



Administering Avaya Multimedia Messaging

Release 3.5
Issue 1
December 2018

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.

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](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](http://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](http://www.mpegla.com).

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <https://support.avaya.com> or such successor site as designated by Avaya.

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction	9
Purpose	9
Change history	9
Chapter 2: Avaya Multimedia Messaging overview	10
New in this release	10
Topology	11
Components	12
Administrator responsibilities	13
Chapter 3: Management tools and commands	14
gluster volume status	16
Usage example	16
cas-nodetool.sh	16
Usage example	17
cleanAMM	18
Usage example	18
clitool	18
Usage example	19
collectlogs	20
System layer commands for Avaya-provided OVA deployments	20
sys seconfig command	21
sys versions command	22
sys volmgt command	22
sys smcvemgt command	26
Chapter 4: Management of Avaya Multimedia Messaging with the administration portal	30
Prerequisites for accessing the admin portal	30
Browser requirements for the admin portal	30
Logging in to the Avaya Multimedia Messaging administration portal	30
Starting and stopping the Avaya Multimedia Messaging service	31
Managing application sessions	31
Application Properties field descriptions	32
Managing server storage	32
Managing messaging domains	33
Managing client device certificates	33
Updating feature entitlements	34
Feature entitlements field descriptions	35
LDAP server management	36
Configuring the UID mapping attributes when using multiple authentication domains	36
Adding a new enterprise LDAP server	37

Configuring Windows Authentication for Active Directory.....	43
Updating enterprise directory settings.....	45
Managing federation gateway connections.....	45
Verifying cluster nodes.....	46
Cluster field descriptions.....	46
Generating performance data and statistics.....	46
Adding and editing local and remote sites for multisite configuration.....	48
Managing logs.....	48
Updating media size limits.....	49
Configuring the LDAP attribute mappings.....	49
Managing certificates in the Avaya Multimedia Messaging web administration portal.....	50
Managing System Manager certificates.....	50
Managing identity certificates.....	51
Managing truststore certificates.....	54
Importing the secure LDAP certificate using the web administration portal.....	55
Push notification management.....	55
Chapter 5: Integrated Windows Authentication administration and management.....	56
Authentication prerequisites.....	56
Setting up the Windows Domain Controller.....	57
Windows Domain Controller command descriptions.....	58
Setting up IWA on the Avaya Multimedia Messaging administration portal.....	59
Chapter 6: Avaya Multimedia Messaging multisite adaptor administration and management.....	61
Connector types for the Avaya Multimedia Messaging adaptor.....	61
Home site ID.....	62
Forcing the user synchronization process.....	62
Multisite adaptor field descriptions.....	63
Chapter 7: Virtual hardware adjustments.....	64
Adjusting the memory resource of a virtual machine.....	64
Adjusting the CPU resource of a virtual machine.....	65
Adjusting the virtual network interface.....	65
Increasing the size of a virtual disk.....	66
Increasing the size of a disk volume on a virtual machine.....	66
Chapter 8: Avaya push notification management.....	69
Push notifications.....	69
Checklist for push notification service configuration.....	69
Third-party push notification provider requirements.....	70
Avaya Cloud account configuration.....	71
Avaya Cloud account registration.....	71
Company domain provisioning.....	71
Adding the Avaya Mobile Push Notification Service to a company profile on your Avaya Cloud account.....	71
Firewall configuration.....	72

Configuring the Avaya Push Notification provider on Avaya Multimedia Messaging.....	72
Configuring a third-party push notification provider on Avaya Multimedia Messaging.....	74
Removing a third-party push notification provider.....	76
Configuring mobile application settings.....	77
Disabling push notifications.....	78
Configuration parameters for iOS applications.....	78
Chapter 9: AWS-specific management options.....	80
Increasing the size of an AWS disk volume.....	80
Block device descriptions.....	81
Updating an existing stack with a new CloudFormation template.....	82
Deleting a CloudFormation stack.....	82
Chapter 10: Monitoring options.....	84
Scheduling periodic repairs of database inconsistencies.....	84
Logs and alarms.....	85
Preventing the creation of audit audispd logs if Avaya Multimedia Messaging is deployed as a software-only application.....	88
Logging trace-level messages on Avaya Multimedia Messaging.....	89
Enhanced Access Security Gateway for real time support.....	89
Enabling the Enhanced Access Security Gateway after Avaya-provided OVA deployment.....	89
Installing and enabling the Enhanced Access Security Gateway if Avaya Multimedia Messaging is deployed as a software-only application.....	91
Disabling EASG.....	93
Removing EASG.....	93
Chapter 11: External customization options.....	94
Customizing the Login screen message for Message Playback.....	95
Chapter 12: Backup and restore.....	97
Backing up Avaya Multimedia Messaging.....	98
Backup command options.....	99
Restoring Avaya Multimedia Messaging.....	100
Prerequisites for restoring Avaya Multimedia Messaging.....	100
Restoring Avaya Multimedia Messaging in a standalone deployment.....	100
Restoring a node from a cluster.....	101
Restoring a cluster.....	103
Restore command options.....	104
Monitoring the Gluster repair status.....	104
Archiving.....	105
Lync or Skype for Business recovery.....	106
Chapter 13: Upgrades and migrations.....	108
Latest software updates and patch information.....	108
Upgrading the Avaya Multimedia Messaging server.....	108
Rollback operations.....	110
Restoring a previous version of the Avaya Multimedia Messaging server.....	111
Migration of the Avaya Aura [®] environment.....	111

Migrating the Data Replication Service.....	112
Presence Services federation migration.....	112
Checking for DRS synchronization after a migration or upgrade.....	114
Chapter 14: System layer (OS) updates for virtual machines deployed using Avaya- provided OVAs.....	116
Determining if a system update is applicable.....	116
Downloading, extracting, and staging a system layer update.....	117
Installing a staged system layer update.....	119
Chapter 15: Resources.....	120
Documentation.....	120
Finding documents on the Avaya Support website.....	122
Avaya Documentation Portal navigation.....	122
Training.....	123
Viewing Avaya Mentor videos.....	123
Support.....	124
Using the Avaya InSite Knowledge Base.....	124
Glossary.....	126

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 3.5 Feature Pack (FP) 1, Issue 1	December 2018	• Updated New in this release on page 10. • Added a new “Avaya push notification management” chapter. • Updated Upgrading the Avaya Multimedia Messaging server on page 108. • Updated Documentation on page 120. • Minor rephrasing 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 other users.
- 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. You can also deploy Avaya Multimedia Messaging through VMware or Amazon Web Services (AWS). 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 3.5 and Feature Pack 1:

Apple Push Notification service (APNs)

The push notification mechanism enables clients to receive incoming call alerts and other notifications from a third-party notification service. Applications can receive notifications even when they are suspended or in Sleep mode.

Topology

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

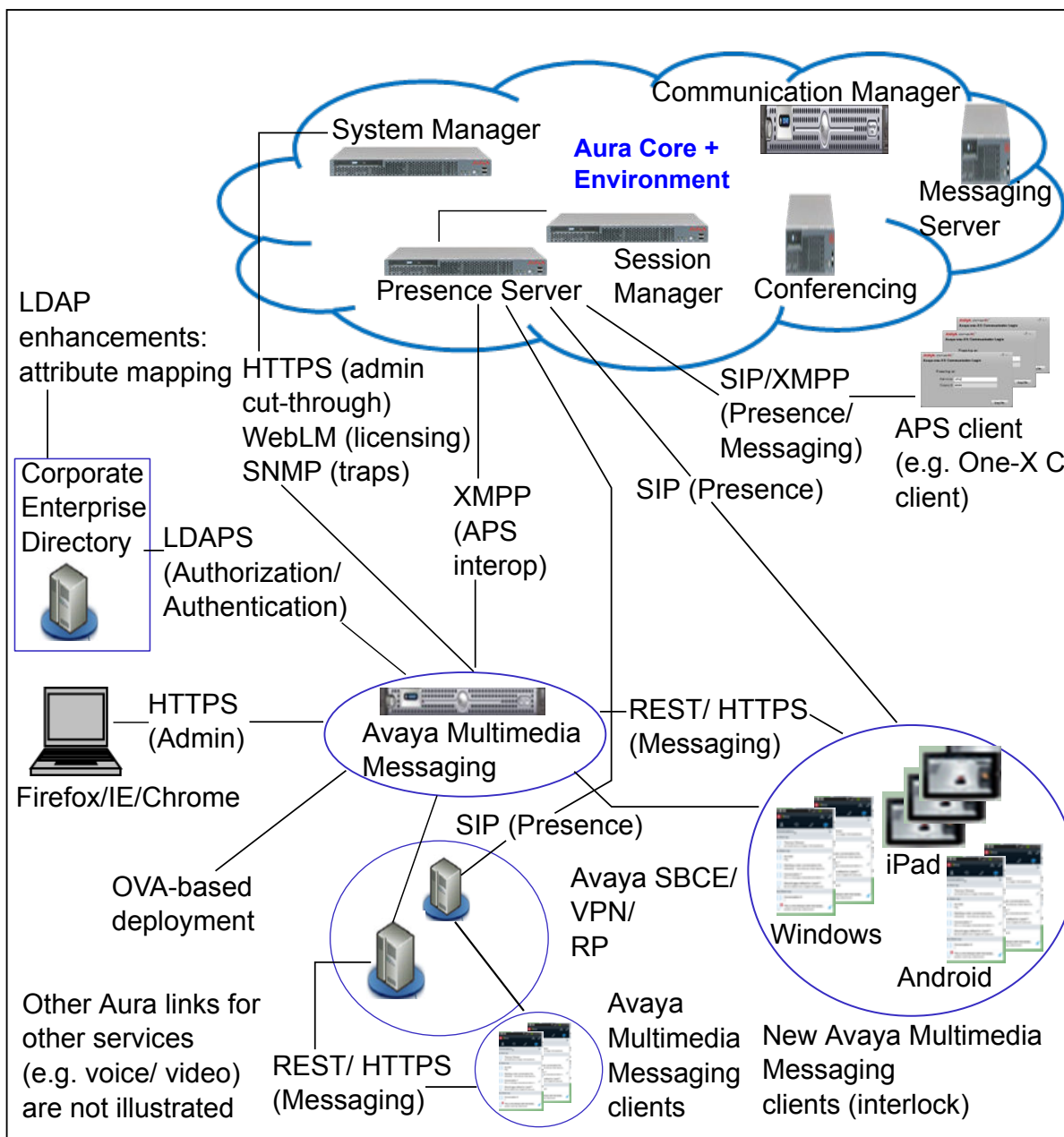


Figure 1: Avaya Multimedia Messaging deployment architecture

Components

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	The network security solution that is required for Microsoft federation with external domains.
Avaya Breeze™	The platform for deploying advanced collaboration capabilities. Avaya Breeze™ is required for hosting Avaya Aura® Presence Services Release 7.0 and above.
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

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 30.
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	cas-nodetool.sh	The cas-nodetool.sh utility provides usage information about the Cassandra database nodes. cas-nodetool.sh uses the Apache Cassandra nodetool utility. For more information about using the Apache Cassandra nodetool utility, 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 <code>logs/cleaner_CLF.log</code> 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.
	statusAMM.sh	A tool that displays the status of the Avaya Multimedia Messaging server and of the related services. Use the statusAMM tool to verify that the Avaya Multimedia Messaging is installed properly and that the services are running. The statusAMM.sh script is located in the <code>/opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/bin/</code> 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 adaptor 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 • sys smcvemgt

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
```

cas-nodetool.sh

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

cas-nodetool.sh uses the Apache Cassandra nodetool utility. For more information about using the Apache Cassandra nodetool utility, see the [Cassandra database documentation](#).

Usage example

To view the status of the database, run the **cas-nodetool.sh status** command.

For example:

```
[root@amm-1 logs]# /opt/AvayaMultimediaMessaging/<version>/CAS/<version>/cassandra/cas-
nodetool.sh 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 **cas-nodetool.sh repair** command.

! Important:

To protect data integrity, you must run the **cas-nodetool.sh** utility 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/AvayaMultimediaMessaging/<version>/CAS/<version>/cassandra/cas-
nodetool.sh repair
[2018-03-04 08:49:01,128] Starting repair command #1, repairing 256 ranges for keyspace
cas_common_data
[2018-03-04 08:49:04,465] Repair command #1 finished
[2018-03-04 08:49:04,492] Starting repair command #2, repairing 256 ranges for keyspace
amm_data
[2018-03-04 08:49:07,756] Repair command #2 finished
[2018-03-04 08:49:07,781] Starting repair command #3, repairing 256 ranges for keyspace
acs
[2018-03-04 08:49:11,015] Repair command #3 finished
[2018-03-04 08:49:11,024] Nothing to repair for keyspace 'system'
[2018-03-04 08:49:11,030] Starting repair command #4, repairing 256 ranges for keyspace
openfire
[2018-03-04 08:49:11,205] Repair command #4 finished
[2018-03-04 08:49:11,229] Starting repair command #5, repairing 256 ranges for keyspace
sip_notification_cql
[2018-03-04 08:49:14,468] Repair command #5 finished
[2018-03-04 08:49:14,492] Starting repair command #6, repairing 256 ranges for keyspace
amm_notification
[2018-03-04 08:49:17,727] Repair command #6 finished
[2018-03-04 08:49:17,751] Starting repair command #7, repairing 256 ranges for keyspace
amm_system
[2018-03-04 08:49:21,005] Repair command #7 finished
[2018-03-04 08:49:21,029] Starting repair command #8, repairing 256 ranges for keyspace
amm_federation
[2018-03-04 08:49:24,507] Repair command #8 finished
[2018-03-04 08:49:24,535] Starting repair command #9, repairing 256 ranges for keyspace
clusteradmin
[2018-03-04 08:49:27,776] Repair command #9 finished
[2018-03-04 08:49:27,785] Starting repair command #10, repairing 256 ranges for
keyspace system_auth
[2018-03-04 08:49:27,966] Repair command #10 finished
[2018-03-04 08:49:27,990] Starting repair command #11, repairing 256 ranges for
keyspace SIP_Notification
[2018-03-04 08:49:31,249] Repair command #11 finished
```

```
[2018-03-04 08:49:31,258] Nothing to repair for keyspace 'system_traces'
[2018-03-04 08:49:31,300] Starting repair command #12, repairing 256 ranges for
keyspace amm_schema_version
[2018-03-04 08:49:34,182] Repair command #12 finished
[2018-03-04 08:49:34,190] Starting repair command #13, repairing 256 ranges for
keyspace OpsCenter
[2018-03-04 08:49:34,352] Repair command #13 finished
```

If you use **cas-nodetool1.sh** 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.

 Note:

If you select the **Auto-Discard for Closed Conversations** option, Avaya Multimedia Messaging will automatically delete closed conversations after a specified number of days. If you use this option, you do not need to run the cleanAMM utility.

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.

*** Note:**

The clitool.sh utility does not create report directories automatically. You must create a report directory and set the read, write, and execute permissions to this directory before running the clitool.sh utility using the following commands:

```
mkdir <report_directory>
sudo chmod 777 <report_directory>
```

For example:

```
[jdoe@pvt5sv213 jdoe]$ mkdir /tmp/reportDirectory
[jdoe@pvt5sv213 jdoe]$ sudo chmod 777 /tmp/reportDirectory
[jdoe@pvt5sv213 jdoe]$ cdto misc
[jdoe@pvt5sv213 misc]$ sudo ./clitool.sh dailyReport /tmp/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 /tmp/reportDirectory/
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 14

System layer commands for Avaya-provided OVA deployments

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@server-dev ~]$ sys
Execute system layer commands.

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

-hh, --hhhelp
    Verbose help

Available commands:

secconfig      [Manage security settings]
versions       [Query version information]
volmgt         [Manage disk volume sizes]
smcvemgt       [Manage Spectre/Meltdown patches]

Command invocation syntax:
    sys <command> <arguments>

Command syntax
    sys <command> -h

[admin@server-dev ~]$
```

! Important:

These system layer commands are not available for Avaya Multimedia Messaging software-only deployments.

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@server-dev ~]$ 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 "--hhhelp") for verbose help.

seconfig
  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.

smcvmgt
  Manages the enablement status of Linux kernel patches for the
  Spectre and Meltdown vulnerabilities.

[admin@server-dev ~]$
```

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

sys seconfig command

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

```
[admin@server4950amm ~]$ sys seconfig --hhhelp

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).

--hhhelp, -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 : 3.4.0.0.8
Partitioning version : 2.0
Original OVA deploy  : amm-3.4.0.0.329

[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
--hhhelp,              -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 --hhhelp

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

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

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 specified,
    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 mebibytes, "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 version 2.0.

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				
Num	Name	Size	Free	Name	LVM Size	File System 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	

sys smcvemgt command

The system layer **smcvemgt** command is used to manage the Linux kernel patches related to the following vulnerabilities:

- Variant #2/Spectre (CVE-2017–5715)
- Variant #3/Meltdown (CVE-2017–5754)

*** Note:**

The kernel patch for the Variant #1/Spectre (CVE-2017–5754) vulnerability is permanently enabled on the system and cannot be disabled.

The choice to enable or disable these patches is a trade-off between performance and security impact:

- If the patches are enabled, the system might experience noticeable performance losses.
- If the patches are disabled, the system is not protected against the Variant #2/Spectre and Variant #3/Meltdown vulnerabilities.

By default, Linux patches for Variant #2/Spectre and Variant #3/Meltdown are enabled. The Variant #2/Spectre patch is enabled with Linux kernel defaults. In default operation mode, the Variant #2/Spectre Linux patch selects the mitigation method that is best suited for the processor architecture of the host machine.

*** Note:**

To be fully functional, patches for the Variant #2/Spectre vulnerability require hardware support, which is provided by VMware and hardware vendors through microcode updates.

Changes made by the **smcvemgt** command to the Linux kernel tunables always cause a server reboot. The script does not manage the state of application services. To ensure that the application services are stopped before the reboot, run the `svc amm stop` command before using the **smcvemgt** command. After the reboot, manually start the application services using the `svc amm start` command.

For more information about Spectre and Meltdown kernel tunables that are affected by the **smcvemgt** command, see <https://access.redhat.com/articles/3311301>. For more information about the Spectre and Meltdown vulnerabilities, see <https://access.redhat.com/security/vulnerabilities/speculativeexecution>.

Syntax help: sys smcvemgt --help

```
[admin@server-dev ~]$ sys smcvemgt --help
```

```
Version 1.2
```

```
Syntax:
```

```
--help,      -h
--hhelp,     -hh
--query,     -q
--set,       -s  enabled
--set,       -s  disabled
--set,       -s  [ v2=<v2-mode> ] [ v3=<v3-mode> ]
               (v2-mode: disabled | default | kernel | user | both | user+retp)
```

```
(v3-mode: disabled | enabled)
--history
```

Verbose help: sys smcvemgt --hhelp

```
[admin@srvr-dev ~]$ sys smcvemgt --hhelp
```

Version 1.2

This script manages the enablement status of the Linux kernel patches for the following Spectre and Meltdown vulnerabilities:

```
Variant #2/Spectre (CVE-2017-5715)
Variant #3/Meltdown (CVE-2017-5754)
```

The kernel patch for the following related vulnerability is permanently enabled on the system (cannot be disabled):

```
Variant #1/Spectre (CVE-2017-5753)
```

Note that hardware support is required for Variant #2/Spectre to be fully functional. CPU microcode updates must be applied in order for this hardware support to be provided. The "--query" argument includes an indication as to whether or not hardware support is provided on this server.

For more information on Spectre/Meltdown kernel tunables, refer to:

```
https://access.redhat.com/articles/3311301
```

For additional information on the Spectre/Meltdown vulnerabilities, refer to:

```
https://access.redhat.com/security/vulnerabilities/speculativeexecution
```

Syntax:

```
--help,    -h
    Provide terse help.

--hhelp,    -hh
    Provide verbose help (this text).

--query,    -q
    Query the configuration of the Variant #2/Spectre and Variant #3/
    Meltdown tunables for system reboots, as well as on the running
    system.

--set,  -s  enabled
--set,  -s  disabled
--set,  -s  [ v2=<v2-mode> ] [ v3=<v3-mode> ]
    Enables and disables Variant #2/Spectre ("v2") and/or Variant #3/
    Meltdown ("v3") patches.
```

This immediately reboots the server. Applications on the server are not managed by this script. Ensure that any applications are disabled, as required, prior to changing kernel settings with this script.

If "enabled" is specified, then both v2 and v3 are enabled, with v2 set to kernel default behavior. If "disabled" is specified, then both v2 and v3 are disabled. Otherwise, kernel patches are enabled or disabled as per the specified "v2" and/or "v3" arguments. If a "v2" or "v3" argument is not specified, the current system value for that item is retained.

```

v2-mode:

    disabled
        Variant #2/Spectre is disabled.

    default
        The kernel decides how to set tunables for Variant #2/
        Spectre, based on the processor architecture. Note that for
        architectures prior to Skylake, the kernel selects
        retpoline ("return trampoline") over ibrs.

    kernel
        Use "ibrs" (i.e., kernel space only).

    user
        Use "ibrs_user" (i.e., userland only).

    both
        Use "ibrs_always" (i.e., kernel space and userland).

    user+retp
        Use "retpoline,ibrs_user".

v3-mode:

    disabled
        Variant #3/Meltdown is disabled.

    enabled
        Variant #3/Meltdown is enabled.
    The following two commands are equivalent:

        sys smcvemgt enabled
        sys smcvemgt v2=default v3=enabled

    The following two commands are equivalent:

        sys smcvemgt disabled
        sys smcvemgt v2=disabled v3=disabled

--history
    Show a history of changes made to the enablement status of the
    Spectre and Meltdown patches.
    
```

sys smcvemgt usage examples

Command for querying current tunable settings

The following command queries the current tunable settings for the next boot, as well as the current runtime. This command also indicates whether there is hardware support for Variant #2/Spectre.

```
sys smcvemgt --query
```

Command for enabling patches with default settings

The following command enables patches for Variant #2/Spectre and Variant #3/Meltdown, where Variant #2/Spectre is configured for default mode. In default mode, the kernel selects the Variant #2/Spectre mitigation mechanism based on the CPU architecture of the host machine.

```
sys smcvemgt --set enabled
```

Commands for enabling patches with specific settings

- The following command enables patches for Variant #2/Spectre and Variant #3/Meltdown, where Variant #2/Spectre is set to kernel space only.

```
sys smcvemgt --set v2=kernel v3=enabled
```

- The following command enables patches for Variant #2/Spectre, which are configured for user space with “Retpoline”, or “return trampoline”. Variant #3/Meltdown retains its current settings.

```
sys smcvemgt --set v2=user+retp
```

Command for disabling patches

The following command disables patches for Variant #2/Spectre and Variant #3/Meltdown.

```
sys smcvemgt --set disabled
```

Command for disabling patches for a specific vulnerability

The following command disables patches for Variant #3/Meltdown. Variant #2/Spectre retains its current settings.

```
sys smcvemgt --set v3=disabled
```

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 host name, 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. On the Avaya Multimedia Messaging web administration portal, navigate to **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. On the Avaya Multimedia Messaging web administration portal, navigate to **Service Control > Application Management**.

2. In the Application Properties area, complete the required settings, which are described in [Application Properties field descriptions](#) on page 32.
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. On the Avaya Multimedia Messaging web administration portal, navigate to **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. On the Avaya Multimedia Messaging web administration portal, navigate to **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. On the Avaya Multimedia Messaging web administration portal, navigate to **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. On the Avaya Multimedia Messaging web administration portal, navigate to **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 <i>Normal</i> , 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: • <i>VALID</i> if the license file is valid and the server can communicate with the WebLM Server. • <i>NO_LICENSE</i> if the license file cannot be found on the WebLM Server. • <i>EXPIRED</i> if install license file is expired. • <i>INVALID</i> 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.

Name	Description
Available	Displays the number of licenses still available for use.
Acquired	Displays the number of licenses currently acquired.

LDAP server management

You must configure the enterprise LDAP server to authenticate the users and administrators of Avaya Multimedia Messaging. When you log in to the Avaya Multimedia Messaging web administration portal, the system displays the enterprise LDAP server that you configure at the time of Avaya Multimedia Messaging deployment.

For secure connectivity to LDAP servers, you must import an LDAP certificate file to the Tomcat trust store. For more information, see [Importing the secure LDAP certificate using the web administration portal](#) on page 55.

Configuring the UID mapping attributes when using multiple authentication domains

About this task

If you are using multiple authentication domains, the UID mapping attribute value set for each LDAP server must be domain-qualified. Therefore, the value must include the `@domain` part. The following values are supported:

- `mail`
- `userPrincipalName`
- Any custom attribute that uses a domain-qualified value.

Note:

If you are not using multiple authentication domains, Avaya Multimedia Messaging supports only the following values for the UID mapping attribute:

- `sAMAccountName`
- `mail`
- `userPrincipalName`

Procedure

1. On the Avaya Multimedia Messaging web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.

The system displays the Enterprise LDAP Server Configuration page.

2. For each LDAP server in the system, in the **UID Attribute ID** field, enter the appropriate value.

Adding a new enterprise LDAP server

Before you begin

If you are planning to use multiple authentication domains, configure the UID mapping attributes as specified in [Configuring the UID mapping attributes when using multiple authentication domains](#) on page 36.

Procedure

1. On the Avaya Multimedia Messaging web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.

The system displays the Enterprise LDAP Server Configuration page.

2. Click the plus (+) icon.

The system displays the New Directory tab.

3. In the **Enterprise-Directory Type** field, click the LDAP server directory that you want to add.
4. In the **Provenance Priority** field, type the priority of the enterprise LDAP server directory.
5. In the Server Address and Credentials section, specify the parameters of the enterprise LDAP server directory.
6. If you want to use the new server for authentication and authorization, do the following:
 - a. Select the **Use for Authentication** check box.
 - b. Configure role-related attributes, such as **Role Filter**, **Role Attribute ID**, and **Role Context DN**.

For more information about attributes, see [Enterprise LDAP Server Configuration field descriptions](#) on page 37.

7. Click **Save**.

Enterprise LDAP Server Configuration field descriptions

New Directory

Name	Description
Enterprise-Directory Type	Specifies the name of the enterprise directory. The options are: • ActiveDirectory_2008 • ActiveDirectory_2012 • Novell 8.8

Name	Description
	• Domino 8.5.3 • LDS_2012 • LDS_2008 • OpenLDAP 2.4.31 • OracleDirectoryServer 5.2
Provenance Priority	Specifies the provenance priority of the enterprise directory. Provenance priority is used while merging contacts. If a value is available in more than one directory, the value in the directory with higher provenance priority is returned. For example, if firstName is obtained from two directories, the firstName from the source with higher provenance priority is returned. You can assign a value between 2 to 10. You cannot assign Provenance priority 1 because it is always assigned to the authorization directory. Provenance priority 1 is the highest and 10 is the lowest. Provenance priority must be different for each enterprise directory or source.

Server Address and Credentials

Name	Description
Secure LDAP	Indicates whether the LDAP Server connection is secure or not.
Windows Authentication	Specifies whether to use Windows Authentication or not. The options are: • None • Negotiate If you select the Negotiate option, the system displays the Configuration for Windows Authentication section.  Note: Windows authentication is only supported if you are using a single authentication directory. If you are using multiple authentication directories, Windows Authentication is disabled.
Address	Specifies the IP address of LDAP Server. This field is mandatory.
Port	Specifies the port of LDAP Server. This field is mandatory.

Name	Description
Bind DN	Specifies the Distinguished Name (DN) of the user that has read and search permissions for the LDAP server users and roles. This is a mandatory setting The format of the Bind DN depends on the configuration of the LDAP server. This field is mandatory.  Note: Even though the parameter name is Bind DN, the format of its value is not limited to the DN format. The format can be any format that the LDAP server can support for LDAP bind. For example: for Active Directory, you can use "domain\user", "user@domain", as well as the actual DN of the user object. For example: for Active Directory, you can use "domain\user", "user@domain", as well as the actual DN of the user object.
Bind Credential	Specifies the password of the administrative user.
Base Context DN	Specifies the complete Distinguished Name (DN) with the Organizational Unit (OU) for starting the search for users on the enterprise directory. This is the primary Base Context DN for Avaya Multimedia Messaging. For example: dc=domain, dc=company, dc=com. If you are using multiple authorization domains, Avaya recommends including a domain component to the Base Context DN. For example: dc=avaya, dc=com.  Note: Some LDAP sources, such as Domino, typically do not contain the domain component in Base Context DNs. For example: o=MyCompany. If Base Context DNs do not contain the domain component, Avaya Multimedia Messaging considers them "empty" Base Context DNs when processing user login or search requests. If Avaya Multimedia Messaging cannot find the domain specified in the request, the search continues in "empty" Base Context DNs.
Use additional Base Context DN	Enables Avaya Multimedia Messaging contact search and quick search. You can add up to 10 Base Context DNs with the same value. The

Name	Description
	primary Base Context DN is used for authentication. Additional Base Context DNs are used for Avaya Multimedia Messaging contact search and quick search, and can also be used for authentication. If you select this check box, you can see the View/Edit button. Auto-configuration will use only the primary base context DN.
View/Edit	Enables access to the Addition Base DN Configuration page, where you can add or delete additional Base Context DNs.
UID Attribute ID	Specifies the unique attribute of the user on LDAP, which is used to search for users in the LDAP server. If you are using multiple authentication domains, you must use one of the following values: • mail • userPrincipalName • Any custom attribute that uses a domain-qualified value. If you are not using multiple authentication domains, you must use one of the following values: • sAMAccountName • mail • userPrincipalName This field is mandatory.
Role Filter	Specifies the search filter that is used to search the roles of the user. For example: (&(objectClass=group) (member={1}))
Role Attribute ID	Specifies that the user is a member of the groups defined by that attribute. For example: objectCategory This field is mandatory.
Roles Context DN	Specifies the complete Distinguished Name (DN) to search for a user role, that is, for Role Filter. For example: dc=domain,dc=company,dc=com
Role Name Attribute	Specifies the name of the role attribute. This field is mandatory only if the Role Name Attribute Is DN field is set to true.

Name	Description
	For example: cn if the role is stored in a DN in the form of cn=admin, ou=Users, dc=company, dc=com.
Role Attribute is DN	Indicates whether the role attribute of the user contains DN. The default value is true.
Allow Empty Passwords	Indicates whether LDAP Server acknowledges the empty password. The default value is false.
Search Scope	Specifies the level of the search in the LDAP hierarchy. The options are: • 0: For searching only for the object. • 1: For including one level in the LDAP hierarchy in the search. • 2: For including subtree in the LDAP hierarchy in the search. The default value is 2.
Role Recursion	Specifies whether role recursion is enabled. The options are: • true • false
Administrator Role	Specifies the administrator role in which the administrative users are assigned.
Security Administrator Role	Specifies the security administrator role in which the administrative users can manage web certificates from the web administration portal.
User Role	Specifies the user role in which the common users are assigned.
Auditor Role	Specifies the auditor role in which the users can audit the system.
Services Maintenance and Support Role	Specifies the services maintenance and support role in which users can maintain and support services.
Services Administrator Role	Specifies the services administrator role.
Language used in Directory	• Simplified Chinese (zh) • German (de) • English (en) • Spanish (es)

Name	Description
	• French (fr) • Italian (it) • Japanese (ja) • Korean (ko) • Russian (ru) • Portuguese (pt)
Active Users Search Filter	Specifies whether the user is active or inactive on LDAP Server.
Last Updated Time Attribute ID	Specifies when the user is updated on LDAP. For example, <code>whenChanged</code> This field is mandatory.

Configuration for Windows Authentication

Name	Description
Service Principal Name (SPN)	Specifies the service principal name UIDAttributeID must be userPrincipalName.
Import keytab file	Imports the <code>tomcat.keytab</code> file and overwrites the existing file.
Kerberos Realm	Specifies the Kerberos realm.
DNS Domain	Specifies the DNS domain of the Domain Controller.
KDC FQDN	Specifies the FQDN of the Domain Controller.
KDC Port	Specifies the port number. The Default KDC port is 88.

Button	Description
Test Connection	Tests the connection changes.
Save	Saves the changes made to the enterprise directory.
Modify Attribute Mappings	Modifies the attributes of LDAP Server.

Configuring additional base context DNs

About this task

Use this procedure to add additional base context DNs. Additional base context DNs are used for Avaya Multimedia Messaging contact search and quick search, and can also be used for authentication. You can add up to 10 base context DNs for one LDAP source.

If you are planning to use the additional base context DN for authorization, the role context DN configured in the primary LDAP will be used for this additional base context DN.

Procedure

1. On the Avaya Multimedia Messaging web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
The system displays the Enterprise LDAP Server Configuration page.
2. In the Server Address and Credentials section, select the **Use additional Base Context DN** check box and click **View/Edit**.
3. In the Additional Base Context DN Configuration window, click **+**.
4. Select the base context DN and in the **Base Context DN** field, provide the value of the base context DN.
5. If you want to use the base context DN for authentication, select the **Use for Authentication** check box.
6. Click **Save**.

Configuring Windows Authentication for Active Directory

About this task

Windows authentication is only supported if you are using a single authentication directory. If you are using multiple authentication directories, Windows Authentication is disabled.

Before you begin

Ensure that the LDAP server you use is the Domain Controller with the appropriate Active Directory version as the server type.

Procedure

1. On the Avaya Multimedia Messaging web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
The system displays the Enterprise LDAP Server Configuration page.
2. In the Server Address and Credentials section, do the following:
 - a. In the **Windows Authentication** field, click **Negotiate**.
 - b. In the Confirm Action pop-up window, click **OK**.
 - c. The **UIDAttributeID** must be userPrincipalName.
 - d. Ensure that the other settings on the Server Address and Credentials page are appropriate for the LDAP configuration of your Domain Controller.
3. In the Configuration for Windows Authentication section, do the following:

+ Tip:

To complete the following fields, use the same values you entered when setting up the Windows Domain Controller.

- a. In **Service Principal Name**, type `HTTP` or `REST_FQDN`.

For example, type `HTTP` or `aads.example.com`.

- b. To import the `tomcat.keytab` file transferred from the Windows Domain Controller, in **Import keytab file**, click **Import**.

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.

You can 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
```

- c. In **Kerberos Realm**, type the Kerberos realm, which is usually in uppercase letters.

For example, `EXAMPLE.COM`.

- d. In **DNS Domain**, type the DNS domain of the Domain Controller.

For example, `example.com`.

- e. 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`.

- f. In **KDC Port**, do not change the default setting , which is 88.

- g. In a cluster deployment, click **Send Keytab File** to send the `tomcat.keytab` file 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. Save the settings to restart the server.

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

Updating enterprise directory settings

Procedure

1. On the Avaya Multimedia Messaging web administration portal, navigate to **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. On the Avaya Multimedia Messaging web administration portal, navigate to **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 Avaya Multimedia Messaging federation configuration section of *Deploying Avaya Multimedia Messaging*.

- 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. On the Avaya Multimedia Messaging web administration portal, navigate to **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. On the Avaya Multimedia Messaging web administration portal, navigate to **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.

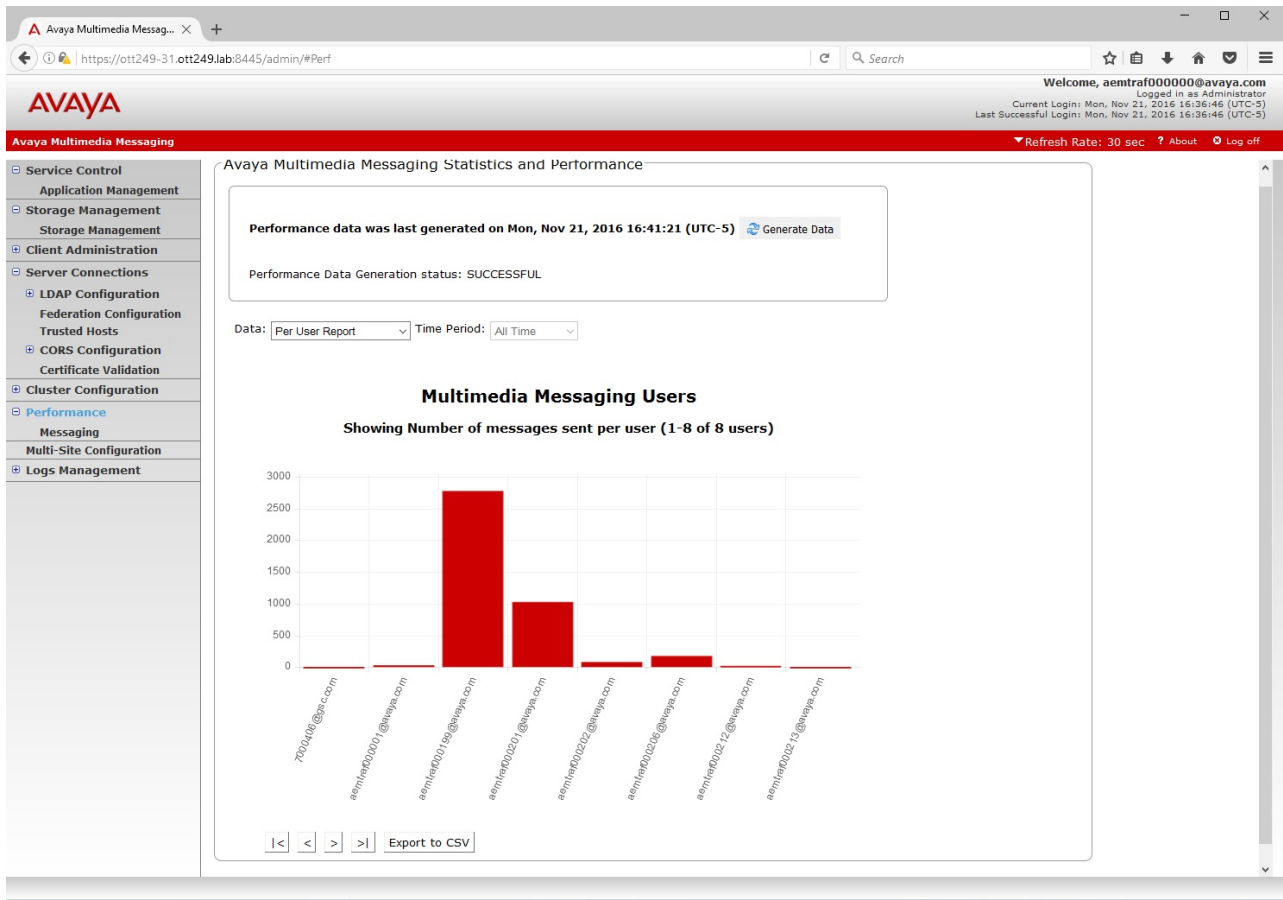
- Message traffic.
 - The number of messages sent per user.
 - Attachment breakdown with media types and size.
4. Select a time period.

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 adaptor administration and management](#) on page 61.

Procedure

1. On the Avaya Multimedia Messaging web administration portal, navigate to **Multi-Site Configuration**.
2. In the Local Site Information and Remote Site Information areas, do one of the following:
 - 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. On the Avaya Multimedia Messaging web administration portal, navigate to **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 substeps b and c.

Updating media size limits

Procedure

1. On the Avaya Multimedia Messaging web administration portal, navigate to **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. On the Avaya Multimedia Messaging web administration portal, navigate to **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**.

Managing certificates in the Avaya Multimedia Messaging web administration portal

About this task

You can use the Avaya Multimedia Messaging administration portal to review and manage certificates. The management options in the administration portal do not replace the setup that you need to complete during installation. After installation is completed, use the web administration portal for management when possible. Only use the configuration utility if the administration portal is not available or for troubleshooting purposes.

Before you begin

- You must have the Security Administrator role to access certificate management options. For more information, see the “LDAP configuration” section in *Deploying Avaya Multimedia Messaging*.
- In a cluster environment, ensure that all nodes in the cluster are running.

Procedure

1. On the Avaya Multimedia Messaging web administration portal, click **Certificate Management**.
2. Click the appropriate tab.

The procedures below describe the tasks you can perform on each tab.

Managing System Manager certificates

About this task

Use this procedure to manage System Manager security identity certificates.

Procedure

1. Click the **SMGR Certificates** tab.

The **System Manager Address**, **System Manager HTTPS Port**, and **Common Name** fields are automatically populated and cannot be modified from the Avaya Multimedia Messaging web administration portal. You can use the Avaya Multimedia Messaging configuration utility to modify this information if required. The configuration utility is described in *Deploying Avaya Multimedia Messaging*.

2. In the **Node Address** drop-down menu, do one of the following to generate a certificate:
 - Choose a node for a cluster configuration.
If you choose the **All Cluster Nodes** option, certificates will be generated automatically for all cluster nodes.
 - Keep the default setting for a standalone configuration.
3. In **System Manager Enrollment Password**, type the enrollment password as defined on the System Manager web console.

4. Click **Generate Certificates** to start requesting certificates from System Manager.
5. Restart the Avaya Multimedia Messaging system after the certificates are generated.

This completes all the certificate updates. For a cluster environment, only the remote node is restarted.

Managing identity certificates

Procedure

1. Click the **Identity Certificates** tab.
2. Use the following subsections to manage CSRs, keystore data, and server identity certificates.
3. After performing the required task, when prompted, restart the Avaya Multimedia Messaging server for the changes to take effect.

Managing CSRs

Procedure

In the Certificate Signing Requests area, do one of the following:

- To set up a new CSR, click **Create** and then follow the steps in [Creating CSRs](#) on page 51.
- To remove an existing CSR, select it and then click **Delete**.
- To process a signed CSR, click **Process Signing Request**. For more information, see [Processing CA signing requests](#) on page 52.

Creating CSRs

About this task

This procedure provides a high-level overview of how to create CSRs.

Procedure

1. If you clicked **Create** in the Certificate Signing Requests area, complete the following settings in the Create Certificate Signing dialog box and then click **Apply**.

- a. In **Alias**, type an alias using alphanumeric characters.

An example of an alias is `ottawacrt123`.

- b. Complete the other settings as required.

You can use the **Show Advanced Settings** button to view additional settings information. For more information about settings, see [Create Certificate Signing Request screen field descriptions](#) on page 52.

2. Ensure that the CSR file is successfully saved on your computer.

The generated CSR is also added to the Certificate Signing Requests area.

In a cluster configuration, the CSR list on all nodes is identical.

3. **(Optional)** In a cluster environment, if the CSR is not available on a node, click **Propagate** to synchronize requests from the current node to the cluster.

Next steps

Provide the CSR file to the CA for signing and apply the signed CSR as described in [Processing CA signing requests](#) on page 52.

Create Certificate Signing Request screen field descriptions

Name	Description
Alias	The name of the certificate
Common Name	The FQDN of the node. For example, <code>amm.example.com</code> You cannot provide wildcard (*) characters in this field.
Use Existing FQDNs for SAN	Use this option to select a particular node in a cluster for which a certificate should be generated. You can also select all cluster nodes.
Specify SAN manually	Use this option to manually specify additional FQDNs or IP addresses for which the certificate should be generated.
Subject Alternative Name	An optional text field that can be used to further identify this certificate. You can provide multiple entries in this field. You cannot provide wildcard (*) characters in this field.
Key Bit Length	The certificate key length in bits.
Signature Algorithm	The hash algorithms to be used with the RSA signature algorithm.
Organizational Unit	The group within the company or organization creating the certificate.
Organization	The name of the company or organization creating the certificate.
City/Locality Name	The city where the certificate is being created.
State/Province Name	The state/province where the certificate is being created.
Country (ISO 3166)	The name of the country within which the certificate is being created in the ISO 3166 format. For more information about the format, see ISO 3166 country codes .

Processing CA signing requests

Procedure

1. Use the appropriate CA documentation to sign the signing request with the CA.
2. In the Certificate Signing Request area, select the appropriate signing request and then click **Process Signing Requests**.
3. In the Process Signing Request dialog box, click **Choose file** to add the signed certificate and then click **Apply**.

Result

The signed certificate is removed from the Certificate Signing Requests area and added to the Keystore area.

Managing keystore data

Procedure

In the Keystore area, do one of the following:

- To import keystore data, click **Import** and then perform [Importing keystore data](#) on page 53.
- To export a certificate in the PKCS12 format, select a keystore file and then click **Export**.

In the Export Certificate dialog box, you can enter a password to protect your exported file.

- To view details about a keystore file, click **Details**.
- To remove an existing keystore file, select it and then click **Delete**.

Importing keystore data

Procedure

If you clicked **Import**, complete the following settings in the Import Certificate dialog box and then click **Apply**.

1. In the **Certificate Type** drop-down menu, select a format for importing the certificate.
2. From **Certificate File**, click **Choose file** to add the certificate file in the selected format.
3. If you selected the PEM format, in **Key File**, click **Choose file** to add the key file in the PEM format.
4. If you selected the PKCS12 format, in **Password**, type the password for the imported certificate.
5. In **Alias**, type an alias to be used for the imported certificate.

Managing server interface certificates

Procedure

1. Navigate to the Server Interfaces area.
2. In a cluster environment, select the node to administer from the **Node Address** list.
3. Do one of the following:
 - To assign the certificate to a specific server interface, click **Assign** and then complete the settings in the Assign Certificates dialog box as described in [Certificate assignment descriptions](#) on page 54.

If the certificate was assigned only to a selected node, then services on that node need to be restarted to apply the change. If the assignment applies to an entire cluster, then you must restart all nodes in the cluster.

- To view details about the certificate, click **Details**.
- To export the certificate in the PKCS12 format, click **Export**.

Certificate assignment descriptions

Name	Description
Application	Specifies the interface for REST API to the clients.
Internal	Specifies the interface being used for server-to-server component communication.
OAM	Specifies the Operations, Administration, and Maintenance (OAM) interface.
LYNC	Specifies the Lync interface.

Managing truststore certificates

About this task

Use this procedure to manage truststore certificates available on the Avaya Multimedia Messaging system.

Procedure

1. Click the **Truststore** tab.
2. In the Truststore area, select a certificate and then click one of the following:

- **Import:** To import a certificate in PEM or PKCS12 format.

If the file imported into the truststore contains multiple certificates, then all CA certificates from the file will be imported. Alias names, other than the first certificate in the chain, are appended with the suffix `_<x>`, where `<x>` indicates a certificate number, such as 1, 2, or 3.

If a new certificate is imported into the truststore or if any certificate is removed from the truststore, then you must restart the system to apply the change. In a cluster environment, all nodes in the cluster must be restarted.

- **Details:** To view information about the certificate.
- **Delete:** To delete the certificate from the truststore.

Important:

After you remove a certificate from the truststore, restart the Avaya Multimedia Messaging system to apply certificate updates. For a cluster configuration, restart the remote node.

- **Export:** To export the certificate in the PEM format.

Importing the secure LDAP certificate using the web administration portal

About this task

For secure connectivity to LDAP servers, you must import an LDAP certificate file to the Tomcat trust store. The following procedure describes how to import the LDAP certificate using the Avaya Multimedia Messaging web administration portal.

Before you begin

Ensure that the FQDN that is configured as the address of the LDAP source is defined in one of the following places:

- The Common Name in the Subject field.
- Subject Alternative Name.

You can use the following `openssl` command in the Avaya Multimedia Messaging CLI to verify the certificate content:

```
openssl s_client -connect <ldap server:port> | openssl x509 -noout -text
```

Procedure

1. On the Avaya Multimedia Messaging web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
2. Select the **Secure LDAP** check box.
3. Click **Import Certificate**.
4. In the Import Certificate window, click **Choose File** and select the certificate from your local system.
5. Click **Save**.

The system uploads the certificate to a secure LDAP Server. If a certificate is already uploaded, the system overwrites the existing certificate.

Push notification management

The push notification mechanism enables clients to receive incoming call alerts and other notifications from the Apple Push Notification service (APNs). Configuring push notifications on the Avaya Multimedia Messaging web administration portal is part of the push notification configuration procedure. Before configuring push notifications on the Avaya Multimedia Messaging web administration portal, you must create and configure an Avaya Spaces account. You also need to configure settings on Avaya Aura® Session Manager and Avaya Aura® Communication Manager. For more information about the entire configuration procedure, see the sections under [Avaya push notification management](#) on page 69.

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 Avaya Multimedia Messaging*.

Authentication prerequisites

You must have the following to set up IWA:

- An Active Directory server.

 Note:

Windows authentication is only supported if you are using a single authentication directory. If you are using multiple authentication directories, Windows Authentication is disabled.

- 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](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 56.

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 58.

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 57 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.	<code>amm.example.com</code>
<Domain user login>	The Windows login ID for the domain user you created.	<code>amm_user</code>
<Kerberos realm>	The domain name for the Kerberos realm. The Kerberos realm is always the uppercase equivalent of the DNS domain name.	<code>EXAMPLE.COM</code>

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 59 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 adaptor administration and management

You can use a multisite adaptor 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 adaptor only runs on one node in a cluster. Each multisite adaptor 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 adaptor

The multisite adaptor uses the following types of connectors:

Conversation ID connector

The adaptor 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 adaptor 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 adaptor creates a separate connector to request the message parts from the remote site. After the adaptor 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 adaptor 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 entity 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.

Forcing the user synchronization process

About this task

The automatic user synchronization process is not run immediately after the user's home site ID is changed in System Manager. So you might need to wait up to 90 minutes before the changes are applied on Avaya Multimedia Messaging. Use this procedure if you want to force the synchronization process and apply changes immediately.

Note:

If you want to apply changes immediately on all sites, perform this procedure for each Avaya Multimedia Messaging site.

Procedure

1. On System Manager, perform force repair synchronization with Avaya Multimedia Messaging from the Synchronization screen.
2. On Avaya Multimedia Messaging, force LDAP synchronization from the LDAP screen.

For more information, see [Updating enterprise directory settings](#) on page 45.

Multisite adaptor field descriptions

The multisite adaptor is configured for every Avaya Multimedia Messaging site. The adaptor 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 48.

The following table describes the multisite adaptor 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 adaptor is 8441.
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 <code>yes</code> . If the checkbox is not selected, no connector is created and the interface displays <code>no</code> .
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.

As of Release 3.3, Avaya Multimedia Messaging supports partitioning version 2.0 only. For information about disk volume sizes on partitioning version 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.

Before you begin

- Ensure that the system layer on the virtual machine has been upgraded to the current release. 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 volmgt --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 volmgt --extend <volume> <x>m
sys volmgt --extend <volume> <x>g
sys volmgt --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 command 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: Avaya push notification management

Push notifications

The push notification mechanism enables clients to receive incoming call alerts and other notifications from the Apple Push Notification service (APNs). The push notification service sends notifications automatically. Therefore, an application can receive notifications even when it is suspended or in Sleep mode.

The Avaya Multimedia Messaging can send push notifications about incoming messages. For telephony-related events, such as incoming call notifications or voice mail status update, use push notifications on the Avaya Aura® Web Gateway.

Push notification provider

Avaya Multimedia Messaging interacts with the APNs through a push notification provider. You must register your Avaya Multimedia Messaging system with the push notification provider before activating push notifications. The default provider is the Avaya Push Notification provider, which must be used to support push notifications for Avaya Equinox® for iOS. If you want to use push notifications for third-party Avaya Breeze Client SDK-based iOS applications, you must use a third-party push notification provider.

For the Avaya Push Notification Provider, you must create and configure an Avaya Cloud account. This account is used to store the data required to authorize your Avaya Multimedia Messaging system. This account requirement does not apply if you are working with a third-party provider.

Checklist for push notification service configuration

Use this checklist to set up the push notification service for your iOS applications.

Depending on whether you are planning to work with the default Avaya Push Notification provider or a third-party push notification provider, the task you perform are slightly different.

No.	Task	Notes	✓
1	Set up an Avaya Cloud account.	See Avaya Cloud account configuration on page 71.	

No.	Task	Notes	✓
		This step is not required for third-party notification providers.	
2	Configure the third-party push notification provider.	See the requirements in Third-party push notification provider requirements on page 70. This step is not required if you are working with the Avaya Push Notification provider.	
3	Configure your enterprise network firewall.	See Firewall configuration on page 72.	
4	Configure the push notification provider on Avaya Multimedia Messaging.	- If you are working with the Avaya Push Notification provider, see Configuring the Avaya Push Notification provider on Avaya Multimedia Messaging on page 72. - If you are working with a third-party push notification provider, see Configuring a third-party push notification provider on Avaya Multimedia Messaging on page 74.	
5	Configure push notifications for mobile applications.	See Configuring mobile application settings on page 77.	
6	Set the parameters to enable push notifications on iOS applications.	See Configuration parameters for iOS applications on page 78. To enable push notifications in iOS applications, you must configure the required parameters using Avaya Aura® Device Services or a settings file. Avaya Aura® Device Services is the recommended option if it is available in your deployment.	

Third-party push notification provider requirements

By default, Avaya Multimedia Messaging uses the Avaya Push Notification provider for Avaya clients, such as Avaya Equinox® for iOS. If you are planning to use push notifications for third-party Avaya Breeze Client SDK-based iOS applications, you must use a third-party provider, for example, developed by the iOS application developer. This provider must implement the following APIs:

- Interface with the Apple Push Notification service (APNs). Implementation of this interface ensures that the APNs trusts the third-party push notification provider to send notifications to

Avaya clients. For more information about implementing the interface and the APIs required by the APNs, see [APNs Overview](#).

- Interface with Avaya Aura® servers. The third-party push notification provider must trust Avaya Multimedia Messaging to receive push notifications from it. Avaya Multimedia Messaging uses the OAuth-based API for authentication. For more information about the APIs, see [Avaya Breeze® Client SDK](#).

Currently, the existing third-party push notification providers do not support Avaya APIs.

Avaya Cloud account configuration

If you are planning to use the Avaya Push Notification provider, you need to create and configure an Avaya Cloud account. This account stores parameters required to authorize your Avaya Multimedia Messaging system.

Use the following sections to create and configure your Avaya Cloud account.

Avaya Cloud account registration

To create an Avaya Cloud account, see [Signing Up for Avaya Cloud Account](#). If you want to use your Avaya Cloud account for push notification management only and do not want to use other Avaya Cloud features, you can choose the Essential plan, which is free of charge.

Company domain provisioning

You must provide the company domain associated with your Avaya Multimedia Messaging system. To add the company domain, follow the steps in “Creating a Company and Domain” at [Configuring Spaces](#).

Adding the Avaya Mobile Push Notification Service to a company profile on your Avaya Cloud account

About this task

To activate the push notification service for Avaya Multimedia Messaging, you must add the Avaya Mobile Push Notification Service application to your company profile on the Avaya Cloud account.

Procedure

1. Log in to your Avaya Cloud account and navigate to **Manage Companies**.
2. Select the required company and navigate to the **Apps** tab.
3. Click **Configure New App**.

4. From the **Product** drop-down list, select **Avaya Mobile Push Notification Service**.
5. Click **Save**.

Firewall configuration

Avaya Aura® Web Gateway communicates with the Avaya Push Notification provider cloud service using HTTPS. To use the Avaya Push Notification provider, your enterprise network firewall and the HTTP proxy server must allow outbound HTTPS connections to the Avaya Push Notification provider address, which is `apnp.avaya.com:443`.

For applications other than Avaya Equinox® for iOS, you must use a third-party provider. The firewall and the HTTP proxy of your enterprise must allow outbound HTTPS connections to this push notification provider.

For iOS devices running in your enterprise network, Apple push notifications rely on connectivity between iOS devices and the Apple Push Notification service network. For more information about port configuration required to receive Apple push notifications, see <https://support.apple.com/en-us/ht203609>

Configuring the Avaya Push Notification provider on Avaya Multimedia Messaging

About this task

To use the Avaya Push Notification provider, you must generate authorization data and export this data to your Avaya Cloud account. You cannot edit other provider data, such as the name or address, and you cannot delete the Avaya Push Notification provider from Avaya Multimedia Messaging.

For a cluster, perform this procedure once, regardless of the number of nodes in the cluster.

Before you begin

- Create and configure an Avaya Cloud account.
- Install the public certificate of the push notification provider on Avaya Multimedia Messaging. For more information, see [Managing truststore certificates](#) on page 54.

Procedure

1. On the Avaya Multimedia Messaging web administration portal, navigate to **Push Notification Settings > Provider Settings**.
2. From **Push Notification Provider**, select **Avaya Provider**.
3. In **Enter Company Domain**, enter your company domain.

You must enter the same company domain that you provided in your Avaya Cloud account.

4. Click **Generate Key**.

The Avaya Multimedia Messaging generates a public and private key pair and an identifier. This data is required to authorize Avaya Multimedia Messaging on the push notification provider. The Avaya Multimedia Messaging also updates the following values:

- **System Id:** A unique identifier for your system.
- **Public Key:** A public key.

5. Click **Export**.

Avaya Multimedia Messaging displays a pop-up window with the authorization information in JSON format. You must provide this data to your Avaya Cloud account.

The following is an example of the authorization data:

```
{
  "systemId": "9bf8f4ab-99b1-452b-9b7f-e75aacf31d19.mycompany.com",
  "description": "Avaya Multimedia Messaging",
  "publicKey": "-----BEGIN PUBLIC KEY-----
\nMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE9rtz4fuYhGm2JlvnI6lZmate8eEX
\na4wvmklSdHGYZHos7y8xNBNCej9wc3klayOKHYIVieL0ryVFgM16Ud5FDQ==\n-----END PUBLIC
KEY-----",
  "alg": "ES256"
}
```

 Important:

- Do *not* close the Provider Settings page on the Avaya Multimedia Messaging administration portal while you are exporting authorization data to your Avaya Cloud account.
 - Do *not* save the data you provided on the Provider Settings page of the Avaya Multimedia Messaging administration portal until you export authorization data to your Avaya Cloud account. Otherwise, the push notification service might not work as expected.
6. Copy the authorization data, including the surrounding curly brackets, and save it in a file on your computer.
 7. In a new browser tab, log in to your Avaya Cloud account and navigate to **Manage Companies**.
 8. Select the required company and navigate to the **Apps** tab.
 9. From the **App** list, select **Avaya Mobile Push Notification Service**.
 10. Replace the content in **Public Settings** with the content of the file that you created in step 6 and then save your changes.

 Note:

- The Avaya Cloud account stores authorization data internally. **Public Settings** only displays the authorization data that you entered last. You will not lose any previously entered authorization data if you overwrite existing content with the new authorization data.

- Ensure that the authorization data you enter in **Public Settings** is a valid JSON string. If the data uses an invalid format, the Avaya Cloud account displays a warning message, but still allows you to save changes.
11. Return to the Provider Settings page on the Avaya Multimedia Messaging administration portal.
 12. Click **Test** to verify that your system can connect and authenticate with the push notification provider.
 13. Do one of the following:
 - If the verification completed successfully, click **Save**.
 - If the verification failed, fix the issue as described in “Avaya Multimedia Messaging cannot connect to a push notification provider” in *Troubleshooting Avaya Multimedia Messaging* and then re-run the connection test.
- If the problem persists, contact Avaya support personnel.

Configuring a third-party push notification provider on Avaya Multimedia Messaging

About this task

To use push notifications on third-party iOS applications, you require a third-party push notification provider. An Avaya Breeze Client SDK application developer can implement a third-party push notification provider. Use this procedure to set up or update a third-party push notification provider on Avaya Multimedia Messaging.

Before you begin

A third-party Avaya Breeze Client SDK application developer must implement the third-party push notification provider. For more information about push notification provider requirements, see [Third-party push notification provider requirements](#) on page 70.

Procedure

1. On the Avaya Multimedia Messaging web administration portal, navigate to **Push Notification Settings > Provider Settings**.
2. Do one of the following:
 - To add a new provider configuration, click **Add**.
 - To edit an existing provider, select the required provider from **Push Notification Provider** and then click **Edit**.
3. In **Enter Company Domain**, enter the domain where your Avaya Multimedia Messaging is deployed.

For example: `mycompany.com`

4. In **Push Notification Provider Name**, enter a name for the provider.

For example: `MyPushNotificationProvider`.

This name is used in the Avaya Multimedia Messaging administration portal for display purposes only.

5. In **Push Notification Provider Address**, enter the FQDN where your push notification provider is deployed.

For example: `mypushnotifications.mycompany.com`

6. In **Push Notification Provider Port**, enter the port number for the push notification provider.

The default port is 443.

7. Click **Generate Key**.

The Avaya Multimedia Messaging generates a public and private key pair and an identifier. This data is required to authorize Avaya Multimedia Messaging on the push notification provider. The Avaya Multimedia Messaging also updates the following values:

- **System Id**: A unique identifier for your system.
- **Public Key**: A public key.

8. Click **Export**.

Avaya Multimedia Messaging displays a pop-up window with the authorization data in JSON format.

The following is an example of the authorization data:

```
{
  "systemId": "9bf8f4ab-99b1-452b-9b7f-e75aacf31d19.mycompany.com",
  "description": "Avaya Multimedia Messaging",
  "publicKey": "-----BEGIN PUBLIC KEY-----
\nMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE9rtz4fuYhGm2JlvnI6lZmate8eEX
\na4wvmklSdHGYZHos7y8xNBNCej9wc3klayOKHYIVieL0ryVFgM16Ud5FDQ==\n-----END PUBLIC
KEY-----",
  "alg": "ES256"
}
```

Important:

- Do *not* close the Provider Settings page on the Avaya Multimedia Messaging administration portal while you are exporting authorization data to your push notification provider.
 - Do *not* save the data you provided on the Provider Settings page of the Avaya Multimedia Messaging administration portal until you export authorization data to your push notification portal. Otherwise, the push notification service might not work as expected.
9. Copy the system ID and public key data and provide it to your push notification provider.

For example:

```
"systemId": "9bf8f4ab-99b1-452b-9b7f-e75aacf31d19.mycompany.com"
"publicKey": "-----BEGIN PUBLIC KEY-----
\nMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE9rtz4fuYhGm2JlvnI6lZmate8eEX
\na4wvmklSdHGYZHos7y8xNBNCej9wc3klayOKHYIVieL0ryVFgM16Ud5FDQ==\n-----END PUBLIC
KEY-----"
```

The steps you must perform to provide authorization data are provider-specific. For more information, contact your third-party push notification provider vendor.

10. Return to the Provider Settings page on the Avaya Multimedia Messaging administration portal.
11. Click **Test** to verify that your system can connect and authenticate with the push notification provider.
12. Do one of the following:
 - If the verification completed successfully, click **Save**.
 - If the verification failed, fix the issue as described in “Avaya Multimedia Messaging cannot connect to a push notification provider” in *Troubleshooting Avaya Multimedia Messaging* and then re-run the connection test.

If the problem persists, contact Avaya support personnel.

Related links

[Removing a third-party push notification provider](#) on page 76

Removing a third-party push notification provider

About this task

Use this procedure to remove the configuration for a third-party push notification provider from Avaya Multimedia Messaging. You can only remove a provider that is not used by any mobile applications. You cannot remove the default, built-in Avaya Push Notification provider.

Procedure

1. On the Avaya Multimedia Messaging web administration portal, navigate to **Push Notification Settings > Provider Settings**.
2. In **Push Notification Provider**, select the required provider.
3. Click **Remove** and then click **Yes** in the confirmation window.

Related links

[Configuring a third-party push notification provider on Avaya Multimedia Messaging](#) on page 74

Configuring mobile application settings

About this task

Use this procedure to configure push notifications for an iOS application.

For third-party iOS applications, you must provide information about the application and select the required third-party push notification provider.

Avaya Multimedia Messaging already contains configuration data for Avaya Equinox® for iOS. You only need to select the amount of information notification messages will contain and to test that Avaya Equinox® for iOS can receive notifications from the Avaya Push Notification provider. You cannot remove Avaya Equinox® for iOS configuration data from the system.

Important:

You must use the Avaya Push Notification provider for Avaya applications, such as Avaya Equinox® for iOS.

Before you begin

Configure a push notification provider on Avaya Multimedia Messaging. For more information, see [Configuring the Avaya Push Notification provider on Avaya Multimedia Messaging](#) on page 72 and [Configuring a third-party push notification provider on Avaya Multimedia Messaging](#) on page 74.

Procedure

1. On the Avaya Multimedia Messaging web administration portal, navigate to **Push Notification Settings > Mobile Application Settings**.
2. Do one of the following:
 - To create a new mobile application configuration, click **Add**.
 - To edit the settings for an existing configuration, from **Application Name**, select the required application and then click **Edit**.
3. In **Application Name**, provide an appropriate application name.
4. In **Application Id**, provide the iOS application bundle identification string.
Each application must have a unique identification string.
5. In **Push Notification Provider**, select the required push notification provider.
6. In **Message Content Restriction**, select one of the following options to specify the amount of information that is provided when an iOS application receives a push notification:
 - **Highly Restricted**: The application indicates that you have a new message. No other message detail is displayed.
 - **Restricted**: The application displays the message subject, sender, and, if the message contains an attachment, the attachment type. It will not display the message text.
 - **Unrestricted**: The application displays the message text and information about the subject, sender, and, if the message contains an attachment, the attachment type. This is the recommended option.

7. To verify that the Avaya Multimedia Messaging can send notifications to the mobile application, click **Test**.
8. Do one of the following:
 - If the verification completed successfully, click **Save**.
 - If the verification failed, fix the issue as described in “iOS application cannot connect to a push notification provider” in *Troubleshooting Avaya Multimedia Messaging* and then re-run the connection test.

If the problem persists, contact Avaya support personnel.

Related links

[Disabling push notifications](#) on page 78

Disabling push notifications

About this task

Use this procedure to disable push notifications for a specific application. You cannot delete the pre-defined configuration for Avaya Equinox® for iOS.

Procedure

1. On the Avaya Multimedia Messaging web administration portal, navigate to **Push Notification Settings > Mobile Application Settings**.
2. In the **Application** field, select the required mobile application.
3. Click **Remove** and then click **Yes** to confirm.

Related links

[Configuring mobile application settings](#) on page 77

Configuration parameters for iOS applications

To enable the use of push notifications on iOS applications, you must provide the ESM_PUSH_NOTIFICATION_ENABLED parameter to iOS applications using an automatic device configuration service. This parameter is used to enable or disable push notifications. To enable push notifications, set the parameter to 1. To disable push notifications, set the parameter to 0.

You can use one of the following methods to configure this parameter:

- Import the parameter to the Dynamic Configuration service on Avaya Aura® Device Services using the `dynamicConfigUpload.txt` file. For more information, see “Administration of the Dynamic Configuration service” in *Administering Avaya Aura® Device Services*.
- Use the `46xxsettings.txt` configuration file to push the parameter to clients.

The Dynamic Configuration service is the recommended method. Use this option if Avaya Aura[®] Device Services is available in your deployment.

Chapter 9: AWS-specific management options

If you deployed Avaya Multimedia Messaging in an Amazon Web Services (AWS) environment, use the following sections to perform AWS-specific management operations. You can perform these management operations anytime.

Increasing the size of an AWS disk volume

About this task

Use this procedure to add additional storage to the system by increasing the size of an attached disk and then allocating the free space to volumes on the disk. You cannot decrease the size of a disk.

Procedure

1. On the Amazon Web Services console, navigate to **Services > Compute**, and then click **EC2**.
2. On the EC2 Management Console page, click **Instances**.
3. Select the instance to which you want to add storage.
The system displays instance details.
4. Click the **Description** tab.
5. In the **Block devices** field, select a disk for which you want to increase the size:

The options are:

- disk1
- disk2
- disk3
- disk4

For more information about disk options, see [Block device descriptions](#) on page 81.

6. In the **EBS ID** field, click the ID.

The system displays the Volumes page with only the selected device.

7. To update the storage on the EBS disk volume, click **Actions > Modify Volume**.
8. In the Modify Volume window, in the **Size** field, enter the required disk size.
9. Click **Modify**.
10. In the Confirmation window, click **Yes**.
11. In the status window, click **Close**.
12. Log in to the system using the SSH console or PuTTY.
13. If you added storage to disk1, restart the system for the changes to take effect.

A restart is not required when increasing the size of the other disks.

14. To use the newly allocated space, update the file system by running the following commands:

- a. `sys volmgt --summary`: To view the current disk space allocation for each volume.

The order of block devices shown on the EC2 management console might not match the order of the devices shown in the summary tool output. Reference the devices by name and not by their display order.

- b. `sys volmgt --scan`: To scan the disks for newly allocated space.

 Important:

If prompted, restart your system before continuing.

- c. `sys volmgt --extend [ <n>m | <n>g | <n>t | --remaining ]`: To assign unallocated disk space to the volumes on a disk, specifying the amount of space you want to add to each volume. Repeat this step for each volume that you want to extend.

For example, to extend the size of the `/var/log/Avaya` volume on disk1 by 10 GiB, run the `\sys volmgt --extend /var/log/Avaya 10g` command.

For more information, run the `sys volmgt --hhelp` command.

- d. `sys volmgt --summary`: To review the disk space allocation for each volume after the changes are made.

Block device descriptions

Block device on AWS	Disk number	Description
/dev/sda1	disk1	Stores operating system and application software.
/dev/xvdb	disk2	Stores application logs.
/dev/xvdb	disk3	Stores application data.
/dev/xvdd	disk4	Stores database commit logs.

Updating an existing stack with a new CloudFormation template

About this task

You can apply changes to an existing CloudFormation stack by updating the stack with a newer CloudFormation template. Changes to the stack can include additional nodes, new resources, and new port configuration. The system updates all the objects contained in the stack to match the new settings. Existing EBS volumes and S3 buckets are preserved.

To update an existing single-node stack you must use a new single-node stack template. To update an existing cluster you must use a new multi-node stack template. If you are expanding a cluster, you must already have a cluster with two or more nodes. You cannot expand a single AWS node into an AWS cluster.

Before you begin

Generate a new CloudFormation template that matches the application and profile of the existing system but includes the additional resources required. For more information about generating CloudFormation templates, see the “Creating CloudFormation templates” section in *Deploying Avaya Multimedia Messaging*.

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Navigate to **Services > Management Tools > CloudFormation**.
3. Select the stack to update.
4. Click **Actions > Update Stacks**.
5. Update the stack using the Update Stack pages.

You can add an additional CIDR block when going from two to three subnets. Do not change the value of any other stack parameters.

Deleting a CloudFormation stack

Procedure

1. Sign in to the AWS console and click **Services > Management Tools > CloudFormation**.
2. On the CloudFormation page, select a stack to delete.
3. Click **Actions > Delete Stack**.
4. Click **Yes, Delete** when prompted.

The AMI virtual machines and other resources that are in the stack are deleted.

 Note:

The stack is not completely deleted if it includes Amazon Route 53. See the next step for information about resolving this issue.

5. **(Optional)** If deleting the stack fails due to the presence of an Amazon Route 53 DNS zone, then do the following:
 - a. Navigate to **Services > Networking & Content Delivery > Route 53 > Hosted zones**.
 - b. Select the Hosted Zone that is no longer required and click **Delete Hosted Zone**.
 - c. Click **Confirm**.
 - d. Navigate to **Services > Management Tools > CloudFormation**.
 - e. Select the stack that previously failed to delete.
 - f. Click **Actions > Delete Stack**.
 - g. Click **Yes, Delete**.

Chapter 10: 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 for whom 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/<cassandra_version>/bin/csa-  
nodetool.sh repair
```

This example contains a crontab configuration that runs the `csa-nodetool.sh` utility 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.

`<cassandra_version>` represents the version of 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/` directory. 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 1: 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	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.	
avAMMVirtuaIPAcquiredFromPrimary	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 if Avaya Multimedia Messaging is deployed as a software-only application

About this task

Use this procedure to prevent the creation of audit audispd logs while installing Avaya Multimedia Messaging as a software-only application on your own RHEL 7.3 physical servers or virtual machines. This procedure does not apply to Avaya-provided 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 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 `.pcap` support for Wireshark reading.

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

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 Avaya-provided 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=
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=
Trust Chain:      .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 if Avaya Multimedia Messaging is deployed as a software-only application

About this task

The EASG is not installed automatically when you deploy Avaya Multimedia Messaging as a software-only application on your own RHEL 7.3 physical servers or virtual machines. Use this procedure to install and enable the EASG if Avaya Multimedia Messaging is deployed as a software-only application. 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 Avaya-provided OVA deployment process to reinstall EASG. If Avaya Multimedia Messaging is deployed as a software-only application on your own RHEL 7.3 physical servers or virtual machines, 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 11: 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 12: Backup and restore

You can perform backups in a standalone or cluster environment. 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.

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 do not perform the backup during busy periods.

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

- 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.

Backing up Avaya Multimedia Messaging

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 system.

If you are using a cluster system, you only need to back up multimedia files on the seed node. Database and configuration data are different on each node, but media is the same.

! Important:

- Because media data requires a large amount of space, backing up media can take several hours.
- Store backup files on an external storage location. If you store backup files on the Avaya Multimedia Messaging system, you can lose your backup files if a system malfunction occurs.

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**.

- 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. **(Optional)** If you want to store backup files on an external storage location, create an NFS mount point on each node that points to the external storage location.

For example, to mount the `bigvol` directory of the NFS `nas.example.com` file server under the `/mnt/backup` directory, run the following commands:

```
sudo mkdir /mnt/backup
sudo mount nas.example.com:/bigvol /mnt/backup
```

3. Do the following to back up database and configuration files:
 - a. From the seed node, run the following command:

```
app backup -t -d <path to directory>
```

For more information about command options, see [Backup command options](#) on page 99.

- b. When the script prompts you to back up media files, enter `n` (no).

The script backs up database snapshots and configuration files from each node in the system to a separate `<date>_<hostname>.tar` file and stores these `.tar` files in the specified directory.

4. If Avaya Multimedia Messaging is *not* deployed on AWS, from the seed node, back up media files by running the following command:

```
app backup -m -d <path to directory>
```

! Important:

Skip this step if your Avaya Multimedia Messaging system is deployed on AWS. In an AWS environment, media backups are not required because multimedia files are stored in the S3 storage.

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
<code>-d <path to directory></code>	Sets the parent directory where the backup files are stored.
<code>-t</code>	Creates the backup as a <code>.tar</code> file, not a directory.
<code>-s</code>	Creates a database snapshot on the current node only.
<code>-R</code>	Removes all the existing Cassandra snapshots.
<code>-h</code>	Prints usage options for the <code>backupAMM.sh</code> script.
<code>-C</code>	Excludes configuration files from the backup.
<code>-c</code>	Excludes database files from the backup.
<code>-m</code>	Backs up only the media files.
<code>-n</code>	Backs up only the database snapshot and configuration files from the current node only.
<code>-v</code>	Displays a verbose output for debugging.

Restoring Avaya Multimedia Messaging

Prerequisites for restoring Avaya Multimedia Messaging

Before restoring an Avaya Multimedia Messaging server:

- Perform the Avaya Multimedia Messaging installation, while ensuring that all the prerequisites are present on the system. For more information about the installation process, see *Deploying Avaya Multimedia Messaging*.

When you are restoring a cluster, you must install a seed node first and then other non-seed nodes. For more information about installing a seed node, see “Installing the initial cluster node” in *Deploying Avaya Multimedia Messaging*. For more information about installing non-seed nodes, see “Installing an additional cluster node” in *Deploying Avaya Multimedia Messaging*.

- If you are deploying Avaya Multimedia Messaging on a virtual machine, set the virtual machine CPU and memory settings to the values set on the original virtual machine. For more information, see [Adjusting the memory resource of a virtual machine](#) on page 64 and [Adjusting the CPU resource of a virtual machine](#) on page 65.
- While installing Avaya Multimedia Messaging, set **Enable Cassandra DB initialization** to **n** (no) in the Advanced Configuration area on the Initial Installation Configuration screen.
- If the size of the backed-up `/media/data` directory is greater than the default size, adjust the `/media/data` size to match the media backup size. For more information, see [Increasing the size of a virtual disk](#) on page 66 and [Increasing the size of a disk volume on a virtual machine](#) on page 66.

Restoring Avaya Multimedia Messaging 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

Review [Prerequisites for restoring Avaya Multimedia Messaging](#) on page 100.

Procedure

1. If Avaya Multimedia Messaging is *not* deployed on AWS, after Avaya Multimedia Messaging is installed, run the following command to build a new Gluster file system on the node:

```
/opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/glusterfs/  
glusterInstall.sh <IP>
```

In this command, `<IP>` is the IP address of the node.

! Important:

Skip this step if your Avaya Multimedia Messaging system is deployed on AWS. AWS deployments do not use a Gluster file system.

2. 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>
```

3. Do the following to restore database and configuration files:

- a. Run the following command:

```
app restore <path to a tar file with database and configuration files backup>
```

For example:

```
app restore /home/avaya/backup/backup2014_02_02_ammhost1.tar
```

For more information about command options, see [Restore command options](#) on page 104.

- b. When you are prompted to restore media files, enter n (no).

4. Run the following command to restore media files:

```
app restore -c -C <path to directory with media files backup>
```

5. Run the following command to start the Avaya Multimedia Messaging server:

```
svc amm start
```

Result

After the Avaya Multimedia Messaging restore is complete, the Gluster repair process might still be running in the background. If you want to monitor the Gluster status, see [Monitoring the Gluster repair status](#) on page 104.

Restoring a node from a cluster

About this task

This procedure describes how to restore a single non-seed node in an Avaya Multimedia Messaging cluster.

If you want to restore a seed node, you must change the seed node first. For more information, see the “Changing the seed node of a cluster” section in *Deploying Avaya Multimedia Messaging*.

Before you begin

- Review [Prerequisites for restoring Avaya Multimedia Messaging](#) on page 100.
- When installing Avaya Multimedia Messaging, set the IP address of the new node to the IP address of the node that must be restored.

*** Note:**

You can run the configuration utility at a later time to modify configuration settings.

Procedure

1. After Avaya Multimedia Messaging is installed, 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>
```

2. From the new node, run the `app restore` command with the path to the backup `.tar` file that was created on the node that must be restored as a parameter.

For example:

```
app restore /home/avaya/backup/backup2014_02_02_ammhost1.tar
```

For more information about command options, see [Restore command options](#) on page 104.

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

The media files must be restored using the Gluster repair procedure.

4. If Avaya Multimedia Messaging is *not* deployed on AWS, from the new node, run the following command to repair the Gluster file system:

```
/opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/glusterfs/glusterFix.sh  
<FixIP> <ExistingIP>
```

In this command, `<FixIP>` is the IP address of the new node, and `<ExistingIP>` is the IP address of any other node that is already in the cluster.

 Note:

You might be prompted to enter the ssh or sudo password.

 Important:

Skip this step if your Avaya Multimedia Messaging system is deployed on AWS. AWS deployments do not use a Gluster file system.

5. From another node in the cluster, set up the SSH RSA public/private keys by running the `configureAMM.sh` script.
6. Run the following command to start the Avaya Multimedia Messaging server:

```
svc amm start
```

7. Run the Cassandra repair command:

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

Result

After the Avaya Multimedia Messaging restore is complete, the Gluster repair process might still be running in the background. If you want to monitor the Gluster status, see [Monitoring the Gluster repair status](#) on page 104.

Restoring a cluster

About this task

Use this procedure to restore the entire Avaya Multimedia Messaging cluster in case of a failure that results in the loss of all nodes.

You must perform this procedure for each node in the cluster on the seed node first and then on all other non-seed nodes.

Before you begin

Review [Prerequisites for restoring Avaya Multimedia Messaging](#) on page 100.

Procedure

1. If Avaya Multimedia Messaging is *not* deployed on AWS, after Avaya Multimedia Messaging is installed, from the seed node, run the following command to build a new Gluster file system:

```
/opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/glusterfs/  
glusterInstall.sh <IP1> <IP2> <...>
```

In this command, <IP1>, <IP2>, and so on are the IP addresses of the nodes in the cluster.

Important:

Skip this step if your Avaya Multimedia Messaging system is deployed on AWS. AWS deployments do not use a Gluster file system.

2. From the seed node, set up the SSH RSA public/private keys by running the `configureAMM.sh` script.
3. Do the following to restore database and configuration files:
 - a. From each node in the cluster, run the `app restore` command, with the path to the backup file or directory as a parameter.

```
app restore <path to a tar file with database and configuration files backup  
for this node>
```

For more information about command options, see [Restore command options](#) on page 104.

- b. When you are prompted to restore media files, enter `n` (no).
4. From the seed node, run the following command to restore media files:

```
app restore -c -C <path to directory with media files backup>
```

5. After all the nodes have been restored, run the following command to start the Avaya Multimedia Messaging server:

```
svc amm start
```

6. Run the Cassandra repair command:

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

Result

After the Avaya Multimedia Messaging restore is complete, the Gluster repair process might still be running in the background. If you want to monitor the Gluster status, see [Monitoring the Gluster repair status](#) on page 104.

Restore command options

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

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

Option	Description
-h	Prints usage options for the restore script.
-C	Does not restore configuration files.
-c	Does not restore Cassandra database files.
-r	Removes stale Avaya Multimedia Messaging nodes from the list.
-s	Skips SHA-256 checksum validation.
-S	Displays SHA-256 checksums.

Monitoring the Gluster repair status

About this task

After Avaya Multimedia Messaging is restored, the Gluster file system repair might still be in progress. The repair process continues as a background process and can take several hours to complete.

Procedure

Run the following command to check the status of the Gluster file system repair:

```
sudo gluster volume heal cs_volume statistics
```

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 97.

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 restoring 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

Scenario	Description
	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 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 13: Upgrades and migrations

Migrations are done from Release 3.2 to 3.3, and then you must upgrade to the latest 3.4 release. This document describes the process to upgrade to Release 3.4. The Release 3.3 migration information has been removed from this document. See the Release 3.3.x documentation at <https://support.avaya.com/documents/> if you need to migrate to Release 3.3.

*** Note:**

When you upgrade to Release 3.4, passwords are encrypted. If you roll back to a previous release, then passwords will no longer be encrypted.

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 applies to Avaya-provided OVA and software-only deployments.

*** Note:**

- In a cluster, all the nodes must run the same Avaya Multimedia Messaging version. All nodes must be upgraded before you start the Avaya Multimedia Messaging service.
- 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 application layer upgrade 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 on all nodes, one at a time.

`ucapp-system-3.4.0.0.9.tgz` is an example of a system layer upgrade artifact.

For more information about upgrading the system layer, see [System layer \(OS\) updates for virtual machines deployed using Avaya-provided OVAs](#) on page 116.

Important:

You must finish upgrading the system layer on all nodes before upgrading the application layer.

2. Upgrade the application layer on the seed node first and then on the non-seed nodes, one at a time.

- 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.

 Important:

Wait until the upgrade completes on the current node before starting the upgrade on another node.

3. **(Optional)** To remove the previous Avaya Multimedia Messaging version after an upgrade, run the following command on each node:

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

4. After you finish upgrading all the nodes, start the Avaya Multimedia Messaging service on every node:

```
svc amm start
```

Next steps

If you configured REST XEP-0045 adaptors, delete and re-add them after upgrading Avaya Multimedia Messaging. For more information, see the “Configuring the HTTPS REST interface in Avaya Multimedia Messaging for federation with Presence Services” section in *Deploying Avaya Multimedia Messaging*.

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.

 Important:

In a cluster environment, perform the rollback operation on non-seed nodes first. After this is complete, perform the rollback operation on the seed node.

 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:

```
svc amm 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 adaptor.

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 adaptor to the REST adaptor.

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 Presence Services 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 host name, 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 **Adaptor 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 a protocol.

 Note:

The current release supports XEP-0033 and XEP-0045 protocols.

- 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 14: System layer (OS) updates for virtual machines deployed using Avaya-provided OVAs

Each VMware or AWS virtual machine that is created by deploying the Avaya Multimedia Messaging OVA file has a system layer (operating system). The system layer 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 virtual machines. Only use update artifacts provided by Avaya.

This section only applies to systems deployed in VMware or AWS virtual environments using Avaya-provided OVAs. As the customer, you are responsible for updating the operating system when Avaya Multimedia Messaging is installed as a software-only application onto your own RHEL physical servers or virtual machines, 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 administrative account of the server to be updated, using standard file transfer methods, such as SFTP or SCP.
3. Log in to the administrative account of the server using SSH
4. To extract the update, use the following command:

```
tar -zxvf ucapp-system-<version>.tgz
```

For example:

```
tar -zxvf ucapp-system-3.3.0.0.9.tgz
```

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

```
cd ucapp-system-<version>
sudo ./update.sh --stage
```

For example:

```
cd ucapp-system-3.3.0.0.9
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-<version>.tgz  
rm -rf ucapp-system-<version>
```

For example:

```
rm ucapp-system-3.3.0.0.9.tgz  
rm -rf ucapp-system-3.3.0.0.9
```

+ Tip:

Avaya recommends 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 15: Resources

Documentation

The following table lists related documentation for Avaya Multimedia Messaging. All Avaya documentation is available at <http://support.avaya.com>. Many documents are also available at <http://documentation.avaya.com/>.

Table 2: Avaya Equinox® and Avaya Multimedia Messaging documentation

Title	Use this document to	Audience
Overview		
<i>Avaya Equinox® Overview and Specification for Android, iOS, Mac, and Windows</i>	Understand high-level product functionality, performance specifications, security, and licensing.	Customers and sales, services, and support personnel
Planning		
<i>Planning for and Administering Avaya Equinox® for Android, iOS, Mac, and Windows</i>	Perform system planning and configuration for: • Avaya Equinox® for Android • Avaya Equinox® for iOS • Avaya Equinox® for Mac • Avaya Equinox® for Windows	• System administrators • Customers and sales, services, and support personnel
<i>Avaya Multimedia Messaging Reference Configuration</i>	Understand technical overview information, system architecture, functional limitations, and capacity and scalability for Avaya Multimedia Messaging.	Customers and sales, services, and support personnel
Implementing		
<i>Deploying Avaya Multimedia Messaging</i>	Install, configure, and administer Avaya Multimedia Messaging.	Implementation personnel
Maintaining		
<i>Updating server certificates to improve end-user security and client user experience</i>	Understand and administer certificates on Avaya Equinox®.	• System administrators • Customers and sales, services, and support personnel
Using		

Title	Use this document to	Audience
<i>Using Avaya Equinox® for Android, iOS, Mac, and Windows</i>	Install and use your Avaya Equinox® client.	Enterprise users
Troubleshooting		
<i>Troubleshooting Avaya Multimedia Messaging</i>	Troubleshoot Avaya Multimedia Messaging.	• System administrators • Customers and sales, services, and support personnel

Table 3: Other related documents

Title	Use this document to:	Audience
Deploying		
<i>Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP</i>	Install and maintain 9601, 9608, 9608G, 9611G, 9621G, and 9641G deskphones.	Implementation engineers, system architects, and administrators.
<i>Configuring GR-unaware elements to work with System Manager Geographic Redundancy</i>	Configure elements that are unaware of Geographic Redundancy to work with Avaya Aura® System Manager	Implementation engineers, system architects, and administrators.
Administering		
<i>Administering Avaya Aura® Session Manager</i>	Administer Avaya Aura® Session Manager	System administrators.
<i>Administering Avaya Aura® Communication Manager</i>	Administer Avaya Aura® Communication Manager	System administrators.
<i>Administering Avaya Aura® Presence Services</i>	Administer Avaya Aura® Presence Services	System administrators.
<i>Administering Avaya Aura® System Manager</i>	Administer Avaya Aura® System Manager	System administration
<i>Administering Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP</i>	Administer 9601, 9608, 9608G, 9611G, 9621G, and 9641G deskphones.	System administrators.
<i>Upgrading and Migrating Avaya Aura® applications from System Manager</i>	Upgrade and migrate Avaya Aura® system.	System administrators.
<i>Avaya Aura® Presence Services Snap-in Reference</i>	Configure the federation between Avaya Multimedia Messaging and Presence Services using HTTP REST.	System administrators.

Finding documents on the Avaya Support website

Procedure

1. Go to <https://support.avaya.com/>.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product > Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at <https://documentation.avaya.com/>.

Important:

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open <https://support.avaya.com/>.

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
 - Type a keyword in the **Search** field.
 - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
 - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

Navigate to the **My Content > My Docs** menu, and do any of the following:

- Create, rename, and delete a collection.

- Add content from various documents to a collection.
- Save a PDF of selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive content that others have shared with you.
- Add yourself as a watcher by using the **Watch** icon (.

Navigate to the **My Content > Watch list** menu, and do the following:

- Set how frequently you want to be notified, starting from every day to every 60 days.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.

- Share a section on social media platforms, such as Facebook, LinkedIn, Twitter, and Google +.
- Send feedback on a section and rate the content.

 Note:

Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

Training

The following courses and tests are available on the Avaya Learning website at <http://www.avaya-learning.com>. After logging in to the website, enter the course code or the course title in the **Search** field and press **Enter** or click **>** to search for the course.

Course code	Course title
3180T	Designing Communications Optimization Solutions Test
5106	Avaya UC Soft Clients Implementation and Maintenance Test

Viewing Avaya Mentor videos

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

About this task

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

Procedure

- To find videos on the Avaya Support website, go to <https://support.avaya.com/> and do one of the following:
 - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
 - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
 - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
 - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

 Note:

Videos are not available for all products.

Support

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

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to <http://www.avaya.com/support>.
2. Log on to the Avaya website with a valid Avaya user ID and password.
The system displays the Avaya Support page.
3. Click **Support by Product > Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

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.
Network Time Protocol (NTP)	A protocol used to synchronize the real-time clock in a computer.
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/ .
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

A

adaptor	
fields	63
adding	
LDAP Server	37
adding to truststore	
Presence Services certificate	113
additional base context DN	42
Adjusting the CPU resource of a virtual machine	65
Adjusting the memory resource of a virtual machine	64
adjusting the size	
disk volumes	66
Adjusting the size of virtual disks	66
Adjusting the virtual hardware of virtual machines	64
Adjusting the virtual network interface	65
administration	
LDAP attribute mappings	49
multisite configuration	48
rollback operations	110
administration portal	
performance	46
administration tools	
cas-nodetool.sh	16
cleanAMM.sh	18
clitool	18
collectlogs	20
gluster volume status	16
Administrator responsibilities	13
archiving	105
audit audispd logs	88
Avaya Cloud	
configuring account	71
provisioning company domain	71
Avaya Push Notification provider	
configuring	72
Avaya support website support	124
AWS-specific management options	80

B

backup and restore	97
backup command options	99
backup of a node	98
restore cluster	103
restore command options	104
restore standalone node	100
Browser requirements for the admin portal	30

C

Cassandra database	
administration tools	16

certificate signing request	
parameter description	52
checklist	
push notification configuration	69
cluster	
restore cluster	103
restoring	103
restoring single non-seed node	101
collection	
delete	122
edit name	122
generating PDF	122
sharing content	122
commands	
management	14
system layer	20
command values	
Windows Domain Controller	58
configuration	
active directory	57
external configurations	94
IWA	56 , 57
local site	48
multisite	48
multisite adaptor	61
remote site	48
Windows Domain Controller	57
configure	
message playback login message	95
configuring	
Avaya Push Notification provider settings	72
firewall for push notifications	72
mobile application settings for push notifications	77
third-party push notification provider	74
windows authentication	43
connector	
multisite adaptor	61
content	
publishing PDF output	122
searching	122
sharing	122
watching for updates	122
creating	
Avaya Cloud account	71
CSR	
create	51

D

daily reports	18
Data Replication Service	111 , 114
migration	112
Data Replication Service synchronization	114

deleting a stack		increasing the size (<i>continued</i>)	
CloudFormation	82	disk volume	80
descriptions		InSite Knowledge Base	124
block devices	81	installing EASG	
certificate assignment	54	software-only application	91
disabling		integrated Windows authentication support setup	56
push notifications for mobile application	78	iOS	
Disabling EASG	93	configuring push notifications	69
documentation portal	122	IWA	
finding content	122	active directory	57
navigation	122	administration portal	59
document changes	9	prerequisites	56
Downloading system layer	117	Windows Domain Controller setup	57
E		K	
enabling		keystore data	53
enhanced access security gateway after OVA		L	
deployment	89	latest software patches	108
enabling EASG		LDAP configuration	
software-only application	91	importing secure LDAP certificate	55
enterprise directory settings	45	LDAP server	
Enterprise LDAP Server Configuration		overview	36
field descriptions	37	LDAP Server	
extracting system layer	117	adding	37
F		logging levels	48
feature entitlements	34	logs and alarms	85
federation connections	45	Lync	
federation settings	45	recovery	106
field descriptions		M	
application properties	32	Management	
cluster nodes	46	AMM	
feature entitlements	35	admin portal	30
finding content on documentation portal	122	Management of AMM with the administration portal	30
firewall		management tools and commands	14
configuring for push notifications	72	manage storage	32
G		managing	
Gluster		application sessions	31
monitoring repairing status	104	client device certificates	33
H		CSRs	51
home site ID		identity certificates	51
multisite needs to review from an intadaptor	62	messaging domains	33
updating in multisite deployment	62	server interface certificates	53
I		System Manager certificates	50
importing		truststore certificates	54
keystore data	53	managing certificates	
importing keystore data	53	web administration portal	50
increasing the size		managing keystore data	53
		messaging domains	
		managing	33
		migration	108
		Avaya Aura environment	111

Index

migration (<i>continued</i>)	
Data Replication Service	112
Presence federation	112
migration from XMPP based	
Presence Services federation	112
migration to REST based	
Presence Services federation	112
mobile application	
disabling push notifications	78
multiple authentication domains	
configuring uid	36
multisite	
port	48
multisite adaptor	
connector	61
fields	63
home site ID	62
My Docs	122

N

New in this release	10
node	
restoring non-seed node	101

O

overview	10
----------------	--------------------

P

patch information	108
performance	46
prerequisites	
IWA	56
restoring AMM	100
Prerequisites for accessing the admin portal	30
Presence federation	
migration	112
Presence Services certificate	
adding to truststore	113
Presence Services federation	
migration from XMPP based	112
migration to REST based	112
preventing	
creation of audit audispd logs	88
processing CA signing requests	52
push notifications	55 , 69
Avaya Cloud account	71
configuration parameters for iOS clients	78
configuring	
Avaya Push Notification provider settings	72
company domain in Avaya Cloud	71
firewall	72
mobile applications settings	77
third-party provider settings	74

configuring (<i>continued</i>)	
creating Avaya Cloud account	71
disabling for mobile application	78
removing provider	76
third-party push notification provider requirements	70

R

recovery	
Lync or Skype for Business	106
related documentation	120
release notes for latest software patches	108
removing	
push notification provider	76
removing EASG	93
replacing	
XMPP with HTTPS REST	113
requirements	
third-party push notification provider	70
restoring	
single non-seed node in cluster	101
restoring AMM	
prerequisites	100
retrieve user conversations	105

S

searching for content	122
secure LDAP certificate	
importing using the web administration portal	55
Server Address and Credentials	
field descriptions	37
setting up	
IWA	59
sharing content	122
Skype for Business	
recovery	106
software-only application	88
software patches	108
staged system layer	119
staging system layer	117
start service	31
statistics	46
stop service	31
storage management	32
support	124
sys	20
sys secconfig	21
sys smcvemgt	26
examples	28
system layer	
secconfig	21
smcvemgt	26 , 28
versions	22
volmgt	22
system layer (OS)	116
system layer commands	20

system update	116
sys versions	22
sys volmgt	22

T

third-party push notification provider	
configuring	74
requirements	70
tools	
management	14
topology	11
components	12
trace-level	
logging messages	89
training	123
troubleshooting	
cluster nodes	46
troubleshooting Cassandra database	
periodic repair of database inconsistencies	84

U

update	
system layer (OS)	116
update entitlements	34
updating an existing stack	
CloudFormation template	82
upgrade	108
restore previous version	111
rollback	111
upgrades	
rolling back to the previous version	110
user synchronization	
forcing	62

V

verify cluster nodes	46
videos	123
virtual hardware	
adjustments	64

W

watch list	122
------------------	---------------------

X

XMPP	
replace with HTTPS REST	113