receive photo, audio, video, and generic file attachments.
- With Avaya Equinox™ for Windows, all users can send generic file attachments, but only users with enhanced privileges can capture photo, audio, and video files on Avaya Multimedia Messaging. With mobile clients, only users with enhanced privileges can send attachments in an IM conversation.
- View and participate in active conversations from multiple devices.

  You can view an active conversation from applications that use Avaya Aura® Presence Services, even if the application does not have Avaya Multimedia Messaging enabled. When viewing a conversation in an application without Avaya Multimedia Messaging, you can use the provided message playback URL to view attachments.
- Search for archived or inactive conversations in the application History fan.

Avaya Multimedia Messaging has its own server that must reside on a Linux based server. A VMware deployment option is also available for the Avaya Multimedia Messaging server. You can deploy Avaya Multimedia Messaging as a single server or within a cluster of servers.

New in this release

The following is a summary of new functionality that has been added to Avaya Multimedia Messaging in Release 3.2:

Presence Server 7.1 federation relay

Microsoft Lync and Skype for Business federation now requires Presence Services Release 7.1. The Avaya Multimedia Messaging relay entity will no longer be used for IM and Presence message signaling.

Read receipt

Support for Read Message and Read Attachment notifications on Avaya Multimedia Messaging clients.

Note:

Read receipts are not supported for federated users outside of Avaya Multimedia Messaging.

System layer commands

The **sys** command line alias has been introduced to facilitate the discovery and use of system layer commands.

New partitioning version 2.0

A new file system structure or partitioning scheme, called partitioning version 2.0, has been introduced to the OVAs for this release. The partitioning scheme created by OVAs from previous releases is called partitioning version 1.0. Both partitioning version 1.0 and 2.0 are supported in this release.

Topology

The following image provides an overview of the architecture and connectivity of Avaya Multimedia Messaging components.

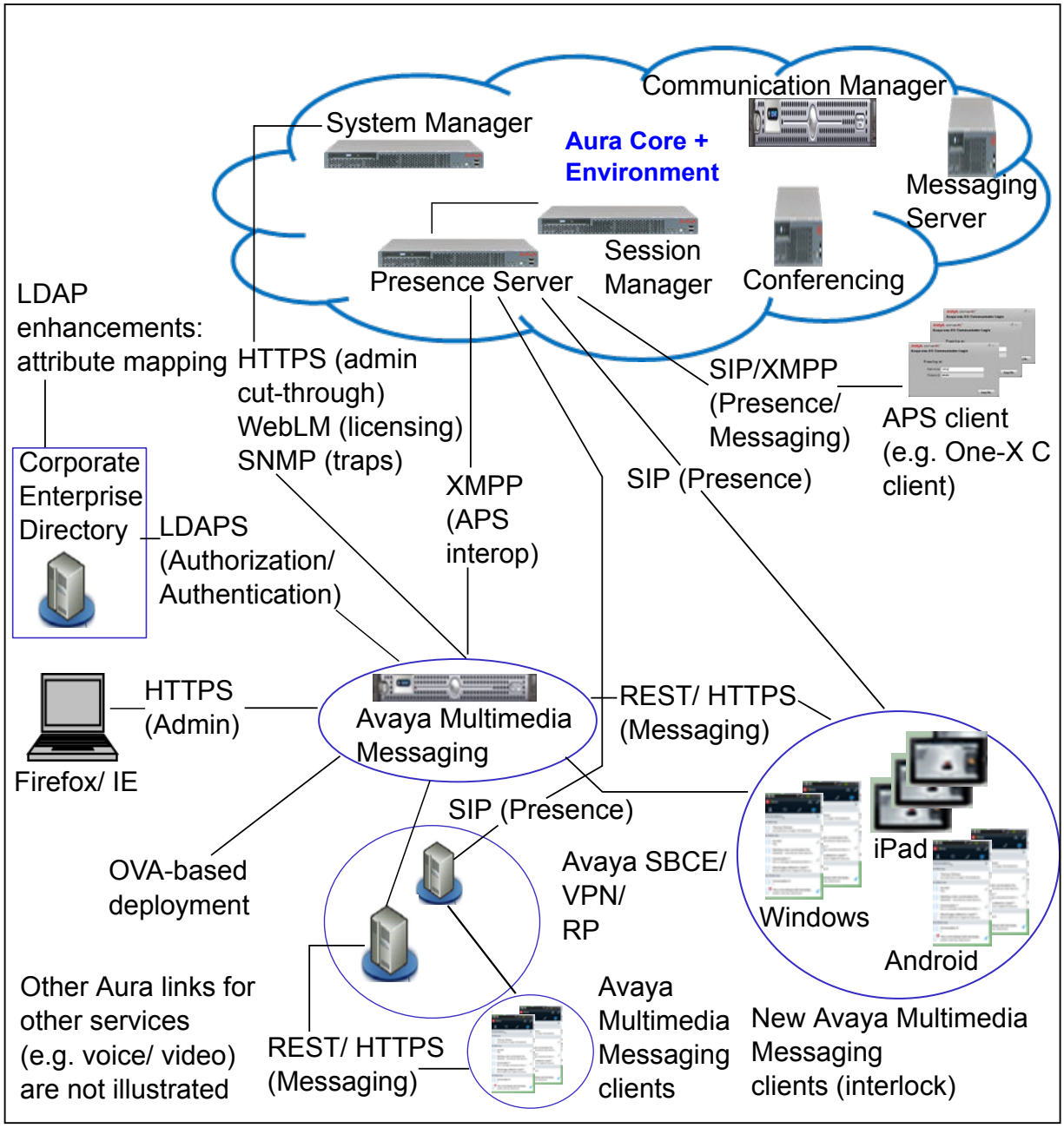


Figure 1: Avaya Multimedia Messaging deployment architecture

Components

Table 1: Avaya Multimedia Messaging Components

The following table describes the main Avaya Multimedia Messaging components. For more information on interoperability and product versions, see https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml?name=Multimedia+Messaging.

Component	Description
Avaya Aura® Core	The Avaya Aura® network, that encompasses the Avaya products needed by Avaya Multimedia Messaging: • Avaya Aura® Presence Services: For Presence and IM federation with other applications. • Avaya Aura® System Manager: For centralized Avaya Aura® management. Avaya Aura® System Manager enables: - Licensing with Avaya WebLM - Viewing capabilities for logs and alarms - Certificate management For applications to perform registration and telephony functions such as call escalation, Avaya Aura® Session Manager can also be present in the system configuration. Avaya Aura® Session Manager is an optional component. • Avaya Aura® Communication Manager: For organizing and routing voice, data, image, and video transmissions. • Avaya Session Border Controller for Enterprise (Avaya SBCE): For Microsoft federation with external domains.
Enterprise Directory	The Corporate LDAP server, Microsoft Active Directory.
Avaya Multimedia Messaging server	A Red Hat Enterprise Linux server that contains the Avaya Multimedia Messaging application.
Endpoints	Applications that support Avaya Multimedia Messaging: • Avaya Equinox™ for iOS • Avaya Equinox™ for Android • Avaya Equinox™ for Mac • Avaya Equinox™ for Windows The following are examples of Avaya Aura® Presence Services applications that support integration with Avaya Multimedia Messaging through the Message Playback functionality: • Avaya one-X® Communicator for Windows

Virtual machine and physical server deployment specifications

The following tables describe VMWare and physical server deployment specifications.

VMWare deployments

Specification	500 users	1000 users	10000 users
vCPUs (at 2.9GHz)	8	8	24
Memory	8 GB	8 GB	32 GB
Storage reservation	0.5 TB	1 TB	5 TB

Physical server deployments

Specification	Deployment on physical server
CPU resources	Each node: Two 2.9 GHz CPUs, 6 core per CPU with hyper-threading
Memory	Each node: 32 GB
Storage reservation	N/A
Hard drive	Each node: 5 TB data as required per RAID configuration

Administrator responsibilities

After the Avaya Multimedia Messaging deployment is completed, an administrator can perform the following key management tasks:

- Manage Avaya Multimedia Messaging services using the web administration portal.
- Set up and customize optional functionality, such as Integration Windows Authentication and multisite support.
- Adjust virtual hardware resources and disk sizes.
- Schedule repairs.
- Check logs and alarms.
- Perform backup and restore operations.
- Upgrade within an Avaya Multimedia Messaging release or migrate to a new Avaya Multimedia Messaging release.
- Manage system layer updates.

Chapter 3: Management tools and commands

Category	Name	Description
Web administration portal		Enables you to start and stop Avaya Multimedia Messaging services, and to manage settings and functionality. For more information about using the administration portal, see the chapter Management of Avaya Multimedia Messaging with the administration portal on page 27.
GlusterFS tools	gluster	The Command Line utility of the Gluster File System, Gluster Console Manager. You can use this utility to check the distributed file system status for remote nodes. For usage instructions, see the Gluster manual.
Java tools	jconsole	JConsole uses the extensive instrumentation of the Java Virtual Machine (Java VM) to provide information about the performance and resource consumption of applications running on the Java platform. You can use jconsole to monitor the following components: • Tomcat • Mobicents • Cassandra • Serviceability Agent (aka spiritAgent) For more information about using the jconsole utility, see the Oracle documentation. **Important:** JConsole is a graphical tool and can be run locally from an Avaya Multimedia Messaging node that has a graphical desktop environment installed.
Cassandra database tools	nodetool	The nodetool utility provides usage information about the Cassandra database nodes. For usage instructions, see the Cassandra database documentation.

Category	Name	Description
Avaya Multimedia Messaging tools	clitool.sh	A tool that has multiple usage possibilities. The parameters specified in the command determine the usage of the clitool utility. Run the clitool utility with the dailyReport as a parameter to generate reports for the current day.
	cleanAMM.sh	The CleanAMM utility must be run on a regular basis, immediately after performing a backup, to remove closed conversations. The cleaner tool creates additional disk space by deleting the oldest closed conversations until the amount of free disk space is less than 75% of the hard disk capacity. The results of the cleaning operation are stored in the `logs/cleaner_CLF.log` file. If the cleaner tool cannot free enough disk space, you can use the web-based administration portal to change the number of days that idle conversations remain open.
	`app collectlogs` command	Enables you to collect and download the logs from an Avaya Multimedia Messaging node.
	perfLogViewer.sh	A tool for reading performance logs. The perfLogViewer tool must be used only for first-level support. **Important:** perfLogViewer is a graphical tool and can be run locally from an Avaya Multimedia Messaging node that has a graphical desktop environment installed.
	statusAEM.sh	A tool that displays the status of the Avaya Multimedia Messaging server and of the related services. Use the statusAEM tool to verify that the Avaya Multimedia Messaging is installed properly and that the services are running. The statusAEM.sh script is located in the `/opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/bin/` directory.
Linux tools	ping	Sends an ICMP ECHO_REQUEST to network hosts.
	nslookup	Queries the internet servers interactively.
	ip	Displays and manages routing devices, policy routing and tunnels. You can use this command to identify nodes that have a virtual IP address.
	ethtool	Queries and manages network driver and hardware settings. You can use this command to confirm that the physical network adapter is enabled and available.
	wget	Downloads files from the Web. You can use this tool to perform resource discovery for a user.

Category	Name	Description
	curl	Transfers a URL.
System layer commands	**sys** command line alias	Enables you to run commands that operate on the system layer. The following commands are currently supported: • **sys secconfig** • **sys versions** • **sys volmgt**

gluster volume status

The **gluster** utility is for managing the Gluster File System.

You can run the **gluster** command with multiple parameters, such as **gluster volume status**, which displays volume information for the Gluster bricks.

For more information about using the **gluster** command, see the Gluster manual.

Usage example

```
[root@pvt5sv213 ~]$ sudo gluster volume status
Status of volume: cs_volume
Gluster process                                 Port  Online      Pid
------------------------------------------------------------------------------
Brick 1.2.3.10:/media/data/content_store/brick0  24009 Y     19129
Brick 1.2.3.20:/media/data/content_store/brick0  24009 Y     43398
Brick 1.2.3.10:/media/data/content_store/brick1  24010 Y     29252
Brick 1.2.3.30:/media/data/content_store/brick0  24009 Y     46907
Brick 1.2.3.20:/media/data/content_store/brick1  24010 Y     43584
Brick 1.2.3.30:/media/data/content_store/brick1  24010 Y     46912
NFS Server on localhost                         38467 Y     29293
Self-heal Daemon on localhost                   N/A   Y     29299
NFS Server on 1.2.3.30                          38467 Y     46920
Self-heal Daemon on 1.2.3.30                    N/A   Y     46926
NFS Server on 1.2.3.20                          38467 Y     43590
Self-heal Daemon on 1.2.3.20                    N/A   Y     43596
```

nodetool

The **nodetool** utility provides usage information about the Cassandra database nodes.

For more information about using the **nodetool** utility, see the Cassandra database documentation.

Usage example

To view the status of the database, run the **nodetool -u cassandra_username -pw Cassandra_password status** command.

For example:

```
[root@amm-1 logs]# /opt/Avaya/MultimediaMessaging/<version>/cassandra/1.2.7/bin/nodetool -
u cassandra_username -pw Cassandra_password status
Datacenter: datacenter1
=======================
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
--  Address        Load       Tokens  Owns   Host ID                               Rack
UN  1.2.3.4  10.99 MB   256     100.0%  a436fb45-226b-4a73-a251-05c05c383794  rack1
```

To repair the Cassandra database either periodically, or after one of the cluster nodes malfunctions, use the **nodetool -u cassandra_username -pw Cassandra_password repair** command.

Important:

To protect data integrity, you must run the nodetool command for repairing the database at least once a week.

If the databases are large, the repair process may need several hours to complete.

```
[root@amm-1 logs]# /opt/Avaya/MultimediaMessaging/<version>/cassandra/1.2.7/bin/nodetool -
u cassandra_username -pw Cassandra_password repair
[2014-07-04 08:49:01,128] Starting repair command #1, repairing 256 ranges for keyspace
cas_common_data
[2014-07-04 08:49:04,465] Repair command #1 finished
[2014-07-04 08:49:04,492] Starting repair command #2, repairing 256 ranges for keyspace
amm_data
[2014-07-04 08:49:07,756] Repair command #2 finished
[2014-07-04 08:49:07,781] Starting repair command #3, repairing 256 ranges for keyspace
acs
[2014-07-04 08:49:11,015] Repair command #3 finished
[2014-07-04 08:49:11,024] Nothing to repair for keyspace 'system'
[2014-07-04 08:49:11,030] Starting repair command #4, repairing 256 ranges for keyspace
openfire
[2014-07-04 08:49:11,205] Repair command #4 finished
[2014-07-04 08:49:11,229] Starting repair command #5, repairing 256 ranges for keyspace
sip_notification_cql
[2014-07-04 08:49:14,468] Repair command #5 finished
[2014-07-04 08:49:14,492] Starting repair command #6, repairing 256 ranges for keyspace
amm_notification
[2014-07-04 08:49:17,727] Repair command #6 finished
[2014-07-04 08:49:17,751] Starting repair command #7, repairing 256 ranges for keyspace
amm_system
[2014-07-04 08:49:21,005] Repair command #7 finished
[2014-07-04 08:49:21,029] Starting repair command #8, repairing 256 ranges for keyspace
amm_federation
[2014-07-04 08:49:24,507] Repair command #8 finished
[2014-07-04 08:49:24,535] Starting repair command #9, repairing 256 ranges for keyspace
clusteradmin
[2014-07-04 08:49:27,776] Repair command #9 finished
[2014-07-04 08:49:27,785] Starting repair command #10, repairing 256 ranges for keyspace
system_auth
[2014-07-04 08:49:27,966] Repair command #10 finished
```

```
[2014-07-04 08:49:27,990] Starting repair command #11, repairing 256 ranges for keyspace
SIP_Notification
[2014-07-04 08:49:31,249] Repair command #11 finished
[2014-07-04 08:49:31,258] Nothing to repair for keyspace 'system_traces'
[2014-07-04 08:49:31,300] Starting repair command #12, repairing 256 ranges for keyspace
amm_schema_version
[2014-07-04 08:49:34,182] Repair command #12 finished
[2014-07-04 08:49:34,190] Starting repair command #13, repairing 256 ranges for keyspace
OpsCenter
[2014-07-04 08:49:34,352] Repair command #13 finished
```

If you use the **nodetool** command without specifying any parameters, the system displays the list of available parameters.

cleanAMM

The CleanAMM utility must be run on a regular basis, immediately after performing a backup, to remove closed conversations. The cleaner tool creates additional disk space by deleting the oldest closed conversations until the amount of free disk space is less than 75% of the hard disk capacity.

The results of the cleaning operation are stored in the `logs/cleaner_CLF.log` file.

If the cleaner tool cannot free enough disk space, you can use the web-based administration portal to change the number of days that idle conversations remain open.

Usage example

```
/opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/bin/cleanAMM.sh
Conversation clean-up will begin within one minute.  Monitor logs at /opt/Avaya/
MultimediaMessaging/<version>//logs/cleaner_CLF.log for progress
```

clitool

The clitool utility provides multiple usage possibilities, depending on which parameters the utility receives in the command line.

You can use the clitool utility with the **dailyReport** option to generate daily reports about the Avaya Multimedia Messaging activity.

Usage example

To generate the reports, run the clitool.sh utility with the **dailyReport <report_directory>** parameters.

For example:

```
[jdoe@pvt5sv213 jdoe]$ /opt/Avaya/MultimediaMessaging/2.1.0.0.833/CAS/2.1.0.0.833/misc/
clitool.sh dailyReport /home/jdoe/reportDirectory
Retrieving user data: 2014-07-04T13:01:14.229Z
Retrieving conversation data: 2014-07-04T13:01:15.502Z
Retrieving attachment data: 2014-07-04T13:01:15.680Z
Retrieving feature data: 2014-07-04T13:01:15.843Z
Retrieving message data.  This may take several minutes: 2014-07-04T13:01:15.980Z
Analyzing data: 2014-07-04T13:01:16.485Z
Producing reports: 2014-07-04T13:01:16.515Z
Done: 2014-07-04T13:01:17.023Z
```

Note:

For Avaya Multimedia Messaging systems with large databases, the reports may take a few minutes to be generated.

If you list the content of the destination directory, the system displays the following report files:

```
$ ls /home/jdoe/dailyReport/
AttachmentBreakdown.txt  ConversationReport.txt  DailyBreakdown.txt  Licenses.txt
PerUserReport.txt  SizeBreakdown.txt
```

An excerpt from one of the report files could be the following:

```
User Name,    avg msg size (MB),       Total Messages,       text only
amm_user000001@avaya.com,                0.00,                  494,             494
amm_user000002@avaya.com,                0.00,                    0,               0
amm_user000003@avaya.com,                0.00,                    0,               0
amm_user000004@avaya.com,                0.00,                    0,               0
amm_user000005@avaya.com,                0.00,                    0,               0
amm_user000006@avaya.com,                0.00,                    0,               0
amm_user000007@avaya.com,                0.00,                    0,               0
amm_user000008@avaya.com,                0.00,                    0,               0
amm_user000009@avaya.com,                0.00,                    0,               0
amm_user000010@avaya.com,                0.00,                    0,               0
```

collectlogs

The **app collectlogs** command enables you to collect and download the logs from an Avaya Multimedia Messaging node. For example, if you run the following command, two logs will be downloaded from the 10.10.10.1 node:

```
$ app collectlogs collect -n 2 -ip 10.10.10.1
```

By default, if details are not specified, the system will download all 20 logs from the local node.

You can also use the web administration portal to collect and download logs.

Related links

Management tools and commands on page 15

System layer commands

The **sys** command line alias facilitates the use and discovery of system layer commands. Typing this command without arguments provides syntax help, and a list of supported system layer commands. The following is an example:

```
[admin@server4889amm ~]$ sys

Execute system layer commands.

    -h, --help
        Command syntax (this help)

    -hh, --hhelp
        Verbose help

Available commands:

    secconfig       [Manage security settings]
    versions        [Query version information]
    volmgt          [Manage disk volume sizes]

  Command invocation syntax:
     sys <command> <arguments>

  Command syntax
    sys <command> -h

[admin@server4889amm ~]$
```

Verbose help information

-hh is used for verbose help information, which provides a brief description of each available system layer command. The following is an example:

```
[admin@server4889amm ~]$ sys -hh

The "sys" command line alias facilitates access to the following commands
related to the system layer of UCApp appliances. To obtain help with
each of these commands, use the "-h" (or "--help") argument for help
with command line syntax, and "-hh" (or "--hhelp") for verbose help.

secconfig
    Manages security-related settings.

versions
    Queries the version information of various elements of the system
    layer.

volmgt
    Queries the sizes of existing disk volumes and extends their sizes.

[admin@server4889amm ~]$
```

Any arguments provided after the name of the system layer command are passed through to that command.

sys secconfig command

sys secconfig provides access to the **secconfig** command, which existed in previous releases. The following is an example of this command:

```
[admin@server4950amm ~]$ sys secconfig --hhelp

This script is used to manage run-time security settings on this appliance.
The following command-line arguments are available:

    --help, -h
        Prints terse help (command line syntax).

    --hhelp, -hh
        Prints verbose help (this help).

    --sshCBC < --enable | --disable | --query >
    -cbc     < -e       | -d        | -q >
        Enables, disables, and queries the current state of SSH daemon
        CBC-based ciphers.

[admin@server4950amm ~]$
```

sys versions command

The **sys versions** command provides a summary of key system layer information, including the type of appliance (OVA), the version number of the system layer, the version of the current partitioning, and the OVA that was originally deployed.

```
[admin@server4889amm ~]$ sys versions

    Appliance type       : AMM
    System layer version : 3.2.0.0.8
    Partitioning version : 1.0
    Original OVA deploy  : amm-3.2.0.0.329

[admin@server4889amm ~]$
```

sys volmgt command

Syntax help: sys volmgt --help

The **sys volmgt** command is used to query and extend disk volumes on the system. The following provides the command line syntax for this command:

```
[admin@server4889amm ~]$ sys volmgt --help

Syntax:
    --help,                 -h
    --hhelp,                -hh
    --version,              -v
    --status,               -st
    --summary,              -s
    --monitor  [tail|less], -m [tail|less]
    --logs,                 -l
```

```
    --scan
    --extend <volume> [ <n>m | <n>g | <n>t --remaining ]
  --extend --all
    --reset

[admin@server4889amm ~]$
```

Verbose help: sys volmgt --hhelp

The verbose help information for the scripts provides more information about what the tool is used for.

```
[admin@server4889amm ~]$ sys volmgt --hhelp

This script provides for the ability to extend the sizes of volumes on this
system. In order for a volume to be extended in size, the disk that hosts
the volume must first be increased in size using the tools that are used
to manage deployed virtual machines (VMware).

The following example illustrates how to add 20 GiB of storage to the
application log volume (/var/log/Avaya). This volume is located on the second
disk of the system and so this example assumes that disk 2 has been increased
in size by 20 GiB.

    sys volmgt --extend /var/log/Avaya 20g

The above example will do two things:

    1) It will extend the size of the LVM logical volume by 20 GiB.

    2) It will then extend the size of the Linux file system that is
       located inside that volume to the new size of the LVM logical
       volume.

Step (2) above may take several minutes to complete for larger volumes. If,
for some reason, this second operation is interrupted, it can be re-run
using the same command, but WITHOUT specifying the size argument. For example,
the following command is used to perform step (2) only for the application
log volume (/var/log/Avaya).

    sys volmgt --extend /var/log/Avaya

If in doubt as to whether or not all file systems have been fully extended in
their respective volumes, step (2) can be executed across all volumes using
a single command as follows:

    sys volmgt --extend --all

Performing step (2) on a file system that is already fully extended in its
LVM volume is a null operation (does no harm).

Note the following general points regarding this script:

- The extending of a volume cannot be undone. Make sure the correct volume
  is being extended, and by the correct size. To confirm any extend
  operation, the user is required to enter the response "confirm"
  (case insensitive).

- In order to avoid impacting system performance, avoid performing extend
  operations during periods of high traffic.

- Extend operations are performed by a background process, in order to
  avoid interference due to loss of an SSH connection. Avoid powering down
  or rebooting a server while there is a background operation in progress.
  The presence of a running background operation can be queried as follows:
```

```
    sys volmgt --status

- Logical volumes on the system are referenced using their Linux file system
  mount points, such as /var/log/Avaya and /media/data, with the exception
  of the volume containing Linux swap, which has no mount point. The Linux
  swap volume is referenced using "swap".

- Sizes are specified in base 2 units rather than base 10 (SI) units. For
  example, 1g = 1 GiB = 1024 x 1024 x 1024 bytes.

- Summary information is displayed in GiB, with a resolution of two decimal
  places. When extending the sizes of LVM volumes, units can be specified
  in mebibytes (m), gibibytes (g), or tebibytes (t).

- Due to file system overhead allocation by the Linux kernel, the size
  of a file system will never exactly match the size as reported by
  the LVM volume that contains that file system. To be certain that a file
  system is fully extended to the size of the volume that contains it,
  inspect the log file after issuing the extend operation as follows:

      sys volmgt --monitor less

  To perform such a check across all volumes:

      sys volmgt --extend --all
      sys volmgt --monitor less

The following arguments are supported by this script:

    --help, -h
        Terse help.

    --hhelp, -hh
        Verbose help (this help).

    --version, -v
        Prints the version of this script to stdout.

    --status, -st
        Prints the current status of this tool. Use this to determine
        if there is a background operation in progress, or the results
        of the last background operation.

    --summary, -s
        Prints a summary of disks, the LVM volumes contained on each disk,
        and the file system contained in each LVM volume. Disk information
        includes the size of the disk and the amount of free space
        available for allocation to volumes on the disk. LVM volume
        information includes the size of the LVM volume. File system
        information includes the size of the Linux file system and the
        current amount of space that is in use on that file system.

        Due to file system overhead allocation by the Linux kernel, the
        size of a file system will never exactly match the size as reported
        by the LVM volume that contains that file system. Refer to the top of
        this help information for more information.

    --monitor [tail|less]
    -m        [tail|less]
        Browse the log file for the latest extend operation. Specify "tail"
        to use the tail browser. Specify "less" to use the less
        browser, which allows scrolling and searching through the log file.
        If neither is specified, the browser defaults to the tail browser.
```

```
   --logs
       Generate a zip file in the current working directory that contains
       all logs generated to date by this script.

   --scan
       Scan disks for newly available storage. Do this after increasing
       the disk size of one of more disks. Once scanned, the newly
       available space appears in the "Free" column in the "--summary"
       output, and is now available for allocation to volumes on that disk.

       A summary is printed after the scan to show the updated volume
       information.

   --extend <volume> [ <n>m | <n>g | <n>t --remaining ]--extend --all
       The first form of the command operates on a single volume. If a size
       is specified, then the LVM volume is extended by that size (step 1),
       and the file system it contains is extended to use the new space
       made available in that volume (step 2). If a size is not specfied,
       then the file system contained in that volume is extended (i.e.,
       step 2 only).

       The "--all" form of the command is used to perform step 2 across
       all volumes on the system.

       For more information, see the examples at the top of this help.

       If "--remaining" is specified for the size, then the specified
       volume is extended with all remaining free space on that disk.
       If a specific increment is provided, then the volume is extended
       by that amount, reducing the amount of free space on the disk
       by that amount. Specific sizes are in the form of a number
       (e.g., "10", "10.5", or ".5") and a unit. Units are "m" for
       mebibites, "g" for gibibytes", and "t" for tebibytes".

       The smallest increment that can be specified is 100 MiB.

       Example invocations:

           sys volmgt --extend /var/log/Avaya 10g
           sys volmgt --extend /var/log/Avaya 10.5g
           sys volmgt --extend /var/log/Avaya 0.5g
           sys volmgt --extend /var/log/Avaya .5g
           sys volmgt --extend /var/log/Avaya 500m
           sys volmgt --extend /var/log/Avaya --remaining
           sys volmgt --extend /var/log/Avaya

 --reset
       Resets internal tracking data. Use this if this script is blocked
       on an invalid background progress indication. This condition can
       arise if a background operation was prematurely terminated due to,
       for example, a system reboot. Verify that no background operations
       are in progress prior to executing this command, through verification
       of the process id as reported by the "--status" argument.

[admin@server4889amm ~]$
```

Partitioning examples: sys volmgt --summary

Avaya Multimedia Messaging supports partitioning versions 1.0 and 2.0.

The following example shows a summary of the information provided by this command for a version 1.0 partitioned system:

```
[admin@server4889amm ~]$ sys volmgt --summary
```

```
                          Disk and Volume Summary

+----------- Disk ------------+------------------- Volume ---------------------+
|                              |                      LVM        File System    |
| Num  Name     Size     Free |    Name              Size      Size     Usage |
+------------------------------+-----------------------------------------------+
|  2   sdb      25.00    0.00 | /home                 4.00      3.94      1.49 |
|                              | /opt/Avaya           21.00     20.67      1.27 |
+------------------------------+-----------------------------------------------+
|  3   sdc      10.00    0.00 | /media/data          10.00      9.84      0.15 |
+------------------------------+-----------------------------------------------+
```

The following example shows a summary of the information provided by this command for a version 2.0 partitioned system:

```
[admin@server4950amm ~]$ sys volmgt -s

                          Disk and Volume Summary

+----------- Disk ------------+------------------- Volume ---------------------+
|                              |                      LVM        File System    |
| Num  Name     Size     Free |    Name              Size      Size     Usage |
+------------------------------+-----------------------------------------------+
|  1   sda      41.78    0.00 | /                     4.00      3.81      1.26 |
|                              | /home                 4.00      3.81      0.05 |
|                              | /opt/Avaya           14.97     14.61      1.14 |
|                              | /tmp                  2.81      2.71      0.01 |
|                              | /var                  3.00      2.89      0.03 |
|                              | /var/log              2.00      1.91      0.00 |
|                              | /var/log/audit        3.00      2.89      0.00 |
|                              | swap                  8.00       n/a       n/a |
+------------------------------+-----------------------------------------------+
|  2   sdb      60.00    0.00 | /var/log/Avaya       60.00     58.93      0.05 |
+------------------------------+-----------------------------------------------+
|  3   sdc      20.00    0.00 | /media/data          20.00     19.56      0.04 |
+------------------------------+-----------------------------------------------+
|  4   sdd      10.00    0.00 | /media/cassandra     10.00      9.71      0.02 |
+------------------------------+-----------------------------------------------+
```

Chapter 4: Management of Avaya Multimedia Messaging with the administration portal

The following sections describe the tasks you can perform on the web-based administration portal. You can make changes to server settings in the administration portal at any time.

Prerequisites for accessing the admin portal

- Complete server installation and configuration. You cannot access the Avaya Multimedia Messaging web-based administration portal until the server is configured.
- To log in to the web-based administration portal, you must configure the Administrator role as part of LDAP configuration. The format for the user name might be `user@yourdomain.com` or `domain\user`, depending on the configuration of the LDAP server.

Browser requirements for the admin portal

To access the administration portal, you must use one of the following web browsers:

- Internet Explorer 9, 10, or 11.
- The latest version of Mozilla Firefox or the version before it.
- Google Chrome 53 and later.

Logging in to the Avaya Multimedia Messaging administration portal

Procedure

Log in to the Avaya Multimedia Messaging administration portal.

The URL for gaining access to the administration portal is `https://<hostname>:8445/admin`.

Important:

For the hostname, always use the same Avaya Multimedia Messaging server FQDN that you use for generating certificates. You will be redirected to the Login page if you use the IP address instead of the FQDN.

To gain access to the web-based administration portal, you must use an account that has the Administrator role defined in the LDAP server configuration.

Result

A menu is displayed on the left side of the screen.

Starting and stopping the Avaya Multimedia Messaging service

Procedure

1. In the Navigation pane, click **Service Control** > **Application Management**.
2. Select the check box for the Avaya Multimedia Messaging service or any other available service.
3. Click **Start** to enable the Avaya Multimedia Messaging service.

   The Avaya Multimedia Messaging server handles client requests when the service is running.
4. Click **Stop** to disable the Avaya Multimedia Messaging service and put the server into service mode.

   Clients are unable to send or receive data from the Avaya Multimedia Messaging server while the service is stopped.

Managing application sessions

About this task

Use this procedure to:

- Set a timeout period for terminating inactive, idle, or unattended sessions.
- Manage concurrent HTTP sessions.

Procedure

1. In the Navigation pane, click **Service Control** > **Application Management**.
2. In the Application Properties area, complete the required settings, which are described in Application Properties field descriptions on page 29.

3. Click **Save**.

Application Properties field descriptions

Name	Description
Admin HTTPSession Timeout (minutes)	The timeout period for the Avaya Multimedia Messaging web administration portal. You can enter a value between 1 and 60 minutes. The default value is 15 minutes.
Application HTTPSession Timeout (minutes)	The timeout period for application components. You can enter a value between 3 and 15 minutes. The default value is 15 minutes.
Maximum Concurrent HTTP Sessions	The maximum number of active sessions that are available for application components. If the number of sessions exceeds the configured value for any component, a 503 error, which indicates that service is unavailable, is generated by that component. You can enter a value between 100 and 1,000,000. The default value is 200,000.
Concurrent HTTP Sessions per User	The number of active sessions that are available per user. If the number of sessions exceeds the configured value for any user, a 429 error, which indicates that there are too many requests, is sent as a response to the user's request. You can enter a value between 10 and 100. The default value is 50.

Managing server storage

About this task

When setting the storage management value, you must be aware of the storage available on the Avaya Multimedia Messaging server. Conversations that remain open for long periods of time consume more storage space than conversations that are closed after a shorter period, such as 30 days of inactivity. If you do not change the value, conversations automatically close after 30 days of inactivity.

The changes made to the storage management value take effect after an audit is performed. This occurs around 4 AM in Avaya Multimedia Messaging server time.

Procedure

1. In the Navigation pane, click **Storage Management**.
2. Adjust the value to indicate how long a conversation remains active.

When participants are inactive in an IM conversation for the number of days specified in this field, the conversation closes. Users can no longer contribute to closed conversations.

Managing messaging domains

About this task

Use this procedure to update the list of messaging domains.

Procedure

1. In the Navigation pane, click **Client Administration** > **Client Settings**.
2. In the Messaging Domains area, to add a new domain:
   a. In **Add new Messaging Domain**, enter the new messaging domain name.
   b. Click **Add To List**.
3. In the Messaging Domains area, to remove a domain:
   a. In the **Messaging Domain List** box, select the messaging domain.
   b. Click **Delete Selected**.
4. Click **Save**.

Managing client device certificates

About this task

Use this procedure to set the client device certificate policy. This policy determines how the server validates certificates for Avaya Multimedia Messaging clients.

Procedure

1. In the Navigation pane, click **Client Administration** > **Client Settings**.
2. In the Client-Device Certificate Policy area, configure the policy for the administration portal by clicking the OAMP drop-down list or for the REST service by clicking the REST drop-down list and then choose one of the following:
   - **NONE**: The server does not check for a certificate. The connection is established with or without a valid certificate.
   - **OPTIONAL**: The server requests a certificate. The connection is established with or without a certificate, but the process stops if a client provides an invalid or untrusted certificate, and the system returns the error code `HTTP 400`.
   - **OPTIONAL_NO_CA**: The server requests a certificate. The connection is established with any valid certificate even if the CA is untrusted, but the process stops if a client provides an invalid certificate, and the system returns the error code `HTTP 400`.

- **REQUIRED**: The server requests a certificate. The server rejects a connection if a client fails to provide a valid certificate, and the system returns the error code `HTTP 400`.

The default value is: **OPTIONAL**.

Note:

If the Client certificate policy for an interface is set to **OPTIONAL**, **OPTIONAL_NO_CA**, or **REQUIRED**, client certificates when presented to the client:

- Must have digitalSignature key usage if key usage information is present.
- Must have id-kp-clientAuth if extended key usage is present. This is the TLS WWW client authentication extended key usage.

If the certificate does not have key usage, key usage is not validated and the certificate is allowed for all key usages.

3. **(Optional)** If you want to set the policy from the shell command line, enter the following command:

```
sudo ./clitool.sh clientCertificateVerificationConfig oampGuiClient <_value_>
```

where _value_ can be `off` (NONE) or `optional` (OPTIONAL) or `on` (REQUIRED).

4. Click **Save**.

Updating feature entitlements

About this task

Feature entitlements determine privileges for Avaya Multimedia Messaging users.

Procedure

1. In the Navigation pane, click **Client Administration** > **Feature Entitlements**.
2. Use the arrows to move users between the **Available** and **Selected** categories.

   Users in the **Selected** category can access enhanced user privileges and send attachments in an IM conversation.
3. Click **Search** to select users from your corporate directory.

   The selected users are the users for whom you want to update feature entitlements.
4. Click **Bulk Load From File** to add a large group of users to the **Available** category.

   The file that contains the users must be in the CSV format and list one user on each line as `<first name>, <last name>, <email_address>` or `<email>`.

   The following is an example of how to list users in the file:

```
Doe, John, john@doe.com
jane@doe.com
```

5. Click **Apply**.

Feature entitlements field descriptions

The informative fields in the feature entitlements section display the following information:

Name	Description
WebLM Server	The WebLM Server is the license server hosting the Avaya Multimedia Messaging license. If the License Server Status is *Normal*, the license is correctly installed and the Avaya Multimedia Messaging server can communicate properly with the WebLM server.
Entitlement Status	Displays the current status and details of the license.
Entitlement Type	Displays the type of license with assigned value.
Validity	Displays the validity and can have one of the following values: • *VALID* if the license file is valid and the server can communicate with the WebLM Server. • *NO_LICENSE* if the license file cannot be found on the WebLM Server. • *EXPIRED* if install license file is expired. • *INVALID* if the license file on WebLM Server is invalid.
Expiry	Displays the date when the installed license file will expire.
Licensed	Displays the total number of available licenses.
Available	Displays the number of licenses still available for use.
Acquired	Displays the number of licenses currently acquired.

Updating enterprise directory settings

Procedure

1. In the Navigation pane, click **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.
2. Under **Server Address and Credentials**, update your configured LDAP server address and server credentials if required.

You populate the LDAP settings as part of the server configuration, but you can change the values of these settings with the administration portal. Additional information about the description of LDAP settings is available in *Deploying Avaya Multimedia Messaging*.

3. Click **Test Connection** to verify your LDAP connection.
4. Under **User Synchronization Update Instructions**, set the rate at which the Avaya Multimedia Messaging server synchronizes with the users in your enterprise directory.
5. Click **Force LDAP Sync** to force an immediate user synchronization.

   Warning:

   Performing a force update during traffic runs may lead to traffic failure.
6. Click **Save** in each section to save your changes.

Managing federation gateway connections

About this task

Use this procedure to manage the configuration of the connection adaptor.

Procedure

1. In the Navigation pane, click **Server Connections** > **Federation Configuration**.
2. In the appropriate section, do one of the following:
   - Add a new adaptor if required to complete federation configuration.

     Adaptors are required for Presence Services and Microsoft federation configuration. For more information, see the links at the end of this procedure.
   - Edit an existing adaptor.
   - Delete an existing adaptor.

Verifying cluster nodes

About this task

Use the following procedure if you are experiencing network issues with your server and want to make sure that all clustered nodes are running properly.

Procedure

1. In the Navigation pane, click **Cluster Configuration** > **Cluster Nodes**.
2. Check to see if the Avaya Multimedia Messaging nodes are active and running properly.

Cluster field descriptions

The following fields supply additional information about the cluster:

Name	Description
Virtual IP	Displays the virtual IP address, if a virtual IP address is configured.
Virtual IP Master	Displays the virtual IP master node, if a virtual IP address is configured.
Virtual IP Backup	Displays the virtual IP backup node, if a virtual IP address is configured.
Seed Node IP	Displays the IP address of the seed node of the cluster.

Generating performance data and statistics

About this task

Use this procedure to generate performance data and statistics in the Avaya Multimedia Messaging web administration portal.

Procedure

1. In the Navigation pane, click **Performance** > **Messaging**.
2. Click **Generate Data** to generate historical data.
3. From the **Data** drop-down menu, select the type of data for which you want to generate a graph.

   You can generate the following types of data:

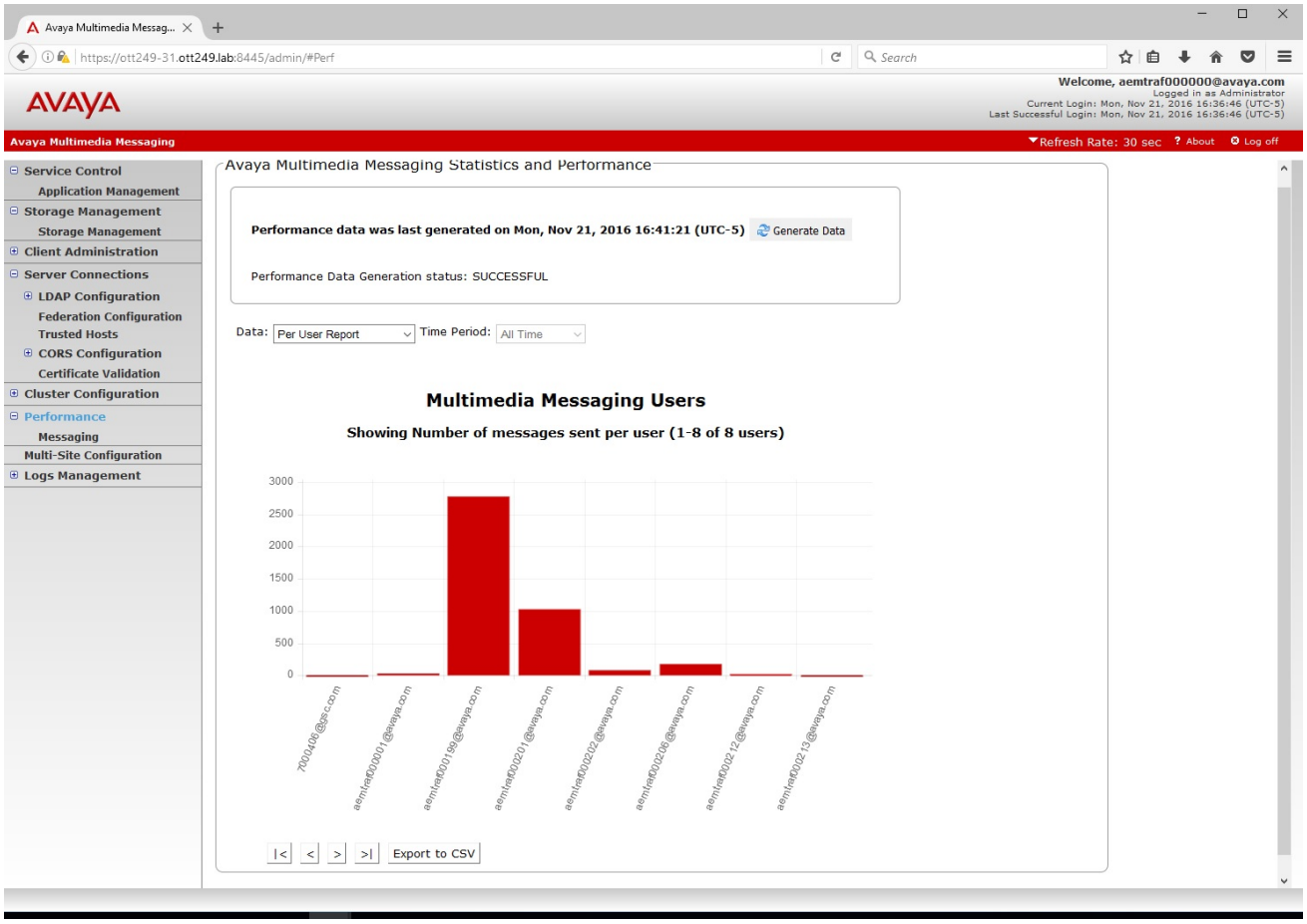
   - The number of Avaya Multimedia Messaging users.
   - Message traffic.
   - The number of messages sent per user.
   - Attachment breakdown with media types and size.
4. Select a time period.

Result

The graph is generated. You can also export it to CSV format.

Example

The following is an example of a graph showing the total number of users.



Adding and editing local and remote sites for multisite configuration

About this task

Use this procedure to update the configuration of a local or remote site. For more information about multisite configuration, see Avaya Multimedia Messaging multisite adapter administration and management on page 43.

Procedure

1. In the Navigation pane, click **Multi-Site Configuration**.
2. In the Local Site Information and Remote Site Information areas, you can:
   - Add a new site name, FQDN, and port details.
   - Edit a site.
   - Delete a site.

Managing logs

About this task

Use this procedure to adjust log levels and collect log files. Support personnel can use the collected log files to assist with troubleshooting.

Procedure

1. In the Navigation pane, click **Logs Management** > **Log Level**.
2. In the Adjust Service Logging Level area, do the following:
   a. From the **Logger** drop-down menu, select the log type.
   b. From the **Current logging level** drop-down menu, select the level of detail that you want captured in log files.
   c. Click **Save** to apply your changes.
3. In the Collect Logs area, do the following:
   a. **(Optional)** To limit the size of the download, type a number between 1 and 20 in **Number of rotated log files to collect (1–20)**.

      This setting specifies the number of files from the log file history to include in the log collection. Leaving this setting empty collects all available logs.
   b. To collect logs for a node, click **Collect** in the corresponding row.
   c. To download the collected logs for a node, click **Download**.
   d. For a cluster, if logs from all the nodes are required, repeat steps 3.b on page 36 and 3.c on page 36.

Updating media size limits

Procedure

1. In the Navigation pane, click **Client Administration** > **Client settings** > **Media Size Limits**.
2. Adjust the media size limits for attachments exchanged during IM conversations.

   You can update the size limit for the following types of attachments:

   - Video files
   - Audio files
   - Images
   - Text-based messages
   - Other generic attachments

   The media size limits you set directly affect available storage on the Avaya Multimedia Messaging server.

Configuring the LDAP attribute mappings

About this task

Use this procedure to configure LDAP attribute mappings.

Procedure

1. In the Navigation pane, click **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.
2. In the **Server Address and Credentials** field, click **Modify Attribute Mappings**.
3. Modify the attribute mappings as required.
4. To restore the last saved values, click **Reset**.
5. Click **Save**.

Chapter 5: Integrated Windows Authentication administration and management

Integrated Windows Authentication (IWA) enables you to log in to different services with the same credentials. To support IWA, some Avaya Multimedia Messaging server administration is required. Users must be able to authenticate to the Avaya Multimedia Messaging API using a preexisting authentication to a Windows domain. Avaya Multimedia Messaging uses SPNEGO to negotiate authentication with the client and Kerberos to validate the authentication of the client user. User roles are retrieved normally through LDAP.

Use the following sections to complete IWA configuration on the Avaya Multimedia Messaging and Active Directory servers. Errors in the setup might cause the authentication to fail. You can enable debug logs to assist with troubleshooting. For general IWA troubleshooting tips, see Troubleshooting best practices for IWA on page 86.

Authentication prerequisites

You must have the following to set up IWA:

- An Active Directory server.
- A DNS server for the DNS domain of Active Directory.
- A Windows client on the Active Directory domain.
- An Avaya Multimedia Messaging server that is resolvable by the DNS.
- A domain user that will be mapped to the Service Principal Name (SPN) of the Avaya Multimedia Messaging server.
- Domain users for all individual users.

Important:

The Active Directory, Windows client, and Avaya Multimedia Messaging server must resolve each other's FQDNs. However, they do not need to use the same DNS server or to belong to the same zone.

Setting up the Windows Domain Controller

About this task

Use this procedure to add the Avaya Multimedia Messaging SPN to a domain user on the Windows Domain Controller or the Active Directory server. The SPN must be unique across the domain. To avoid issues with duplicated SPNs, keep track of any SPNs assigned to users.

For detailed information about Domain Controller users, see https://technet.microsoft.com/en-us/library/cc786438(v=ws.10).aspx.

Important:

Enter all commands exactly as shown in this procedure, and use the following guidelines:

- The host name used to access the Tomcat server must match the host name in the SPN exactly. Otherwise, authentication will fail.
- The server must be part of the local trusted intranet for the client.
- The SPN must be formatted as `HTTP/<host name>` and must be exactly the same everywhere.
- The port number must not be included in the SPN.
- Only one SPN must be mapped to a domain user.
- The Kerberos realm is always the uppercase equivalent of the DNS domain name. For example, `EXAMPLE.COM`.

Before you begin

Review Authentication prerequisites on page 38.

Procedure

1. Create a new IWA service account.

   Do not select an account associated with an existing user.

2. If you are using Active Directory 2008 or higher, run the following command to attach the SPN to the domain name:

   ```
   setspn -S HTTP/<FRONT-END FQDN> <Domain user login>
   ```

   In the following example, “<FRONT-END FQDN>” is `amm.example.com` and “<Domain user login>” is `amm_user`:

   ```
   setspn -S HTTP/amm.example.com amm_user
   ```

   Important:

   - If you are using Active Directory 2003, you must use `setspn -A` instead of `setspn -S`.
   - When you use `setspn -S`, the Active Directory server searches for other users with the same SPN assigned. If the server finds a duplicated SPN, see step 3 on page 40.

3. **(Optional)** To remove a duplicated SPN from another user, run the following command:

```
setspn -d <SPN> <old user>
```

4. Use the following command to generate a `tomcat.keytab` file:

```
ktpass /out c:\tomcat.keytab /mapuser <Domain User Login>@<Kerberos realm> /princ
HTTP/<FRONT-END FQDN>@<Kerberos realm> /pass +rndPass /crypto all /kvno 0
```

   In the following example, `<Domain User Login>` is `amm_principal`, `<Kerberos realm>` is `EXAMPLE.COM`, and `<FRONT—END FQDN>` is `amm.example.com`:

```
ktpass /out c:\tomcat.keytab /mapuser amm_user@EXAMPLE.COM /princ HTTP/
amm.example.com@EXAMPLE.COM /pass +rndPass /crypto all /kvno 0
```

   The `tomcat.keytab` file enables Avaya Multimedia Messaging to authenticate against the Kerberos Key Distribution Center (KDC). This file assigns a random password to the user.

5. Transfer the generated `tomcat.keytab` file to the Avaya Multimedia Messaging server using the OAMP administration portal.

   Since this is a credentials file, handle it securely and delete the original file after this file is imported into the Avaya Multimedia Messaging server. You can generate and re-import a new `tomcat.keytab` file anytime.

Windows Domain Controller command descriptions

Setting up the Windows Domain Controller on page 39 uses the following command values:

Command	Description	Example value
<FRONT—END FQDN>	The REST front host FQDN of the Avaya Multimedia Messaging server. This is either the FQDN of the Virtual IP assigned to the cluster (if internal load balancing is used) or the FQDN of the external load balancer, if it is used.	`amm.example.com`
<Domain user login>	The Windows login ID for the domain user you created.	`amm_user`
<Kerberos realm>	The domain name for the Kerberos realm. The Kerberos realm is always the uppercase equivalent of the DNS domain name.	`EXAMPLE.COM`

Setting up IWA on the Avaya Multimedia Messaging administration portal

About this task

This procedure describes the changes you must perform on the Avaya Multimedia Messaging administration portal to configure IWA.

Procedure

1. On the Avaya Multimedia Messaging administration portal, click **LDAP Configuration**.
2. In the Server Address and Credentials area, do the following:
   a. In the **Windows Authentication** drop-down menu, select **Negotiate**.
   b. In the Confirm Action dialog box, click **OK**.
   c. In **UID Attribute ID**, type `userPrincipalName`.

      If this field is not set to `userPrincipalName`, you might encounter license issues and other unpredictable behavior.
   d. Ensure that the other settings are appropriate for the LDAP configuration of your Domain Controller.

      Important:

      The LDAP server that you use must be the domain controller with the appropriate Active Directory version as the server type.
3. In the Configuration for Windows Authentication area, complete the following information using the same values you provided when setting up the Windows Domain Controller:
   a. In **Service Principal Name (SPN)**, type `HTTP/<FRONT—END FQDN>`.

      For example, `HTTP/amm.example.com`.
   b. Click **Import** to import the `tomcat.keytab` file transferred from the Windows Domain Controller.

      In cluster deployments, the file is transferred to all nodes in the cluster. An additional option is available to send the file to specific nodes in a cluster.
   c. In **Kerberos Realm**, type the Kerberos realm, which is usually in all uppercase letters. For example, `EXAMPLE.COM`.
   d. In **DNS Domain**, type the DNS domain of the Domain Controller.

      For example, `example.com`.
   e. **(Optional)** Select the **Use SRV Record** check box.
   f. **(Optional)** If **Use SRV Record** is not selected, in **KDC FQDN**, type the FQDN of the Domain Controller.

      This value also includes the DNS domain at the end. For example, `ad.example.com`.
   g. **(Optional)** In **KDC Port**, retain the default value of 88.

      This field is only visible if **Use SRV Record** is not selected.
   h. **(Optional)** In a cluster deployment, click **Send Keytab File** to send the `tomcat.keytab` file you imported in step 3.b on page 41 to a specific node.

      This option is useful if the import to a node failed or if you add a new node to your cluster.

4. Click **Save** to retain the settings and restart the server.

   The settings that you updated are used to generate the files needed to configure the Tomcat JAASRealm and the corresponding Sun JAAS Login module for GSS Bind.

Chapter 6: Avaya Multimedia Messaging multisite adapter administration and management

You can use a multisite adapter to share messages between two or more Avaya Multimedia Messaging sites. Each site can either consist of a standalone Avaya Multimedia Messaging or an Avaya Multimedia Messaging cluster. The adapter only runs on one node in a cluster. Each multisite adapter has a Sender and a Receiver. The Receiver creates connectors to the other sites within the Avaya Multimedia Messaging federation. When a conversation is updated with a message that includes a recipient from a different site, the message is shared with the remote site. The Sender defines a REST API used by the connectors and responds to requests from the connectors.

Important:

The allowable media sizes on each site must be the same. Otherwise, the files that are allowed by a site with a larger media size, which exceeds another site's smaller allowable media size, will not be transferred to that site.

Connector types for the Avaya Multimedia Messaging adapter

The multisite adapter uses the following types of connectors:

Conversation ID connector

The adapter creates a separate long-poll connector for each enabled remote site. This connector requests conversation IDs from the remote site. If a remote site has one or more conversations with a message that includes recipients on the local site, a 200OK response is sent with the conversation IDs. The request from the connector is site-based, not user-based. The response might include conversation IDs for messages sent from the remote site to any valid user homed on the local site.

Messages connector

When the Conversation ID connector receives a response with conversation IDs, the adapter creates a separate connector for each received conversation ID and requests the relevant conversation messages from the remote site. The response only includes the messages in the conversation that have at least one recipient homed on the local site.

Message Parts connector

If a received message has an attachment, the adapter creates a separate connector to request the message parts from the remote site. After the adapter receives a message and attachments are transferred from the remote site, the Avaya Multimedia Messaging service sends the message to the local homed users.

Home site ID

If the multisite adapter is enabled, all users must have a home site ID. This ID is not case sensitive. If no home site ID exists or if you are using an incorrect home site ID, requests to Avaya Multimedia Messaging will fail.

Avaya Multimedia Messaging obtains the home site ID for the user from the Presence Services profile IM Gateway in System Manager. The IM Gateway value is provided when Avaya Multimedia Messaging requests a directory search for the user's address. The Avaya Multimedia Messaging SIP entity is a placeholder and does not require corresponding e arntity links.

Note:

The user synchronization process for multisite deployments will also update the home site ID of users if they were changed in System Manager. This process updates Avaya Multimedia Messaging to reflect the recent changes made in System Manager. The process must be run on both the user's former and new sites. Changes are reflected immediately after the user synchronization and home site audit are completed.

Multisite adapter field descriptions

The multisite adapter is configured for every Avaya Multimedia Messaging site. The adapter is only active if local site and remote site information is provisioned. For information about adding and editing local and remote sites, see Adding and editing local and remote sites for multisite configuration on page 35.

The following table describes the multisite adapter configuration fields:

Field	Description
Name	The Site ID. Each site must have a local site ID with at least one remote site ID. The site ID is a valid IM Gateway provisioned in System Manager. The local Site ID of one site must match a remote site ID on the remaining sites.
Address	The FQDN of the cluster or standalone server. The local address of one site must match the remote address on the remaining sites.
Port	The default port used by the Avaya Multimedia Messaging multisite adapter is 8441.

Field	Description
Status	This field displays the status of the connection to the remote site, and it can not be edited.
Enabled	A checkbox that indicates whether a connector is created. If the checkbox is selected, a connector is created to connect to the remote site and the interface displays `yes`. If the checkbox is not selected, no connector is created and the interface displays `no`.
Timeout	The connection alarm timeout in seconds. If a problem occurs with the connection to the remote site, the connector tries to establish a connection five times before raising an alarm. The timeout value represents the time duration between retries before the alarm is raised. This timeout allows for flexibility if different network characteristics exist between remote sites.
Long Poll Timeout	The menu that contains the **Recommended Long Poll Timeout** configuration option. Use this option for setting the value to use in the Avaya-Request-Timeout HTTP header for long-poll requests. **Important:** The long poll timeout value can be from 30 to 120. Lowering this value results in increased traffic on the server, but network configuration may require that you set a lower value. If you do not configure this parameter, the default database initialization setting is used.

Chapter 7: Virtual hardware adjustments

The following sections describe how to perform virtual hardware adjustments on a virtual machine. The required virtual hardware adjustments depend on your system's partitioning version. The current release supports both partitioning versions 1.0 and 2.0. When you upgrade from a previous release, the system remains on partitioning version 1.0. The only way to have the system on partitioning version 2.0 is to deploy an OVA from the current Release 3.2.

For information about disk volume sizes on partitioning versions 1.0 and 2.0, see the disk volume specifications in *Avaya Multimedia Messaging Reference Configuration*.

Adjusting the memory resource of a virtual machine

About this task

This procedure describes how to adjust the memory size and memory reservation for a virtual machine.

Procedure

1. If the virtual machine is installed and running, log in to the system, and shut down the operating system by running the following command:

   ```
   sudo shutdown -h now
   ```

2. Stop your virtual machine if it is still running.
3. Click **Edit Settings**.
4. Click the **Hardware** tab and select **Memory**.
5. From **Memory Configuration**, enter the new numeric value for the memory size and select the unit of measure.
6. Click the **Resources** tab.
7. From **Settings**, click on **Memory**.
8. In **Resource Allocation**, use the **Reservation** slider to set the desired memory reservation.
9. Click **OK**.

Adjusting the CPU resource of a virtual machine

About this task

This procedure describes how to adjust the number of virtual CPUs and the CPU reservation for a virtual machine.

Procedure

1. If the virtual machine is installed and running, log in to the system, and shut down the operating system by running the following command:

   ```
   sudo shutdown -h now
   ```

2. Stop your virtual machine if it is still running.
3. Click **Edit Settings**.
4. From the Hardware tab, click **CPUs**.
5. In **Number of virtual sockets**, select the desired number of virtual CPUs for the virtual machine.
6. In **Number of cores per socket**, select **1**.
7. Click the **Resources** tab.
8. From **Settings**, click **CPU**.
9. In **Resource Allocation**, use the **Reservation** slider to set the desired CPU reservation.
10. Click **OK**.

Adjusting the virtual network interface

About this task

This procedure describes how to adjust the virtual network interface setting for your virtual machine.

Procedure

1. Click **Edit Settings**.
2. Click the **Hardware** tab.
3. Click **Network adapter 1**.
4. From **Network Connection**, select the desired network.
5. Click **OK**.

Increasing the size of a virtual disk

About this task

Each virtual disk holds one or more disk volumes. Before you can increase the size of a disk volume, you must first increase the size of the host disk to provide the required disk space.

This procedure describes how to adjust the size of a virtual disk in the Virtualization Enabled (VE) environment. The VE environment uses the standard VMware infrastructure facilities. This procedure applies to virtual machines on both partitioning versions 1.0 and 2.0.

Before you begin

- Ensure that the system layer on the virtual machine has been upgraded to the current Release 3.2. You can verify this using the `sys versions` command.
- Delete all snapshots from the virtual machine. You cannot adjust disk sizes while snapshots exist.
- Determine the disk volume to be increased in size.
- Determine the disk number that hosts the disk volume. You can use the `sys volmgt --summary` command for more information.

Procedure

1. If the virtual machine is installed and running, log in to the system, and shut down the operating system by running the following command:

   ```
   sudo shutdown -h now
   ```

2. Stop your virtual machine if it is still running.
3. Click **Edit Settings**.
4. From the Hardware tab, select the hard disk to be enlarged.
5. In **Disk Provisioning**, enter a higher value for the disk size and select the appropriate unit of measure.
6. Click **OK**.
7. Power on the virtual machine.

Next steps

Increase the size of the disk volume.

Increasing the size of a disk volume on a virtual machine

About this task

Use this procedure to increase the size of a disk volume. The following are examples of situations where you might need to increase the disk volume size:

- The deployment of the latest Avaya Multimedia Messaging OVA requires an increase in the size of the `/media/data` volume in accordance with the size of the supported user base.

- The upgrade process for an OVA from a previous release requires an increase in the size of one or more disk volumes.

In rare circumstances, Avaya support might recommend specific increments in disk volume sizes to address unexpected disk engineering issues.

Before you begin

Increase the size of the virtual disks that host the volumes to be increased. This process makes new disk space available. For example, if the volume requires an additional 20.0 GiB of space and the host disk is currently 50.0 GiB, then you must change the size of the host disk to 70.0 GiB.

Procedure

1. If the virtual machine is not running, then power it up.
2. Scan the disks on the virtual machine to detect newly available disk space by running the following command:

   ```
   sys volmgt --scan
   ```

   Tip:

   For more information about this command, you can use the following commands:

   - For syntax help: `sys volmgt -h`
   - For verbose help: `sys volmgt -hh`

   After the scan is complete, an updated file system summary is displayed. The newly available disk space is reported in the Disk > Free column.
3. Allocate all of the unused space on the disk to the target volume by running the following command:

   ```
   sys volgt --extend <volume> --remaining
   ```

   For `<volume>`, specify the name of the volume as it appears in the Volume > Name column.

   All `--extend` operations are run as background tasks.

   a. To monitor the status of the operation in progress or of the last completed operation, run the following command:

      ```
      sys volmgt --monitor less
      ```

   b. To gather all volume management logs into a zip file in the current working directory, run the following command:

      ```
      sys volmgt --logs
      ```

   c. If a disk has multiple volumes and more than one volume is being increased in size, use one of the following commands to allocate a specific amount of unused space to a volume:

      ```
      sys volgt --extend <volume> <x>m
      sys volgt --extend <volume> <x>g
      sys volgt --extend <volume> <x>t
      ```

In these commands, `m` means megabytes, `g` means gigabytes, `t` means terabytes, and `<x>` is a decimal number. For example, the following increments the `/var/log` volume by 10.5 GiB:

```
sys volmgt --extend /var/log 10.5g
```

4. Verify that the new space has been allocated to the volume by running the following command:

   ```
   sys volmgt --summary
   ```

   Due to disk overhead, the size of the volume reported under the Volume > LVM Size column will never exactly match the size reported under the Volume > File System > Size column.

   a. If you suspect that the file system size is not correct, verify that the operation is complete by running the following command:

      ```
      sys volmgt --status
      ```

   b. If the status is reported as “Complete”, you can correct the situation using `--extend` without an increment value:

      ```
      sys volmgt --extend /var/log
      ```

      This operation does not add more space to the volume that hosts the file system. Instead, it reissues the command to make full use of the current volume.

      Tip:

      Similar to using `--extend` to increase volume sizes, you can also monitor the `--extend` operation and gather logs using the following commands:

      ```
      sys volmgt --monitor less
      sys volmgt --logs
      ```

Chapter 8: Monitoring options

Scheduling periodic repairs of database inconsistencies

About this task

On every Avaya Multimedia Messaging node, a periodic repair of the database must be performed to ensure that the information present in the database is consistent throughout the nodes.

Procedure

1. Open the Avaya Multimedia Messaging server CLI.
2. Run the crontab command, by also specifying the name of the Linux user on the behalf of which the task is performed.

   For example:

   ```
   crontab -e
   ```

3. In the crontab file, add a line similar to the following:

   ```
   05 23 * * 6 <installation_directory>/cassandra/1.2.7/bin/nodetool -u
   <cassandra_username> -pw <cassandra_password> repair
   ```

   This example contains a crontab configuration that runs the **nodetool** command once a week, on Saturday, at 11:05 PM.

   For more information about automating system tasks, see the Red Hat documentation.

   `<installation_directory>` represents the installation directory of the Avaya Multimedia Messaging server.

   `<database_user>` and `<database_password>` represent the user name and the password configured during the installation for gaining access to the Cassandra database.

   Note:

   The command must run at least once in a week, when the network traffic is low. For example: during the night, on weekends.

   For more information, see the documentation of the Cassandra database.

Logs and alarms

Logs

Most of the log files for the Avaya Multimedia Messaging components are located in the `/opt/Avaya/MultimediaMessaging/<version>/logs/` and `/opt/Avaya/logs/` directories. Other components such as Tomcat or nginx store the log files in specific directories.

The logs written by the Avaya Multimedia Messaging server are also visible in the Avaya Aura® System Manager Log Viewer.

Alarms

The alarms that the Avaya Multimedia Messaging triggers are visible in the Avaya Aura® System Manager Alarm Viewer.

Important:

To enable alarm reporting on Avaya Aura® System Manager, you must create SNMP user and target profiles. For more information, see *Administering Avaya Aura® System Manager*.

The following table contains the major and critical alarms used by the Avaya Multimedia Messaging server and their descriptions:

Table 2: Avaya Multimedia Messaging alarms

Name	Description	Severity
avESMComponentNotRunning	The system raises this alarm when a component has stopped functioning, does not start, or does not restart: • Cassandra • Nginx • Tomcat • Mobicents • snmpd • spiritAgent • glusterd/glusterfsd • keepalived • openfire	Major
avAMMLDAPServerConnectionLost	The system raises this alarm if the Avaya Multimedia Messaging application cannot connect to the corporate LDAP server. This alarm can be triggered manually by testing the LDAP connectivity through the Avaya Multimedia Messaging administration portal or as the result of an audit that is being performed every 60 seconds.	Major

Name	Description	Severity
	The Avaya Multimedia Messaging application relies on the LDAP server for authentication, authorization and identity management.	
avAMMDataStoreAccessFailed	The system raises this alarm if the Avaya Multimedia Messaging application cannot connect to the database or the database cluster. This alarm is triggered by an audit process performed every 60 seconds.	Major
avAMMMediaStoreAccessFailed	The system raises this alarm if the Avaya Multimedia Messaging application cannot connect to the distributed file system, GlusterFS. This alarm is triggered by an audit process performed every 60 seconds. Under this alarm condition, the end users are only able to send text messages. Multimedia and generic attachments are rejected by the Avaya Multimedia Messaging server.	Major
avAMMDBStorageReachedCriticalThreshold	The system raises this alarm when the disk partition size where the Cassandra database is hosted exceeds 95% of the total size. The disk audit is performed every 60 minutes.	Critical
avAMMRESTCertificateFault	The system raises this alarm if the REST certificate is about to expire, has expired or if the application is unable to read the certificate file. The certificate audit is performed every 60 seconds.	Major
avAMMOAMCertificateFault	The system raises this alarm if the OAM certificate is about to expire, has expired or if the application is unable to read the certificate file. The certificate audit is performed every 60 seconds.	Major
avAMMSIPCertificateFault	The system raises this alarm if the SIP certificate is about to expire, has expired or if the application is unable to read the certificate file. The certificate audit is performed every 60 seconds.	Major
avAMMLicenseErrorModeActive	The system raises this alarm if one or more license errors are present.	Major
avAMMLicenseRestrictedModeActive	The system raises this alarm if one or more license errors are present and the 30 day grace period has expired.	Critical
avAMMRemoteDomainConnectionLost	The system raises this alarm if the Avaya Multimedia Messaging application is unable to ping one or more remote domains.	Major

Name	Description	Severity
	The audit is performed every 30 seconds.	
avAMMVirtualIPAcquiredFromPrimary	The system raises this alarm when the primary node hosting the virtual IP address of the application has stopped.	Major
avAMMSMGRLDAPServerConnectionLost	The system raises this alarm if the application cannot establish connectivity with the Avaya Aura® System Manager LDAP server. This alarm can be triggered manually by testing the LDAP connectivity through the Avaya Aura® System Manager administration portal or as the result of an audit that is being performed every 60 seconds.	Major
avAMMMediaStorageReachedWarningThreshold	The system raises this alarm when the disk partition size where the media files are stored exceeds 90% of the total size. The disk audit is performed every 60 minutes.	Minor
avAMMMediaStorageReachedCriticalThreshold	The system raises this alarm when the disk partition size where the media files are stored exceeds 95% of the total size. The disk audit is performed every 60 minutes.	Critical
avAMMTimeServerSynchronizationLost	The system raises this alarm if the Avaya Multimedia Messaging application does not have time synchronization with one or multiple NTP servers. An audit is performed every 60 seconds.	Major
avAMMNodeCertificateFault	The system raises this alarm if the node certificate is about to expire, has expired or if the Avaya Multimedia Messaging application is unable to read the certificate file. The certificate audit is performed every 60 seconds.	Major
avAMMPPMConnectionLost	The system raises this alarm if the Avaya Multimedia Messaging application cannot connect to the PPM service on the Session Manager. This alarm is cleared if the connection is re-established.	Major
avAMMMSExchgConnectionLost	The system raises this alarm if the Avaya Multimedia Messaging application cannot connect to the Microsoft Exchange, either because the connection cannot be made or because the delegate account credentials are rejected. This alarm is cleared if the connection is re-established.	Major

Name	Description	Severity
avAMMMultiSiteConnectionLost	The system raises this alarm if the Avaya Multimedia Messaging application cannot connect to one or more remote sites in a multisite configuration. This alarm is cleared if the connection is re-established.	Major
avAMMUserLicensesUnavailable	The system raises this alarm when it automatically assigned all available rich media feature entitlements. The system no longer assigns automatically feature entitlements.	Major
avAMMUserLicensesThresholdReached	The system raises this alarm when it assigned 90% of available rich media feature entitlements.	Minor
avAMMCertificateAuthorityCertificateAlarmRaised	The system raises this alarm if the certificate authority certificate is about to expire, has expired or if the application is unable to read the certificate file. The certificate audit is performed every 60 seconds.	Major
avSIPAdapterContactLostAlarmRaised	The system raises this alarm if the Avaya Multimedia Messaging application cannot connect to either the Lync/Skype for Business server or the Session Manager. This is required for interoperability with Lync or Skype for Business.	Major

Preventing the creation of audit audispd logs on a physical server

About this task

Use this procedure to prevent the creation of audit audispd logs while installing Avaya Multimedia Messaging on a physical server. This procedure does not apply to OVA image installation.

For more information about audit log files, see https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/sec-Understanding_Audit_Log_Files.html.

Procedure

1. Open the `/etc/audisp/plugins.d/syslog.conf` file using a text editor and then replace the `LOG_INFO` text with `LOG_LOCAL0`.
2. Open the `/etc/syslog.conf` file, and in line number 42, add `local0.none` to the first part of the line as follows:

```
*.info;mail.none;authpriv.none;auth.none;cron.none;local0.none /var/log/messages
```

Logging trace-level messages on the Avaya Multimedia Messaging

About this task

This procedure describes how to log trace-level messages on the Avaya Multimedia Messaging server.

Procedure

1. Use the **tcpdump** command to collect the trace messages.

   For example:

   ```
   sudo tcpdump-XX -I eth0 >trace
   ```

   The **tcpdump** option must be installed manually. After you finish using **tcpdump**, uninstall it.

2. Use Wireshark to read the trace messages, by performing the following actions:

   a. Make a capture with the .pcap format.

   b. Run the **tcpdump** command:

      ```
      sudo tcpdump -ni eth0 -s0 -w trace.pcap
      ```

      The –w option writes the raw packet to a file with .pcapsupport for Wireshark reading

3. In the OAMP GUI, set the log level to `system`.

   For information about the level of detail captured in the log files, see *Administering Avaya Multimedia Messaging*.

Enhanced Access Security Gateway for real time support

Enabling the Enhanced Access Security Gateway after OVA deployment

About this task

Use this procedure to enable Enhanced Access Security Gateway (EASG) functionality in Avaya Multimedia Messaging. Avaya support engineers can use this functionality to access your computer and resolve product issues in real time.

The EASG is installed automatically when you deploy the Avaya Multimedia Messaging OVA on a VMware standalone host or on vCenter.

Procedure

1. Open the SSH console as an administrator.
2. Check the status of EASG by running the following command:

   ```
   EASGStatus
   ```

   By default, the EASG status is disabled.
3. To enable EASG, run the following command:

   ```
   sudo /usr/sbin/EASGManage --enableEASG
   ```
4. Run the following command to verify the product certificate:

   ```
   sudo EASGProductCert --certInfo
   ```

   The system displays the product certificate details.

   For example:

   ```
   [admin@amm-ova-test ~]$ EASGStatus
   EASG is disabled
   [admin@amm-ova-test ~]$ sudo /usr/sbin/EASGManage --enableEASG

   By enabling Avaya Services Logins you are granting Avaya access to
   your system.  This is required to maximize the performance and value
   of your Avaya support entitlements, allowing Avaya to resolve product
   issues in a timely manner.

   The product must be registered using the Avaya Global Registration
   Tool (GRT, see https://grt.avaya.com) to be eligible for Avaya remote
   connectivity.  Please see the Avaya support site (https://support.avaya.com/
   registration) for additional information for registering products and
   establishing remote access and alarming.

   Do you want to continue [yes/no]? yes

   EASG Access is enabled. Performed by user ID: 'admin', on Oct 19 2016 - 12:28
   [admin@amm-ova-test ~]$ EASGProductCert --certInfo
   Subject:        CN=                              , OU=EASG, O=Avaya Inc.
   Serial Number:  10005
   Expiration:     Aug  6 04:00:00 2031 GMT
   Trust Chain:
      1. O=Avaya, OU=IT, CN=AvayaITrootCA2
      2. DC=com, DC=avaya, DC=global, CN=AvayaITserverCA2
      3. O=Avaya Inc, OU=EASG, CN=EASG Intermediate CA
      4. CN=Product EASG Intermediate CA, OU=EASG, O=Avaya Inc.
      5. CN=                              .0, OU=EASG, O=Avaya Inc.
   [admin@amm-ova-test ~]$
   ```

   If the certificate expires within 360, 180, 30, or 0 days, the system logs a certificate expiry notification to the `/var/log/messages` file.

Installing and enabling the Enhanced Access Security Gateway on a physical server

About this task

The EASG is not installed automatically when you deploy Avaya Multimedia Messaging on a physical server. Use this procedure to install and enable the EASG on a physical server deployment. After you install and enable the EASG, Avaya support engineers can access your computer and resolve product issues in real time.

Procedure

1. Open the SSH console as an administrator.
2. To install EASG, run the following command:

   ```
   sudo /opt/Avaya/MultimediaMessaging/<version number>/CAS/<version number>/easg/
   easgInstall.sh
   ```

   The system installs the EASG `.rpm` file and creates the `susers` group if it is unavailable. It also adds the users to the `susers` and `ucgrp` groups.
3. Check the EASG status by running the following command:

   ```
   EASGStatus
   ```

   By default, the EASG status is disabled.
4. To enable EASG, run the following command:

   ```
   sudo /usr/sbin/EASGManage --enableEASG
   ```
5. To verify the product certificate, run the following command:

   ```
   sudo EASGProductCert --certInfo
   ```

   The system displays the product certificate details.

6. To complete the sshd_config setting, edit `/etc/ssh/sshd_config`, and then set ChallengeResponseAuthentication to `yes`.

```
login as: craft
This system is restricted solely to authorized users for legitimate business
purposes only. The actual or attempted unauthorized access, use, or
modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or
criminal and civil penalties under state, federal, or other applicable
domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and
security reasons. Anyone accessing this system expressly consents to such
monitoring and recording, and is advised that if it reveals possible evidence
of criminal activity, the evidence of such activity may be provided to law
enforcement officials. All users must comply with all corporate instructions
regarding the protection of information assets.

Using keyboard-interactive authentication.


Challenge: 10005-37279073              Product ID: 3548b37a63d84ecf8ee4c6ae5cce8
df001

Response:
```

7. To complete the Pluggable Authentication Module (PAM) settings for user authentication, do the following:
   a. In the PAM file stack, add `auth [success=done auth_err=bad default=ignore] pam_asg.so` so that it appears before `pam_unix.so`.
   b. In the password stack, add `password sufficient pam_asg.so` so that it appears in the first line.

      The following is an example of the PAM settings:

```
#%PAM-1.0
auth required pam_env.so
auth [success=done auth_err=bad default=ignore] pam_asg.so
auth sufficient pam_unix.so  try_first_pass
auth required pam_deny.so

account required pam_access.so

password sufficient pam_asg.so
password required pam_cracklib.so retry=3 minlen=6
password sufficient pam_unix.so use_authtok sha512 remember=4
password required pam_deny.so

session required pam_limits.so
```

Disabling EASG

Procedure

To disable EASG, run the following command:

```
sudo /usr/sbin/EASGManage --disableEASG
```

Removing EASG

About this task

Use this procedure to remove EASG permanently. You can use the OVA deployment process to reinstall EASG. With an Avaya Multimedia Messaging physical server deployment, you can use the installation directory path to reinstall EASG.

Procedure

In the SSH console, run the following command to remove EASG:

```
sudo /opt/Avaya/permanentEASGRemoval.sh
```

Chapter 9: External customization options

Install Adobe Flash Player for Message Playback

The Message Playback feature requires the presence of a Web browser with multimedia playing capabilities on the endpoint device that uses the feature.

The majority of the new Web browsers have an incorporated technology that enables multimedia playback without installing additional plugins.

Note:

Avaya applications that use the Message Playback feature require a manual installation of Adobe Flash Player on Microsoft Internet Explorer 8. You can download the plugin from the Adobe Flash Player website.

Do Not Disturb functionality for Avaya Aura® Presence Services

Avaya Multimedia Messaging and Avaya Aura® Presence Services support the following functionality with Avaya Equinox™ clients when your presence status is set to “Do Not Disturb”:

- The administrator can set a feature that delays the receipt of incoming instant messages. This feature is available if Avaya Aura® Presence Services Feature Pack 4 is the instant messaging provider and you set your presence status to “Do Not Disturb”. If the administrator sets the feature, you do not receive incoming instant messages while your presence is set to “Do Not Disturb”. Instead, when you change your presence status, these instant messages appear as missed conversations in the Avaya Equinox™ IM fan.
- With Avaya Multimedia Messaging, if the administrator sets the feature, you continue to receive incoming messages, but notifications are suppressed.
- With this feature, you can still begin a new instant messaging conversation and receive responses immediately while your presence is set to “Do Not Disturb”.

  The feature is unavailable with earlier versions of Avaya Aura® Presence Services. When the feature is unavailable, you continue to receive IMs regardless of your presence status.

For information about disabling the “Do Not Disturb” feature, see *Administering Avaya Aura® Presence Services*.

Disable file transfer from Avaya one-X® Communicator to Avaya Multimedia Messaging

Use Avaya one-X® Communicator file transfer in deployments where Avaya one-X® Communicator is the only client. In deployments with Avaya Multimedia Messaging, Avaya Equinox™, hard phones, or federated IM, Avaya one-X® Communicator file transfers have unpredictable results.

To disable file transfers from Avaya one-X® Communicator to the Avaya Multimedia Messaging server, see the Avaya one-X® Communicator documentation.

Disable instant messaging for 96x1 SIP desk phones

Avaya Multimedia Messaging does not support IM on 96x1 SIP deskphones. You can use the IM functionality on 96x1 SIP deskphones with Avaya one-X® Communicator.

To disable the IM functionality for the 96x1 SIP phones, see the *Administering Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP* document.

Configure Avaya Equinox™ for iPad to use the IM capabilities

You can configure Avaya Equinox™ for iOS and Windows to use the Instant Messaging capabilities of either Presence Services or Avaya Multimedia Messaging.

- You can configure Avaya Equinox™ for iOS and Windows for only Presence Services messaging when you do not have Avaya Multimedia Messaging deployed in the solution.
- You must configure Avaya Equinox™ for iOS and Windows to use Avaya Multimedia Messaging for messaging when you deploy Avaya Multimedia Messaging in the solution, even if Presence Services continues to provide messaging for other endpoints.

If you have configured Avaya Equinox™ for iOS and Windows clients for Presence Services messaging, you must reconfigure to use Avaya Multimedia Messaging for messaging. Presence Services continues to provide Self and Buddy Presence for Avaya Equinox™ for iOS and Windows clients after you reconfigure Avaya Multimedia Messaging for instant messaging.

Customizing the Login screen message for Message Playback

About this task

The login screen of the Message Playback component displays login instructions for the users who want to view or retrieve the multimedia attachments.

The default text for the instructions is: `Enter your GLOBAL handle in the Username field.` in English and in any other languages supported for localization.

You can customize the instructions during the post-installation configuration phase and update the instructions at any time.

Procedure

1. Log on to the Avaya Multimedia Messaging server using the non-root user.
2. Run the **`su`** command to log in as the root user.
3. Open the `/var/www/configuration/login-admin.properties` file using a text editor.
4. Update the login instructions text for every supported language.

   The `value` attribute contains the instructions text.

For example:

```
 {"key":"_EnterGlobalHandle_",
"lang":"en-en",
 "value":"Enter customized login instructions text here",
"description":"Login field details"}
```

5. Save the login-admin.properties file and restart the browser on the client machine to view the updated login instructions.

Chapter 10: Backup and restore

Avaya Multimedia Messaging provides the possibility of backing up the data on the servers, in standalone as well as clustered environments.

In case of a system malfunction where one or more Avaya Multimedia Messaging servers must be reinstalled and reconfigured, you can restore the database and the multimedia files that are present on the servers when you made the backup.

Important:

The backup and restore procedures are the same, regardless of the deployment method. The same procedures apply for deployments made on physical servers, as well as deployments in VMware virtual machines.

If the restore involves the deployment of the current Release 3.2 OVA, the system will be on partitioning version 2.0.

Warning:

- The restore operation must be performed on the same Avaya Multimedia Messaging build version from which the backup was made.
- Patches can cause changes to the format and content of the data that is stored when a backup is taken. Before you restore data, patch the build to the same patch level that the build was on at the time that the backup was taken.

The backup procedure of a server requires significant resources, so you must not perform the backup during busy periods.

You can perform the backup by a running a script located in the Avaya Multimedia Messaging installation directory. On an Avaya Multimedia Messaging server, the backup script performs the following operations:

- Takes a snapshot of the Cassandra database
- Copies the Cassandra snapshot files and the configuration data to the backup storage device
- Copies the media files to the backup storage device

In an Avaya Multimedia Messaging cluster, you must run the backup script on every node for database and configuration file backup and copy the media files only from the seed node.

Note:

The media files require a large amount of disk space, so you must ensure that the backup storage device has enough disk space for all the Avaya Multimedia Messaging files. The backup storage device can be an external hard drive or a Storage Area Network (SAN) mounted to a local directory on the Avaya Multimedia Messaging server.

The transfer speed depends on the hardware platform used as a backup storage device. For example:

For a 1 Terabyte media store of approximately 100,000 10 Megabyte clips and an effective disk transfer rate of 100 MB/sec, 10,000 seconds are required for the media copy step. Hardware platforms with higher speed interconnects can reduce the backup time.

Important:

The firewall configuration is not restored automatically. Before restoring an Avaya Multimedia Messaging node, you must perform the firewall configuration as part of the installation process.

Making a backup for an Avaya Multimedia Messaging node

About this task

The following procedure describes how to make a backup of the database, configuration, and multimedia files present on an Avaya Multimedia Messaging node.

Before you begin

Ensure that:

- The non-root user who performs installation and administration tasks has sudo permissions.
- SSH access is configured through all the nodes in the cluster, when backing up a cluster.

  You can configure SSH access by running the Avaya Multimedia Messaging configuration utility and selecting **Cluster Configuration** > **Configure SSH RSA Public/Private Keys**.
- You have the Cassandra database user name and password. You will require this information if you are backing up database content.
- The backup directory and all parent directories must be executable, using the `x` command, by the application ID.

Procedure

1. Log in to the Avaya Multimedia Messaging CLI as the non-root user with sudo privileges.
2. Run the backup script.

   For example:

   ```
   /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/bin/backupAMM.sh -t -d /media/data/backup
   ```

   `-t` in this command enables a backup to a single `.tar` file, which facilitates copying the file. A tarred backup can be directly restored without undoing the tarring.

   If you do not provide a backup name, the backup name is generated automatically as a combination of the host name and the date and timestamp.
3. To back up media, type `yes` when you are prompted with the question `Do you want to include media files in the backup?`

If you do not back up your media files, you cannot restore media. You do not need to back up media on all nodes in a cluster. Cassandra data is different on each node, but media is the same.

Backup command options

The script that performs the Avaya Multimedia Messaging server backup is located in the Avaya Multimedia Messaging installation directory. For example: if the installation directory is `/opt/Avaya`, the path to the backup script is `/opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/bin/backupAMM.sh`.

When you run the Avaya Multimedia Messaging backup script, you can use the following options:

Option	Description
-d	Sets the parent directory where the backup files are stored.
-t	Creates the backup as a .tar file, not a directory.
-R	Removes all the existing Cassandra snapshots.
-h	Prints usage options for the backupAMM.sh script.
-C	Excludes configuration files from the backup.
-c	Excludes database files from the backup.
-m	Copies only the media files.
-n	Copies only the database and configuration files.
-v	Displays a verbose output for debugging.

Restoring Avaya Multimedia Messaging

Restoring an Avaya Multimedia Messaging node in a standalone deployment

About this task

The following procedure describes how to restore an Avaya Multimedia Messaging node in a standalone configuration.

Before you begin

Before you begin restoring an Avaya Multimedia Messaging server, you must first perform the Avaya Multimedia Messaging installation, while ensuring that all the prerequisites are present on the system.

Procedure

1. Run the Avaya Multimedia Messaging server installation command.

   For example:

   ```
   sudo /opt/Avaya/amm-<version>.bin
   ```

2. On the Initial Installation Configuration screen, in the Advanced Configuration area, set **Gluster Configuration** to `y` (yes) and **Enable Cassandra DB initialization** to `n` (no).
3. Proceed with the Avaya Multimedia Messaging installation.

   Note:

   Configuring the Avaya Multimedia Messaging server is not mandatory in this case. You can run the configuration utility at a later time. Please note, however, that firewall configuration is mandatory and is not restored automatically.

4. Change the ownership of the backup file to `<admin_user:admin_grp>` by running the following command:

   ```
   sudo chown -R ucapp:ucgrp <full_path_to_backup_tar_file>
   ```

5. Run the **`restoreAMM`** command with the path to the restore file or directory as a parameter.

   For example:

   ```
   $ sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/bin/restoreAMM.sh
   /home/avaya/backup/backup2014_02_02_ammhost1
   ```

6. When the script prompts you to restore the media files, enter `y` (yes).

   The script restores the Cassandra database files, the media files, and the Avaya Multimedia Messaging configuration settings.

7. Start the Avaya Multimedia Messaging server.

   ```
   service AMMService start
   ```

Restoring a node from a cluster

About this task

This procedure describes how to restore an Avaya Multimedia Messaging node in a standalone configuration.

Before you begin

Before you begin restoring an Avaya Multimedia Messaging server, you must first install the Avaya Multimedia Messaging, while ensuring that all the prerequisites are present on the system.

Procedure

1. Run the Avaya Multimedia Messaging server installation command.

For example:

```
sudo /opt/Avaya/amm-<version>.bin
```

2. In the **General Configuration** menu, configure the following settings to `n` (no):
   - **Configure Gluster**
   - **Enable Cassandra DB initialization**
3. Proceed with the Avaya Multimedia Messaging installation.

   Note:

   Configuring the Avaya Multimedia Messaging server is not mandatory in this case. You can run the configuration utility at a later time.
4. Change the ownership of the backup file to `<admin_user:admin_grp>` by running the following command:

   ```
   sudo chown -R ucapp:ucgrp <full_path_to_backup_tar_file>
   ```
5. Run the **`restoreAMM`** command with the path to the restore file or directory as a parameter.

   For example:

   ```
   sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/bin/restoreAMM.sh
   /home/avaya/backup/backup2014_02_02_ammhost1
   ```
6. When the script prompts you to restore the media files, enter `n` (no).

   The media files must be restored using the Gluster recovery procedure.
7. Restore the Gluster file system.

   The procedure that you must use varies depending on the situation. The key situations are:
   - Restoring a single-node system or an entire cluster.
   - Repairing a single node.
8. From another node in the cluster, set up the SSH RSA public/private keys by running the **`configureAMM.sh`** script.
9. Run the Cassandra repair command:

   ```
   /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/cassandra/
   cassandraRepair.sh -M
   ```

Next steps

Reestablish the alarm connection to System Manager.

Restoring a cluster

About this task

The cluster restoring tasks that you can perform for the Avaya Multimedia Messaging server are:

- Restore a standalone node when a single node in the Avaya Multimedia Messaging cluster is not functional.
- Restore a cluster.

To restore an Avaya Multimedia Messaging node, you must install the Avaya Multimedia Messaging software, then restore the configuration and data files from a previously made backup.

The following procedure describes how to restore an Avaya Multimedia Messaging a cluster in case of a failure that results in the loss of all the nodes.

You must perform this procedure for each node in the cluster.

Important:

If multiple nodes from a cluster are recovered, you must first restart the Openfire server before restarting the Avaya Multimedia Messaging service.

Before you begin

Before you begin restoring a node from the Avaya Multimedia Messaging cluster, you must ensure that all the prerequisites are present on the system.

Procedure

1. Run the Avaya Multimedia Messaging server installation command.

   For example:

   ```
   sudo /opt/Avaya/amm-<version>.bin
   ```

2. In the **Advanced Configuration** menu, configure the following settings:
   - **Configure Gluster**:
     - set to `y` (yes) for the first node of the cluster.
   - **Enable Cassandra DB initialization**: set to `n` (no).
3. Proceed with the Avaya Multimedia Messaging installation.

   Note:

   Configuring the Avaya Multimedia Messaging server is not mandatory in this case. You can run the configuration utility at a later time.

4. If you are installing an additional node, configure the Gluster file system.

   Additional information about installing additional nodes is available in *Deploying Avaya Multimedia Messaging*.

5. From another node in the cluster, set up the SSH RSA public/private keys by running the **`configureAMM.sh`** script.

6. Run the **restoreAMM** command on every node, with the path to the restore file or directory as a parameter.

   For example:

   ```
   sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/bin/restoreAMM.sh
   /home/avaya/backup/backup2014_02_02_ammhost1
   ```

7. When the script prompts you to restore the media files, enter `n` (no).

   Note:

   You must enter `y` (yes) for restoring the media files only in the seed node of the cluster and no on all the other nodes.

8. Restore the Gluster file system.

   The procedure that you must use varies depending on the situation. The key situations are:

   - Restoring a single-node system or an entire cluster.
   - Repairing a single node.

9. On the last node that you are restoring, restart the Openfire server if Avaya Multimedia Messaging is federated with Presence Services.

   ```
   sudo service AMMOpenfire restart
   ```

   Warning:

   Restart the Openfire server only after restoring the other nodes in the cluster.

10. After all the nodes have been restored, start the Avaya Multimedia Messaging server.

    ```
    service AMMService start
    ```

11. Run the Cassandra repair command:

    ```
    /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/cassandra/
    cassandraRepair.sh -M
    ```

Next steps

Reestablish the alarm connection to System Manager.

Restoring Gluster on a single-node system or for an entire cluster

Procedure

1. Install Avaya Multimedia Messaging on each node.
2. Create an empty `cs_volume` directory as described in *Deploying Avaya Multimedia Messaging*.
3. Restore media files from the backup on one node.

   You do not need to back up media on all nodes in a cluster. Cassandra data is different on each node, but media is the same.

Repairing Gluster after replacing a node

About this task

Every node in a cluster hosts two Gluster file system (GlusterFS) bricks. Use this procedure to restore these bricks after replacing a node.

Procedure

1. Install Avaya Multimedia Messaging on the new node.

   For more information about installation, see *Deploying Avaya Multimedia Messaging*.

   Important:

   Do not configure GlusterFS during the installation.

2. Integrate the new node into the cluster.

   The new node has the same IP address and FQDN as the node that it is replacing. GlusterFS assigns a Universally Unique Identifier (UUID) to every node during installation. You must ensure that the UUID does not change.

   a. From another node in the cluster, use `sudo gluster pool list` to discover the old UUID.

      In this example, if `amm1` is the node being replaced, then the UUID is `30640f4c-23d4-49bc-8915-ad81e0949984`.

      ```
      UUID                    Hostname                State
      30640f4c-23d4-49bc-89   amm1.example.com        Connected
      15-ad81e0949984
      4cad28fd-               localhost               Connected
      e626-4dae-8c09-70be1f
      53895e
      ```

   b. From the new node, edit `/var/lib/glusterd/glusterd.info` so that the UUID is the same.

      ```
      UUID=30640f4c-23d4-49bc-8915-ad81e0949984
      operating-version=31000
      ```

   c. Restart GlusterFS.

      ```
      sudo service glusterd restart
      ```

   d. Reacquaint the new node with each of the other nodes in the cluster using the following command:

      ```
      sudo gluster peer probe <ip>
      ```

      For example, if the cluster consists of nodes with IP addresses 10.10.10.1 and 10.10.10.2, with the former being the new node, then from 10.10.10.1, issue the following command:

      ```
      sudo gluster peer probe 10.10.10.2
      ```

3. Rebuild the bricks on the new node.

   The bricks from the new node are reconstituted from another copy on other nodes in the background. Explicitly restoring from the backup is not necessary. The following is an example from the new node:

```
BRICKDIR=<newip>:/media/data/content_store
sudo gluster volume reset-brick cs_volume $BRICKDIR/brick0 start
sudo gluster volume reset-brick cs_volume $BRICKDIR/brick1 start
sudo install -d -o ucapp -g ucgrp -m 700 /media/data/content_store/brick0 /media/
data/content_store/brick1
sudo gluster volume reset-brick cs_volume $BRICKDIR/brick0 $BRICKDIR/brick0 commit
sudo gluster volume reset-brick cs_volume $BRICKDIR/brick1 $BRICKDIR/brick1 commit
```

Archiving

About this task

The following procedure describes how to search for user conversations in an Avaya Multimedia Messaging database that is already present on the system after restoring.

For more information about writing select statements in the Cassandra Query Language (CQL), see the Cassandra documentation.

Before you begin

To prevent disk space exhaustion, user conversations that are older than a configured number of days are automatically removed.

To preserve the conversations for long-term usage, you must perform a backup of the Avaya Multimedia Messaging server periodically.For more information about backups, see Backup and restore on page 64.

To search for user conversations that are older and are no longer present on the Avaya Multimedia Messaging server, you must first restore the Avaya Multimedia Messaging configuration that was present on the system in the time period of interest. After restring the Avaya Multimedia Messaging configuration, you must perform searches in the database to find the conversations.

Procedure

1. In the Avaya Multimedia Messaging server CLI, type the following command to start the Cassandra query tool:

```
/opt/Avaya/MultimediaMessaging/<version>/cassandra/1.2.7/bin/cqlsh -u <uname> -p
<passwd>
```

2. In the CQL console, select the AMM_Data keyspace.

```
use AMM_Data;
```

3. Run Cassandra queries for the user ID and other attributes of interest.

For example:

- To retrieve the conversations of a user based on the user ID, run a command similar to the following:

```
select * from conv_metadata_by_entityid where
entityid='amm_user@avaya.com&contact';
```

- To retrieve a conversation from the list returned by the previous query, run a command similar to the following:

```
select * from messages where conversationid='fe7a4904-5e13-4fb3-
adc5-58546002c584';
```

- To also limit the results based on the timestamp, run a command similar to the following:

```
select * from messages where conversationid='fe7a4904-5e13-4fb3-
adc5-58546002c584' and timestamp>'2014-06-24' and timestamp<'2014-06-25' allow
filtering;
```

  The `allow filtering` statement is required if CQL must perform slower operations such as comparisons.

- To limit the number of fields displayed in the result, include the fields of interest in the select statement:

```
select messageid, body, subject from messages where
conversationid='fe7a4904-5e13-4fb3-adc5-58546002c584' and timestamp>'2014-06-24'
and timestamp<'2014-06-25' and subject='' allow filtering;
```

  This statement only returns the message ID, message body, and subject in the result.

- To retrieve the conversations that have a particular property, you must first index the column:

```
CREATE INDEX ON messages(subject) ;
select messageid, body, subject from messages where
conversationid='fe7a4904-5e13-4fb3-adc5-58546002c584' and timestamp>'2014-06-24'
and timestamp<'2014-06-25' and subject='subject1' allow filtering;
```

  Warning:

  Operations that require indexing must not be performed on a running system, because these operations affect performance.

- To view the participants in a message, include the `fromaddr` and the `toaddr` fields in the select statement:

```
h:amm_data> select messageid, body, subject, fromaddr, toaddr from messages
where conversationid='fe7a4904-5e13-4fb3-adc5-58546002c584' and
timestamp>'2014-06-24' and timestamp<'2014-06-25' and subject='subject1' allow
filtering;
```

4. To exit the CQL tool, run the following command:

```
quit;
```

Lync or Skype for Business recovery

The Microsoft Lync or Skype for Business client, which is also referred to as the “Microsoft client”, periodically refreshes its SIP dialogs with the server. If the refresh fails, the client tries twice to re-establish its dialogs before giving up. The client also attempts to re-establish a failed dialog when sending a message. The server never tries to re-establish connections with a client. The following cases describe the recovery of Lync or Skype for Business sessions after an Avaya Multimedia Messaging host node fails.

Scenario	Description
The Microsoft client reconnects to an Avaya Multimedia Messaging focused conference	The client performs its regular recovery protocol. Avaya Multimedia Messaging reconnects and provides the current view of the participants.
Avaya Multimedia Messaging server reconnects to a Microsoft client from an Avaya Multimedia Messaging focused conference	You cannot bring a disconnected client back into a conference from the server side. The server can only process an invitation to a new conference. In this case, Avaya Multimedia Messaging must change the conference ID used with Lync or Skype for Business after a recovery. The client will display a new window for the recovered conversation. The old window remains, but is no longer usable.
Avaya Multimedia Messaging server reconnects to a Microsoft focused conference	Avaya Multimedia Messaging functions as a Microsoft client. The Lync or Skype for Business server accepts the Avaya Multimedia Messaging initiated session re-establishment. Avaya Multimedia Messaging must perform an audit between the Microsoft client and Avaya Multimedia Messaging view of the conversation. Additions and deletions on each side must be reflected to the other. Handling deletions requires an explicit audit. Reflecting an Avaya Multimedia Messaging deletion on the Microsoft client requires re-establishing the connection for the deleted Avaya Multimedia Messaging party and then immediately closing it.
Lync or Skype for Business server reconnects to Avaya Multimedia Messaging from a Microsoft focused conference	The Lync or Skype for Business server does not try to reconnect to Avaya Multimedia Messaging. However, in some cases, messages from the Lync or Skype for Business server reach an Avaya Multimedia Messaging node after the node fails and recovers. This situation occurs when node recovery is quick and the SIP dialogs remain intact within Session Manager, and the SIP relay or the Lync or Skype for Business edge server. When Avaya Multimedia Messaging detects such messages, it might initiate the recovery for the Avaya Multimedia Messaging side.

Chapter 11: Upgrades and migrations

Migrations are done from Release 2.x to Release 3.0, and then Avaya Multimedia Messaging must be upgraded to the latest 3.2 release. If you need to migrate to Release 3.0, see “Avaya Multimedia Messaging migration” in the Release 3.0.x version of *Deploying Avaya Multimedia Messaging* at https://downloads.avaya.com/css/P8/documents/101033390. The operating system is also changed as part of the process to migrate to Release 3.0.

Note:

- When performing an upgrade, you can roll back to the previously installed Avaya Multimedia Messaging version.
- The rollback feature is not supported for migrations. Instead, you must take a backup and use it to restore data.

Latest software updates and patch information

Before you start the deployment or upgrade of an Avaya product or solution, download the latest software updates or patches for the product or solution. For more information, see the latest release notes, Product Support Notices (PSN), and Product Correction Notices (PCN) for the product or solution on the Avaya Support Web site at https://support.avaya.com/.

After deploying or upgrading a product or solution, use the instructions in the release notes, PSNs, or PCNs to install any required software updates or patches.

For third-party products used with an Avaya product or solution, see the latest release notes for the third-party products to determine if you need to download and install any updates or patches.

Upgrading the Avaya Multimedia Messaging server

About this task

Upgrading to the current release requires you to upgrade both the system layer and the application layer.

This procedure describes how to perform an upgrade of the Avaya Multimedia Messaging server on one node. You must perform this procedure on every individual cluster node, one node at a time. This procedure is valid for physical server and virtual machine deployments.

Note:

- In a cluster, all the nodes must run the same Avaya Multimedia Messaging version. All the nodes must be upgraded before the Avaya Multimedia Messaging service starts on the nodes.
- In a standalone deployment, if the Avaya Multimedia Messaging service runs at the start of the upgrade, the Avaya Multimedia Messaging service becomes unavailable until the upgrade is complete.
- You must start the upgrade with the seed node, which is the virtual IP master.
- In a cluster, you must finish the upgrading procedures on one node, before moving on to another.

Before you begin

Before upgrading the Avaya Multimedia Messaging server, you must perform a number of verifications. These verifications are required regardless of the deployment model. In a single-node deployment, make the verifications on the Avaya Multimedia Messaging server. In a cluster, make the verifications on every node in the cluster.

- Ensure that Cassandra database server and all other Avaya Multimedia Messaging services are running.
- Ensure that the SSH configuration process is finished.
- Ensure that you can connect to all the nodes through SSH.
- Ensure that NTP is configured and synchronized on all nodes.
- Ensure that the nodes have enough disk space available.
- Ensure that debug logs are disabled in the Avaya Multimedia Messaging administration portal.
- Log in to the Avaya Multimedia Messaging administration portal and ensure that the nodes are functioning without issues.

Important:

Make a backup of the log files before starting the upgrade. The upgraded Avaya Multimedia Messaging will use new log files and the old files are lost.

Procedure

1. Upgrade the system layer.

   `ucapp-system-3.2.0.0.9.tgz` is an example of a system later upgrade artifact.

2. Make the required adjustments to the partitioning 1.0 volumes.

   a. Confirm that the system is on partitioning version 1.0 using the `sys versions` command.

   b. If the size of the `/opt/Avaya` volume is currently less than 95.0 GiB, then increase it so that the new size is 95.0 GiB.

      For information about disk volume specifications for the partitioning versions, see *Avaya Multimedia Messaging Reference Configuration*.

3. Upgrade the application layer.
   a. On the Avaya Multimedia Messaging node, download or copy the latest binary build.
   b. Run the installer of the latest build, as if you are performing a new installation.

      Additional information about running the installer is available in *Deploying Avaya Multimedia Messaging*.
   c. When the system prompts you to confirm that you want to perform an upgrade, select **Yes** and press `Enter` to start the upgrade.
4. **(Optional)** To remove the previous Avaya Multimedia Messaging version after an upgrade, run the following command:

   ```
   sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/uninstaller/
   removeVersion.sh
   ```
5. After you finish upgrading all the nodes, start the Avaya Multimedia Messaging service on every node:

   ```
   service AMMService start
   ```

Rollback operations

When performing an upgrade, you can roll back to the previously installed Avaya Multimedia Messaging version. To make the rollback feature possible, the previous Avaya Multimedia Messaging build is not removed by an upgrade.

When you perform an upgrade of the Avaya Multimedia Messaging server, the new version is installed in a duplicate directory and the configurations and database schema are copied from the previous installed version.

You can restore a previous Avaya Multimedia Messaging version under the following conditions:

- The rollback operation can only be applied to the latest installed version of the Avaya Multimedia Messaging server.
- The previous Avaya Multimedia Messaging version must still be present on the server.
- The rollback operation can only be applied once.
- The rollback operation cannot be performed on the initial Avaya Multimedia Messaging version installed.
- In a cluster, the rollback operation must be performed on every node before the nodes are started.

Warning:

If you restore a previously installed Avaya Multimedia Messaging version, you will lose the conversations sent since the last backup.

Restoring a previous version of the Avaya Multimedia Messaging server

About this task

The following procedure describes how to reverse an upgrade to an earlier version of the Avaya Multimedia Messaging server. Some steps are applicable to Avaya Multimedia Messaging clusters.

Note:

The AMMService process can run at the beginning of the restore operation. The service becomes unavailable during the restore.

Before you begin

Before you perform the rollback operation, ensure that the Cassandra database server is running and trace logging is stopped. In a cluster, the Cassandra database server must run on all the nodes.

Procedure

1. In the Avaya Multimedia Messaging CLI, run the following command:

   ```
   sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/uninstaller/
   rollbackAMM.sh
   ```

2. In an Avaya Multimedia Messaging cluster, run the same command on every node to roll back to the previous version.
3. After the rollback operation ends on every node of the cluster, run the following command to start the Avaya Multimedia Messaging service:

   ```
   service AMMService start
   ```

4. (Optional) Run the following command to remove the latest Avaya Multimedia Messaging version, which remains on the server but is inactive:

   ```
   sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/uninstaller/
   removeVersion.sh
   ```

Migration of the Avaya Aura® environment

For a fresh installation of Avaya Multimedia Messaging with the latest Avaya Aura® Release 7.x environment, perform the standard installation and configuration. As part of the configuration, you must set up the Data Replication Service (DRS) for System Manager and the HTTPS REST Presence adapter.

When you are migrating Avaya Multimedia Messaging, the Avaya Aura® environment must also be upgraded. You must migrate Avaya Multimedia Messaging first and then migrate the Avaya Aura® environment. You must also configure Avaya Multimedia Messaging to work with the new Avaya Aura® environment.

See the following documents for more information on migrating:

- Avaya Aura® environment: *Upgrading and Migrating Avaya Aura® applications from System Manager*.
- Avaya Aura® Presence Services: *Avaya Aura® Presence Services Snap-in Reference*.

Migrating the Data Replication Service

Before you begin

Complete the Avaya Multimedia Messaging update.

Procedure

1. Open a SSH session to the designated Avaya Multimedia Messaging server and log in as an administrator.
2. Launch the Avaya Multimedia Messaging configuration tool using the following command:

   ```
   sudo /opt/Avaya/MultimediaMessaging/< 3.0.0. version>/CAS/< 3.0.0 version>/bin/configureAMM.sh
   ```
3. Select **Front-end host, System Manager and Certificate Configuration**.
4. Select **System Manager Version**.
5. To upgrade to the System Manager 7 DRS, select **Version 7.x** > **OK**.
6. **(Optional)** To set the System Manager FQDN to point to version 7.x, type the address and then select **OK**.
7. Select the System Manager Enrollment password and enter the password that is configured in the System Manager.
8. Enter a new password for the keystore that holds the certificates configured with the System Manager.
9. To apply the setting, select **Apply**.

Presence Services federation migration

Use the following procedures to migrate the Presence Services federation from an XMPP-based to a REST-based environment. You must copy the configuration for the XMPP adapter to the REST adapter.

Adding the Presence Services trust certificate to the Avaya Multimedia Messaging truststore

Procedure

1. Obtain the Presence Services Presence Services Certificate Authority.

   You can usually download this certificate from System Manager.

2. Copy the certificate file onto the Avaya Multimedia Messaging server using a file transfer mechanism, such as SCP.

   Important:

   Make sure the Presence Services certificate is correct and contains all the data for the server to identify itself.

3. Put the file in an accessible directory, such as `/tmp` or `/opt/Avaya`.
4. Start the Avaya Multimedia Messaging Configuration tool by running the following command:

   ```
   sudo /opt/Avaya/MultimediaMessaging/<3.0.0 version>/CAS/<3.0.0 version>/bin/
   configureAMM.sh
   ```

5. From the **Advanced Configuration** menu, select **Import PSNG Trusted Certificate**.
6. Enter the path to the certificate file and Select **OK** to apply the change.
7. Exit the Configuration tool.

Replacing the Avaya Multimedia Messaging XMPP adaptor configuration with the HTTPS REST configuration

Procedure

1. Log in to the Avaya Multimedia Messaging administration portal.

   The URL for gaining access to the administration portal is `https://<hostname>:8445/admin`.

   Important:

   For the hostname, always use the same Avaya Multimedia Messaging server FQDN that you use for generating certificates. You will be redirected to the Login page if you use the IP address instead of the FQDN.

   To gain access to the web-based administration portal, you must use an account that has the Administrator role defined in the LDAP server configuration.

2. In the left panel, select **Server Connections** > **Federation Configuration**.
3. Open the XMPP Adaptor page.
4. Note the following:
   - The values in the **Routing Domain**, **Remote Domains**, and **Timeout** fields.
   - Whether the **Send Presence Ping** check box is selected.
5. Disable the adaptor. .
   a. Select the **Adapter Enabled** check box.
   b. Click **Save**.

   The application restarts.
6. Go back to the Federation Configuration page.

7. In **HTTPS REST to Avaya Presence Services Connection Adaptors**, click **Add**.
8. In the new Adaptor page, do the following:
   a. Select the **XEP-0033** protocol.

      Note:

      Only the XEP-0033 protocol is supported.

   b. Select the **Adaptor Enabled** check box.
   c. Enter the previously noted and new values in the corresponding fields for **HTTPS REST to Avaya Presence Services Connection Adaptors**.

      Additional details on configuration of HTTPS REST adaptor are available in *Deploying Avaya Multimedia Messaging*.

   d. **(Optional)** In the **Port** field, update the port number.

      The default port is 443. The port you enter must correspond with the Presence Services configuration.

Note:

If the value for Remote Domains is already in use by an existing XMPP Adaptor, you might not be able to save. In this case, go back and delete the value in the existing XMPP Adaptor and then create the HTTP Adaptor.

9. Ensure that the HTTPS adaptor is enabled and save the new configuration.

   The application restarts.

Checking for DRS synchronization after a migration or upgrade

About this task

Avaya Multimedia Messaging can take 5 to 30 minutes to sync after an installation, upgrade, or migration. Messaging might fail if the DRS is not in sync. Use this procedure to check if the DRS is synchronized.

Procedure

1. In System Manager, navigate to **Services** > **Replication**.
2. Select the replication group.
3. Search for the Avaya Multimedia Messaging nodes and check if they are listed as “Synchronized”.

Chapter 12: System layer (OS) updates on VMware virtual machines

Each VMware virtual machine that is created by deploying the Avaya Multimedia Messaging OVA file has a system layer (operating system). The system later is updated with system layer updates provided by Avaya.

Important:

Do not apply updates obtained from sources other than Avaya to the system layer of Avaya Multimedia Messaging VMware virtual machines. Only use update artifacts provided by Avaya.

Note:

This section only applies to VMware virtual machines. Customers are responsible for updating the operating system when Avaya Multimedia Messaging is installed onto physical servers, using update artifacts from Red Hat.

The process to install a system layer update involves the following steps:

- Determine if the system layer update is applicable to the given virtual machine. If the update is not applicable, then there is no action required.
- Download, extract, and stage the update.
- Install the update during a maintenance window.

Determining if a system update is applicable

About this task

Before installing a system update for a virtual machine, query the version of the currently installed system. Use the current version to determine if the system layer requires an update. It is possible that the machine was installed using an OVA that was already built with the latest system layer version.

Procedure

1. Log in to the virtual machine using the administrative user id.
2. Query the version number of the system version by running the `sys versions` command.

Note:

The patch level reported by the above command is not used at this time, and is to be ignored.

Next steps

If the above system version is already on the recommended system update, then no further action is required.

If the above system version is lower than the recommended system update version, then continue with the process to download and stage the update.

Downloading, extracting, and staging a system layer update

About this task

Before installing a system layer update, you must first download the update from the Avaya support site, and then extract and stage the update on the system. The staging process places the update into a system area, which prepares the system for installation of the update.

Procedure

1. Download the update from the Avaya Support web site.
2. Transfer the update to the admin account of the server to be updated, using standard file transfer methods, such as SFTP or SCP.
3. Log in to the admin account of the server using SSH
4. To extract the update, use the following command:

   ```
   tar -zxf ucapp-system-3.2.0.0.9.tgz
   ```

5. To stage the update, change to the required directory and perform the following staging command:

   ```
   cd ucapp-system-3.2.0.0.9
   sudo ./update.sh --stage
   ```

6. (Optional) To free up disk space, clean up the downloaded and extracted files using the following commands:

   ```
   cd..
   rm ucapp-system-3.2.0.0.9.tgz
   rm -rf ucapp-system-3.2.0.0.9
   ```

   Tip:

   It is recommended to clean up the downloaded and extracted artifacts after staging. The staging operation copies the content to an internal system area. The downloaded and extracted content are no longer required.

7. To verify that the update has been staged, query the status:

```
sysUpdate --status
```

Note:

The **sysUpdate** command is added to the system the first time a system update is staged. After staging, if the command is not recognized, you must exit the current session and establish a new session. Establishing a new session creates the **sysUpdate** command (alias) for the new session.

Tip:

If a system update is staged in error, the staged update can be deleted as follows. It is not possible to delete a staged update once the installation of the update has started.

```
sysUpdate --delete
```

For additional help with the **sysUpdate** command, use one of the following commands. The **--help** option provides command line syntax. The **--hhelp** option provides verbose help.

```
sysUpdate --help
sysUpdate --hhelp
```

Next steps

Install the staged update during a maintenance window.

Installing a staged system layer update

About this task

After a system update is staged, it can then be installed. The installation runs in the background in order to minimize the possibility of interference, such as the loss of an SSH session. The background installation process follows these steps:

- A login warning message is created so users logging into the system know that a system update is in progress.
- If the application is running, it is shut down.
- The update is installed onto the system.
- The server is rebooted.
- Post-reboot cleanup actions are performed.
- The application is started.
- The login warning message is removed.

Important:

Do not perform any system maintenance actions, such as starting, stopping, or upgrading the application, while the system update is in progress.

Procedure

1. Log in to the administrative account using SSH.
2. Type `sysUpdate --install` to start the installation

Tip:

The progress of the update can be monitored using one of the following commands. The first command uses the Linux tail browser, whereas the second uses the Linux less browser.

```
sysUpdate --monitor
sysUpdate --monitor less
```

The status of the update can be queried using the command:

```
sysUpdate --status
```

You can obtain logs of the current, and previous, system layer update installations, by using the following command. This command places a zip file of the logs in the current working directory.

```
sysUpdate --logs
```

Chapter 13: Troubleshooting

Troubleshooting best practices for IWA

Try the following solutions if you experience problems with IWA.

Solution

- To enable Kerberos debugging, add the following line in the `AMMTomcat` file, under `etc/init.d`, after the `CATALINA_OPTS` lines:

```
CATALINA_OPTS="$CATALINA_OPTS -Dsun.security.krb5.debug=true"
```

- To enable authentication debugging in Tomcat, add the following line in the `log4j.properties` file, under `/opt/Avaya/MultimediaMessaging/<version>/tomcat/8.0.24/lib`, after the `CATALINA_OPTS` lines:

```
log4j.logger.org.apache.catalina.authenticator=DEBUG,CATALINA
```

- If you encounter a `checksum failed` error log on the server and the SPN was modified, try logging out the domain account that is trying to access the server as it may have cached an incorrect ticket or token.

Cannot log in to the web-based administration portal using Internet Explorer 10

Condition

When using the SSO cut-through link with Internet Explorer 10, you are not logged in to the web-based administration portal. You are still prompted to enter credentials.

Solution

1. From Internet Explorer, click **Tools** > **Internet options** > **Settings**.
2. Do one of the following:
   - Select **Enable Protected Mode**.
   - Add the server URL to the Local Intranet sites list.

Networking issues after upgrading

Condition

After upgrading, cloning, or changing the host of the Avaya Multimedia Messaging server, you may experience networking issues.

Solution

1. In the Avaya Multimedia Messaging CLI, run the following command to remove the persistent rules:

   ```
   sudo rm -f /etc/udev/rules.d/70-persistent-net.rules
   ```

2. Check and change the MAC address (HWADDR) of the network interface accordingly.

   ```
   sudo vi  /etc/sysconfig/network-scripts/ifcfg-eth0
   ```

3. Restart the Avaya Multimedia Messaging server.

   ```
   sudo /sbin/shutdown -r now
   ```

Participant has invalid messaging address

Condition

The Avaya Multimedia Messaging server client displays an error, which indicates that the participant has an invalid messaging address.

Solution

1. Ensure that the participant is an enterprise user who has an email address in the LDAP directory.
2. Ensure that the Sender is an active user in Enterprise LDAP.
3. Check that the System Manager user record for the participant has an email address as a handle and matches the LDAP email address or that LDAP synchronization is enabled with System Manager.
4. Ensure that Force LDAP Sync has been triggered on the Avaya Multimedia Messaging administration portal after the Sender and Participant email address have been added or modified in System manager.
5. Ensure that rich message entitlements have been granted to the Sender in the Avaya Multimedia Messaging administration portal, otherwise the Sender can send only text messages using the Avaya Multimedia Messaging client.

Latest TLS version is not supported

Condition

If your Avaya Multimedia Messaging deployment contains a client, such as Avaya Communicator for Windows Release 2.1, which does not support TLS 1.2, you can enable previous TLS versions. When your client is upgraded, you can disable the previous TLS versions.

Warning:

Enabling previous TLS versions can make your system vulnerable to attacks that use these protocols.

Solution

Perform these steps on both the master and backup virtual IP nodes.

1. Run one of the following commands:
   - To enable previous TLS versions:

     ```
     sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/misc/
     allowLegacyTLS.sh on
     ```

   - To disable previous TLS versions:

     ```
     sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/misc/
     allowLegacyTLS.sh off
     ```

   In these commands, `<version>` is the Avaya Multimedia Messaging build version that you are using.
2. Run `sudo service AMMNginx reload` to reload Nginx.

   This step will not cause a service outage.

Avaya Multimedia Messaging server returns alarm code 00064: Remote domain connection lost

Cause

When the Avaya Multimedia Messaging server cannot connect to Presence Services, the Avaya Multimedia Messaging raises alarm code 00064. The Avaya Multimedia Messaging server maintains the outgoing messages in its buffer, to later send the messages when the connection is restored. Over time, the accumulation of messages in the internal buffer occupies Avaya Multimedia Messaging server memory.

Solution

Restore the connection between Avaya Multimedia Messaging and Presence Services as soon as possible.

The time until the memory is occupied depends on the traffic volume from Avaya Multimedia Messaging to Presence Services during the connection failure.

Client cannot connect to the Avaya Multimedia Messaging server

Condition

The Avaya Equinox™ clients cannot connect to the Avaya Multimedia Messaging server.

Solution

1. Ensure that the Avaya Multimedia Messaging server is accessible through a browser resource discovery URL in a web browser, such as Chrome.
2. In the web browser, enter the following URL: `https://<amm-server>:8443/aem/resources`.
3. Enter the LDAP user credentials.

   The user name can have the following formats: username@domain.com or domain \username, depending on the LDAP server configuration.

   The browser displays a web page that lists the details of the user. You can download a file that contains the following details:

   ```
   {"addresses":"https://<amm-server>:8443/aem/resources/users/user-name@domain.com/
   addresses", "avayaRequestTimeout":{"maximum":120,"minimum":30,"recommended":
   120},"capabilities":{"richContent":true},
   "conversationsResource":{"href":"https://<amm-server>:8443/aem/resources/users/
   <user-name@domain.com>/conversations","maxMessageCount":15},
   "limits":{"maxAudioSize":1048576,"maxGenericAttachmentSize":3145728,"maxImageSize":
   1048576,"maxTextLength":250,"maxVideoSize":3145728},
   "messages":"https://<amm-server>:8443/aem/resources/users/user-name@domain.com/
   messages",
   "outbox":"https://<amm-server>:8443/aem/resources/messages",
   "self":"user-name@domain.com","services":{"markAsReadIf":"https://<amm-server>:
   8443/aem/services/users/user-name@domain.com/conversations/markAsReadIf",
   "validateAddresses":"https://<amm-server>:8443/aem/services/users/user-
   name@domain.com/validateAddress"}}
   ```

4. If the web page displays an error or you are unable to download the file, perform the following actions:
   a. If the page displays `Error Code 401`, the password that you have entered is not correct.
   b. If the page displays `Error Code 403`, the user does not have the privileges required for gaining access to the Avaya Multimedia Messaging client interface. You must add the respective user to the Admin group configured in the LDAP structure.
   c. If the page displays `Error Code 500`, ensure that the Avaya Multimedia Messaging server is running.

      You can use the **`ping`** command to verify that the Avaya Multimedia Messaging server is running:

      ```
      ping amm-server.domain.com
      ```

      Note:

      If you are not able to ping the Avaya Multimedia Messaging server, contact Avaya support.

d. On the Avaya Equinox™ client, navigate to **Settings** > **Services** > **Messaging** and ensure that Avaya Multimedia Messaging is enabled.

e. Ensure that the Avaya Multimedia Messaging server address and port are entered correctly and that the Avaya Multimedia Messaging server address matches the Avaya Multimedia Messaging server virtual IP address or FQDN.

HTTP services disabled due to storage capacity reaching critical threshold

Condition

Avaya Multimedia Messaging disables HTTP services and displays one of the following alarms:

- `avAMMDBStorageReachedCriticalThreshold`
- `avAMMMediaStorageReachedCriticalThreshold`

You can see that HTTP services are disabled on the **Service Control** tab of the web-based administration portal.

Cause

The database partition or the media partition is more than 95% full. You cannot start HTTP services from the administration portal as long as disk space is above the critical level.

Solution

1. Perform a backup with the backup directory on an off-node disk or another disk reserved for backups.

   Important:

   Do not perform the backup on the full disk.

2. Run the **`cleanAMM`** tool and monitor logs as directed.
3. When the cleanup is complete, check to see if sufficient disk space is available.
4. If sufficient disk space is not yet available, check to see if other large files have accumulated on the disks.
5. **(Optional)** On the **Storage Management** tab of the web-based administration portal, reduce the number of days that inactive conversations stay open.

   Note:

   The changes made to the storage management value take effect after an audit is performed. This occurs around 4 AM in Avaya Multimedia Messaging server time.

6. When sufficient disk space becomes available, start Avaya Multimedia Messaging services from the web-based administration portal.

OpenFire log displays “Requested node not found in cluster” error

Condition

Invalid zombie sessions appear when restarting members of the OpenFire cluster. As a result, a message such as the following appears in the `/opt/openfire/log/warn.log` log file.

```
2014.05.22 00:22:52 com.jivesoftware.util.cache.ClusteredCacheFactory - Requested node
e6e9ba50-5d0e-4fe4-9436-74af7a927ed4 not found in cluster
```

Cause

A race condition exists in the OpenFire 3.8.2 cluster. The side effect of this condition is that other Avaya Multimedia Messaging server components might use invalid sessions, and this results in errors.

Solution

1. Ensure you are logged in as a non-root user.
2. Stop all members of the OpenFire cluster using the following command on each node:

   ```
   sudo service AMMRecoveryManager disableWatchdog
   sudo service AMMOpenfire stop
   ```

   Note:

   This command prevents Recovery Manager from restarting OpenFire automatically.
3. Restart OpenFire on the first node using the following command:

   ```
   sudo service AMMOpenfire start
   ```
4. Monitor the `/opt/openfire/log/stderror.log` log file until you see the following:

   ```
   Members [1] {
       Member [ip of the 1st node]:5701
   }
   ```
5. Start OpenFire on the second node.
6. Wait until you see the following on the `/opt/openfire/log/stderror.log` log file:

   ```
   Members [2] {
      Member [ip of the 1st node]:5701
       Member [ip of the 2nd node]:5701
   }
   ```
7. Start OpenFire on the third node.
8. Wait until you see the following on the `/opt/openfire/log/stderror.log` log file:

   ```
   Members [3] {
       Member [ip of the 1st node]:5701
       Member [ip of the 2nd node]:5701
       Member [ip of the 3rd node]:5701
   }
   ```
9. Re-enable the watchdog functionality on each node using the following command:

   ```
   sudo service AMMRecoveryManager enableWatchdog
   ```

Performing a force update of the LDAP configuration after the resource discovery returns error 404

Condition

The resource discovery operation returns error code 404.

Solution

Use the following procedure to configure the email attribute of the users and perform a force update of the LDAP server.

1. Log in to the Avaya Multimedia Messaging administration portal.

   The URL for gaining access to the administration portal is `https://<hostname>:8445/admin`.

   Important:

   For the hostname, always use the same Avaya Multimedia Messaging server FQDN that you use for generating certificates. You will be redirected to the Login page if you use the IP address instead of the FQDN.

   To gain access to the web-based administration portal, you must use an account that has the Administrator role defined in the LDAP server configuration.
2. Select **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.
3. Click **Force LDAP Sync**.
4. Click **Save**.

Special characters displayed incorrectly when playing multimedia attachment

Condition

On the Microsoft Windows 7 operating system with Korean, Japanese, or Simplified Chinese, certain web browsers might display special characters incorrectly in the tool tips while viewing video or audio attachments.

The web browsers that may encounter this issue are the following:

- Microsoft Internet Explorer 8, 9
- Google Chrome
- Mozilla Firefox

Cause

The characters are displayed incorrectly because the operating system may have not loaded the corresponding font sets at startup.

Solution

1. On the Windows Desktop, create an empty file and name the file using special characters.

   Creating this file on the Desktop and naming it using special characters will force the operating system to load the font sets next time at startup.
2. Log off and then log in to your computer or restart the operating system.
3. Click the attachment URL in Avaya one-X® Communicator to retrieve the attachment.

User cannot send a message to a non-Avaya Multimedia Messaging Presence Services enabled client

Condition

An Avaya Multimedia Messaging user cannot send an Avaya Multimedia Messaging message, with or without media files, to a non-Avaya Multimedia Messaging, Presence Services-enabled XMPP participant, using a client, such as Avaya one-X® Communicator or Avaya Equinox™ 2.0 for Windows.

The correct behavior in this context is the following:

- The Avaya one-X® Communicator user that uses the Avaya one-X® Communicator client receives an IM containing a URL link from the Avaya Multimedia Messaging user
- The Avaya one-X® Communicator user clicks on the URL link and logs in using windows credentials with the handle user-name@domain.com and windows password or alternative (domain/user-name and Microsoft Windows password) as suggested on the Web page
- After logging in, the Avaya one-X® Communicator user can see the rich media attachment or download it

The Avaya Multimedia Messaging enabled client shows an error to the Sender saying that the Avaya one-X® Communicator participant does not have a valid messaging address.

Solution

1. Ensure that the Avaya one-X® Communicator user has the Avaya XMPP/presence handle configured correctly in System Manager.
2. Ensure that the Federation is enabled in Avaya Multimedia Messaging and Presence Services administration portals.
3. Ensure that there are no XMPP connectivity issues by checking if there are any alarms sent by Avaya Multimedia Messaging to System Manager or NMS Systems. For example:
   `Failed to reach the presence server.`

Unable to view Avaya Multimedia Messaging logs using Log Viewer

Condition

If you cannot see the Avaya Multimedia Messaging logs in the Avaya Aura® System Manager Log Viewer, you must ensure that you have provided the Avaya Aura® System Manager FQDN using the configuration tool.

Solution

1. Run the Avaya Aura® System Manager configuration script.
2. Navigate to the System Manager Alarm Configuration menu and select **System Manager IP/ FQDN**.
3. Type the Avaya Aura® System Manager FQDN and press Enter.
4. In the System Manager Alarm Configuration menu, select **Apply** and press Enter.

Upgrade fails when trace logging is turned on

Condition

When performing an Avaya Multimedia Messaging rollback, the operation times out and the upgrade fails.

Cause

The logging level is set to Trace.

Solution

Set the log level for **All** back to **Warn**.

Unable to view alarms using Avaya Aura® System Manager Admin Viewer

Condition

To view the alarms that Avaya Multimedia Messaging generates, you must use the Avaya Aura® System Manager Admin Viewer application.

If Avaya Aura® System Manager Admin Viewer does not display the Avaya Multimedia Messaging alarms, you must ensure that the Avaya Multimedia Messaging server is active in the Serviceability Agents menu and that at least one SNMP trap is configured.

Solution

1. Do the following to activate the Avaya Multimedia Messaging server.
   a. Log in to the Avaya Aura® System Manager Admin Viewer as described in *Administering Avaya Aura® System Manager*.
   b. In the left panel, click **Inventory** > **Agents** > **Serviceability Agents**.
   c. Click the **Selected Agents** tab.
   d. In the Agent List, select the Avaya Multimedia Messaging server, using the host name or the IP address of the server.
   e. If the status of the Avaya Multimedia Messaging server is *inactive*, click the **Activate** button.
2. Do the following to configure an SNMP trap.
   a. Log in to the Avaya Aura® System Manager Admin Viewer.
   b. In the left panel, click **Inventory** > **Agents** > **Serviceability Agents**.
   c. Click the **SNMP Target Profiles** tab.
   d. In the **Assignable Profiles** and **Removable Profiles** fields, identify the SNMP traps that might be related to the Avaya Multimedia Messaging server.

      For more information about viewing and adding SNMP traps, see *Administering Avaya Aura® System Manager*.
   e. On the Avaya Multimedia Messaging server, view the content of the `snmpd.conf` file and ensure that the file reflects the SNMP trap destination defined in Avaya Aura® System Manager Admin Viewer.

      Example:

```
# cat /var/net-snmp/snmpd.conf | grep 1.2.3.4
targetAddr 1.2.3.4_V2_1 .1.3.6.1.6.1.1.1 0x8714f61227b2 3000 3 "1.2.3.4_V2_1"
1.2.3.4_V2_1 3 1
targetParams 1.2.3.4_V2_1 1 2 public 1 3 1
```

Glossary

API	Application Programming Interface
Cassandra	Third party NoSQL database, which is used by Avaya Multimedia Messaging to store messaging data and configuration information. For more information, see https://cassandra.apache.org/.
Domain Name System (DNS)	A system that maps and converts domain and host names to IP addresses.
Extensible Messaging and Presence Protocol (XMPP)	A communications protocol for message-oriented middleware based on XML (Extensible Markup Language).
Federation	Multiple computing or network providers agreeing upon standards of operation in a collective fashion.
Fully Qualified Domain Name (FQDN)	A domain name that specifies the exact location of the domain in the tree hierarchy of the Domain Name System (DNS).
GlusterFS	Third party distributed file system, which is used by Avaya Multimedia Messaging to store multimedia attachments. For more information, see https://www.gluster.org/.
IM	Instant Messaging.
Kerberos Key Distribution Center	A network service that supplies session tickets and temporary session keys to users within an Active Directory domain. The KDC runs on each domain controller.
Nginx	Third party web server, which is used by Avaya Multimedia Messaging for TLS termination and load balancing. For more information, see https://nginx.org/.
NTP (Network Time Protocol)	A protocol used to synchronize the real-time clock in a computer.
REST	Representational state transfer. This is a software architectural style used with Application Programming Interfaces (APIs).

RSA	A public-key cryptographic system used for secure data transmission.
Secure Shell (SSH)	Secure Shell (SSH) is a group of standards and an associated network protocol that the system can use to establish a secure channel between a local and a remote computer. SSH uses public-key cryptography to mutually authenticate a user and a remote computer. SSH uses encryption and message authentication codes to protect the confidentiality and integrity of the data that is exchanged between the two computers.
Service record (SRV record)	A specification of data in the Domain Name System defining the location, i.e. the hostname and port number, of servers for specified services.
Simple Network Management Protocol (SNMP)	A protocol for managing devices on IP networks.
TLS	Transport Layer Security

Index

I

L

M

N

O

P

R

S

T

U

V

X