Deploying 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.

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

Contents

Chapter 1: Introduction

Purpose

This document describes planning, initial setup, and configuration for Avaya Multimedia Messaging. It also provides information about known troubleshooting issues related to deployment.

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 Software-only deployment checklist on page 33. • Updated Removing a node from an Avaya Multimedia Messaging cluster on page 90. • Updated Documentation on page 200. • 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 3.4:

XMPP federation

Avaya Multimedia Messaging has been updated to comply with XEP-0045 specifications, the XMPP protocol extension for multi-user text chat. Not all XEP-0045 features are supported.

Password encryption

For security purposes, Avaya Multimedia Messaging now encrypts stored passwords using the SHA-512 hashing algorithm.

Multiple authentication and authorization domains

Avaya Multimedia Messaging now supports multiple LDAP domains for authentication and authorization. For more information, see Multiple authentication and authorization domains on page 143.

Topology

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

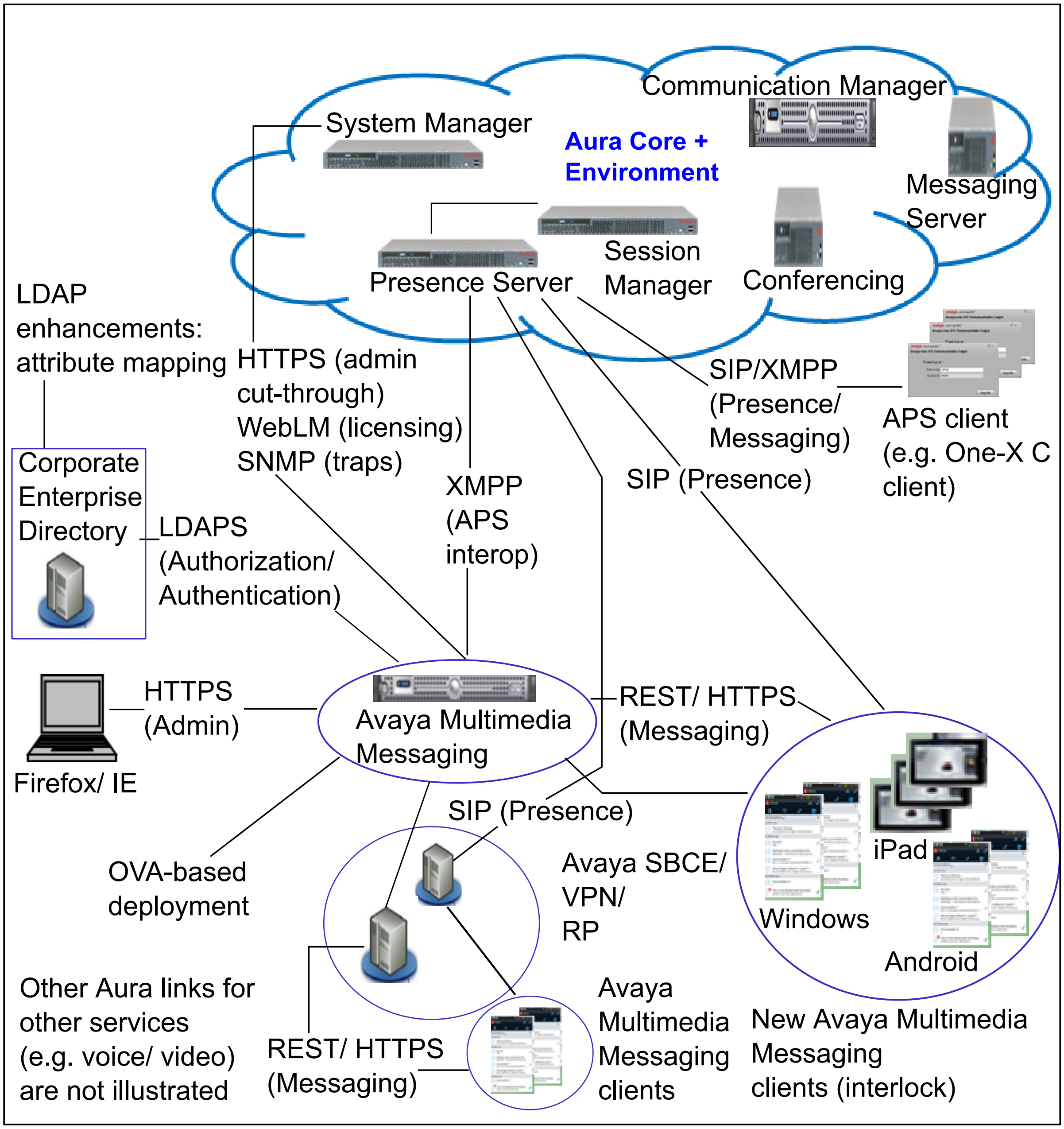


Figure 1: Avaya Multimedia Messaging deployment architecture

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

Chapter 3: Planning and pre-configuration

This chapter describes the planning and pre-configuration that you must perform before installing the Avaya Multimedia Messaging server.

⚠ **Warning:**

When you deploy Avaya Multimedia Messaging, avoid copying and pasting commands directly from this document. This can introduce unwanted characters and errors. Double-check all inputs you copy or type them manually.

Planning and pre-configuration checklist

Table 1: Planning and pre-installation checklist for the Avaya Multimedia Messaging server

Task	Notes	✔
Ensure that you can log in to the Avaya Product Licensing and Delivery System (PLDS) and download software.	Ensure that you have access to PLDS and can download files. Download the Avaya Multimedia Messaging installation file from PLDS. You can access PLDS at http://plds.avaya.com/.	
Obtain the required components.	For more information about the required Avaya Multimedia Messaging components, see Components on page 13.	
Obtain the required licenses.	Avaya Multimedia Messaging software and enhanced user privileges are licensed capabilities. You can obtain licenses using PLDS at http://plds.avaya.com/.	
Ensure your network meets security requirements.	Ensure you understand security requirements and prerequisites for Avaya Multimedia Messaging and other Avaya components.	
Complete required questionnaires.	Fill out the information about the Avaya Multimedia Messaging installation requirements for your deployment in the general questionnaire worksheet.	
Complete site preparation.	Prepare your network so that you can install and connect equipment without costly delays.	

Table continues…

Task	Notes	✔
	Set up the following Avaya Aura® infrastructure components for Avaya Multimedia Messaging: • Avaya Aura® Presence Services • Avaya Aura® Session Manager • Avaya Aura® System Manager To use the Avaya Multimedia Messaging features, users must have a UC application that supports Avaya Multimedia Messaging, such as Avaya Equinox® for iOS.	
If you are using a single authentication directory, ensure that all users are in a single authentication domain. **Note:** This is not required if you are using multiple authentication directories.	The first LDAP domain added to the system is the server that handles user authentication and role assignment. All users that require authentication must be located in this LDAP domain and must be able to authenticate with it.	
Understand required skills and knowledge for Avaya Multimedia Messaging deployments.	Before deploying Avaya Multimedia Messaging, make sure you have all required skills and knowledge defined in this chapter.	

PLDS overview

Avaya Product Licensing and Delivery System (PLDS) provides customers, Avaya Partners, distributors, and Avaya Associates with tools for managing license entitlements and electronic delivery of software and related license files.

Installation software packages for Avaya Multimedia Messaging are available as OVA and binary files on PLDS. Users can download the OVA files or the binary files to a computer, and choose to either burn a DVD for installation or transfer the file to the target server for installation.

You can check PLDS to determine if a later service pack or software release is available. If updates do exist, see the appropriate upgrade procedures, contact Avaya, or contact the Avaya Partner Service representative.

When you place an order for a PLDS-licensed software product, the license entitlements on the order are automatically created in PLDS. When the license entitlements are created, PLDS sends you an email notification. The email notification includes a license activation code (LAC). Using LAC, you can find and activate the newly purchased license entitlements in PLDS. You can then download the license file.

Important:

You must provide the WebLM host ID to activate the license file in PLDS. You can view the WebLM host ID in the WebLM Server Properties page.

Examples of license management tasks that you can perform in PLDS include:

- Adding more license entitlements to an existing activation
- Upgrading a license file to a new major release
- Moving license entitlement activations between license files
- Regenerating a license file with an new host ID

Downloading software from PLDS

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Click the search icon (🔍) for Company Name.
6. In the Search Companies dialog box, do the following:
    a. In the **%Name** field, type `Avaya` or the Partner company name.
    b. Click **Search Companies**.
    c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
    - In **Download Pub ID**, type the download pub ID.
    - In the **Application** field, click the application name.
8. Click **Search Downloads**.
9. Scroll down to the entry for the download file, and click the **Download** link.
10. Select a location where you want to save the file, and click **Save**.
11. **(Optional)** If you receive an error message, click the message, install Active X, and continue with the download.
12. **(Optional)** When the system displays the security warning, click **Install**.

    When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Licensing requirements

Avaya Multimedia Messaging is an entitlement in the Avaya Unified Communications (UC) bundles. Core Suite licenses include Avaya Multimedia Messaging Basic user licenses. Power

Suite licenses include Avaya Multimedia Messaging Enhanced user licenses. You can uplift a Core Suite license to include Avaya Multimedia Messaging Enhanced user licenses. You also require a per server license, which must be purchased separately.

Material codes and pricing are available in *Avaya Multimedia Messaging Offer Definition* at https://sales.avaya.com/cs/Sites?lookuphost=/&lookuppage=/en/pss/avaya-multimedia-messaging&view=collateral. To access this web site, you must log in using your Avaya Customer or Partner credentials.

The following table summarizes the instant messaging features available for Basic users and Enhanced users. You can use the Avaya Multimedia Messaging web administration portal to update user privileges.

Table 2: IM features available for different users

Functionality	Available for Basic users	Available for Enhanced users
Send text-based IMs.	Y	Y
Send generic attachments over IM.	Y, on Windows and Mac clients only. This feature is not available to Basic users on mobile clients.	Y, on all clients.
Receive text-based IMs from other users.	Y	Y
Receive photo, audio, and video attachments from other users over IM.	Y	Y
Capture photo, audio, and video media from the IM window. Avaya Multimedia Messaging also provides guidance on attachment sizes.	N	Y

Note:

When an administrator revokes your enhanced user privileges, you might still be able to capture and send rich media attachments in an IM conversation until you log out of your Avaya Equinox® client. Your basic user entitlements will take effect when you log out and log back in to the client.

Server node license tracking

After you start Avaya Multimedia Messaging, it communicates with the license server to obtain licenses for nodes. As of Release 3.0, license files include the server node feature. When this feature is available, the server tries to acquire the required licenses.

The license server enters a 30-day grace period in the following circumstances:

- The license does not have the server node feature.
- Enough licenses are not available.

The grace period is for the complete license file. During this period, Avaya Multimedia Messaging operations remain uninterrupted.

When licensing errors occur, logs and alarms are raised and the server might also display error messages.

In a cluster environment, only one node, usually the seed node, communicates with the license manager on behalf of all the nodes. For a cluster with one seed node and two child nodes, three licenses are obtained if they are available. If there is an extra node, the license manager is updated when the regular audits occur.

When a service is unavailable, the license for the node is released after approximately 10 minutes.

Security requirements

Before deploying the Avaya Multimedia Messaging server, ensure that the customer security staff reviews and approves the Avaya Multimedia Messaging deployment. This means that customers must engage the expertise of their security staff early in the deployment process. The security staff must incorporate Avaya Multimedia Messaging into their routine maintenance of virus protection, patches, and service packs.

Additional security information

Additional security information for Avaya Multimedia Messaging and Avaya components that integrate with Avaya Multimedia Messaging is available on the Avaya Support web site at http://support.avaya.com/security. For example, you can find information about the following:

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

For US customers: You can also find additional information about security practices at the National Security Agency web site at https://www.nsa.gov/.

Avaya Multimedia Messaging general questionnaire worksheet

Obtain the following general information as part of your site preparation. You must complete this worksheet before deploying the Avaya Multimedia Messaging server.

Information to obtain	Your value	Purpose and how to obtain the information
Approximate number of users		To determine the following: • Whether you need a single server or a cluster. • Storage and disk size or volume requirements. To obtain this value, you must estimate the number of Avaya Equinox® users using Avaya Multimedia Messaging.
LDAP type and version For example: Microsoft Active Directory 2016		To determine the enterprise directory that you can use with Avaya Multimedia Messaging. The LDAP enterprise directory synchronizes user details for messaging and handles user authentication and authorization. To obtain this information, contact your LDAP administrator.
Custom LDAP schema or standard schema		To determine LDAP schema compatibility. If the LDAP schema has custom attributes, contact your LDAP administrator.
External access type (optional) Examples include the following: • VPN • Avaya SBCE • Reverse proxy • None		For Avaya Equinox® clients users to connect to the enterprise network remotely.
Avaya Multimedia Messaging server type The supported Avaya Multimedia Messagingserver types are: • Physical servers or virtual machines (using a VMware host) with your own Red Hat Enterprise Linux (RHEL) operating system. • VMware deployment with an Avaya-provided OVA.		To determine the server allocated for Avaya Multimedia Messaging deployment. The options are: • Deployment on a physical server or VMware virtual machine using your own RHEL operating system. • Deployment on a VMware virtual machine using an Avaya-provided OVA. • Deployment in AWS environment using an Avaya-provided OVA. To obtain this information, contact your IT department.

Table continues…

Information to obtain	Your value	Purpose and how to obtain the information
• Amazon Web Services (AWS) deployment with an Avaya-provided OVA.		❗ **Important:** Avaya recommends deploying the Avaya Multimedia Messaging server on a VMware virtual machine using the Avaya-provided OVA.
Virtualized machine VMware or ESXi version		To determine the version of VMware that your enterprise uses.
Additional instant messaging applications Examples include the following: • Avaya Aura® Presence Services client, such as Avaya one-X® Communicator • Lync or Skype for Business • Other XMPP servers		To determine if you require federation to send and receive IMs from clients without Avaya Multimedia Messaging, such as Avaya one-X® Communicator.
Backup high availability (HA) mechanism for storage		To determine whether the system performs a data backup. This is required if the Avaya Multimedia Messaging file server is on a SAN NAS or NFS system with RAID or other HA provisions.

Prerequisites

Required skills and knowledge

You must have the following skills to install and configure the Avaya Multimedia Messaging server.

- Know how to use a Red Hat Enterprise Linux (RHEL) operating system and basic Linux commands.
- Understand how to install, configure, and use Avaya Aura® System Manager, Avaya Aura® Presence Services, and Avaya Aura® Session Manager.
- Be familiar with LDAP. General information about setting up LDAP is not described in this document. For information about configuring LDAP settings with Avaya Multimedia Messaging, see the chapter LDAP settings configuration on page 136.
- Understand hardware capacity and disk partitioning requirements for your servers before you deploy Avaya Multimedia Messaging.

Server prerequisites

- You must have a server available. You can use a physical server or a virtual machine.

- After installing your own RHEL operating system on a physical server or virtual machine, ensure you modify the `ifcfg-eth0` file and set the ONBOOT parameter to `Yes`. Otherwise, the installation fails during network configuration.

VMware deployments

The supported ESXi versions for Avaya Multimedia Messaging deployments using VMware are 5.5, 6.0, and 6.5.

VMware provides many features and capabilities. Some VMware capabilities require additional configuration. For general information about VMWare functionality, see http://www.vmware.com/. VMware capabilities include the following:

- Customizing for the High Availability (HA) feature

  For information about HA configuration, see the vSphere documentation and the VMware vSphere High Availability Deployment Best Practices document.

- Creating snapshots

  For best practice information, see the Best practices for virtual machine snapshots in the VMware environment page.

- Installing VMware Data Recovery

  For information about using and configuring the Data Recovery feature, see the VMware Data Recovery Admin Guide.

- Installing VMware Site Recovery Manager

  For information about installing and administering the Site Recovery Manager, see the VMware vCenter Site Recovery Manager documentation page.

- Enabling time synchronization for ESXi hosts

  Events such as startup and taking or restoring snapshots synchronize time in the guest operating system, so you must ensure that the time of the host operating system is correct. See the VMware Knowledge Base for details and instructions.

Configuration prerequisites

Before you start installing the Avaya Multimedia Messaging server, you must perform the following configuration tasks:

- Configure the enterprise DNS server to make the required domains reachable
- Configure Avaya Aura® System Manager for user provisioning and connecting to the Avaya Multimedia Messaging server
- Configure the enterprise LDAP server according to the Avaya Multimedia Messaging requirements

Note:

Collect all the information that you need for these configurations by completing the Avaya Multimedia Messaging questionnaires. The questionnaires ensure that you have all the necessary data before you start the Avaya Multimedia Messaging deployment.

Avaya Multimedia Messaging domains configuration

Before you install the Avaya Multimedia Messaging server, you must configure the DNS server to include all the domains required for Avaya Multimedia Messaging.

You must also list the messaging domains as a configuration step during or after the Avaya Multimedia Messaging server installation. For more information, see Messaging Domains Configuration on page 134.

Messaging domains

The list of reachable domains consists of a union of all domains to which Avaya Multimedia Messaging can route messages. This includes the federated remote domains defined for any messaging adaptors as well as a list of messaging domains that applies only to Avaya Multimedia Messaging messages.

- Any configured domain in the list is considered a full domain name literally. No sub-domain should be assumed or derived. For example, configured domain `a.b` means that only domain `a.b` is reachable. It does not imply that sub-domains like `x.a.b` are also reachable.
- The list of reachable domains is checked upon client login. A user ID belonging to a non-reachable Avaya Multimedia Messaging messaging domain would prevent the user from logging in. In other words, A user ID belonging to a non-reachable messaging domain cannot become an Avaya Multimedia Messaging user.
- Having a domain in this list simply means that the domain can be used to send or receive messages but does not guarantee the state of the domain. For example: if the messaging server is not working, no message can be sent, but its remote domain is still listed in the routable domain list.
- An address that belongs to a routable domain does not guarantee that the address is valid. This means that the domain of the address is routable. To verify that the address is valid, the client must make a validateAddress request.
- An address with a domain that is not in the routable domain list can still be validated through a client as long as the address is properly configured.

In general, the client uses the routable domain list to filter the address that Avaya Multimedia Messaging cannot route to, then validate the remaining addresses.

Avaya Multimedia Messaging reachable domains

Presence Services supports multiple domains. With Avaya Multimedia Messaging, you can only send instant messages to Presence Services users with addresses in reachable domains. Some users can only access presence and telephony services. You can put these types of users into an unreachable domain list.

Supported address types

The Avaya Multimedia Messaging server supports the following address types:

- Avaya SIP
- Avaya E.164
- Avaya Presence and IM
- Google Talk
- IBM Sametime
- Lotus Notes
- Microsoft Exchange
- Microsoft OCS SIP
- Other Email
- Other SIP
- Other XMPP

Changing the local FQDN

Procedure

1. Locate the `network` file at `/etc/sysconfig/` and change the value of the *HOSTNAME* variable to the new FQDN.
2. Locate the `hosts` file in the `/etc/` folder and change the FQDN associated with the local node’s IP address to the new FQDN.
3. Enter the following command to change the operating system’s current hostname:

   ```
   hostname <new_FQDN>
   ```

4. To create and import new certificates and update the Avaya Multimedia Messaging configuration, do the following:
   a. Start the `configureAMM` script.
   b. Open the Front-End, System Manager and Certificate Configuration page and complete all the fields.

      You must also set the FQDN of the new local front-end host.

   c. Cick **Apply**.
5. Restart the application by exiting the `configureAMM` script.

System Manager configuration

Configuring Avaya Aura® System Manager for LDAP synchronization

About this task

The following procedure describes how to configure Avaya Aura® System Manager users according to the above specifications. The procedure is optional if the System Manager login name is properly configured to map the LDAP server.

⚠ **Warning:**

If you change the Avaya Aura® System Manager settings after installing Avaya Multimedia Messaging and you need to use Avaya Multimedia Messaging immediately, you must perform a forced LDAP sync using the Avaya Multimedia Messaging administration portal.

Before you begin

Use the following rules to perform the communication profile configuration:

- Configure the `mail` attribute in Microsoft Active Directory with a valid email address.
- The email address configured in Avaya Aura® System Manager for the user can be of the following types:
  - Microsoft Exchange
  - Other email
- Configure the Avaya Aura® System Manager Login Name mapping by accessing the Enterprise Directory Mappings page in the web-based administration portal.

  Note:

  Configure the Login Name after you create the user in Avaya Aura® System Manager.
- On Avaya Aura® System Manager, you must configure the Avaya Presence/IM handle for every user.

To understand how attribute mapping between System Manager and the LDAP server works, see Attribute mapping use cases on page 25.

The following table displays the configurations supported individually or simultaneously:

Microsoft Exchange	Other email	Login Name
X		
	X	
		X
X		X
	X	X

Procedure

1. Log in to the Avaya Aura® System Manager administration portal.
2. Select **User Management** > **Manage Users**.
3. In the Users table, select a user and click **Edit**.
4. Click the **Communication Profile** tab, and click **New**.
5. Perform the following actions:
   a. In the Type field, select **Microsoft Exchange** or **Other Email**.
   b. In the Fully **Qualified Address** field, type the email address of the user as provided in the `mail` LDAP attribute.

      For example: `username` @ `yourcompany.com`

    c. Click **Add**.

6. Click **Commit** or **Commit and Continue** to save the changes.

Next steps

After the installation of the Avaya Multimedia Messaging server is complete, open the administration portal and configure the Avaya Multimedia Messaging server for LDAP synchronization with Avaya Aura® System Manager.

Attribute mapping use cases

Attribute mapping consists of associating the Avaya Multimedia Messaging Application fields with attributes from the LDAP server configuration, depending on the organization requirement.

You can configure attribute mapping using the **Attribute Mapping** menu of the Avaya Multimedia Messaging administration portal.

Attribute mapping for Active Directory users

The following example is for attribute mapping using a mandatory and an optional field:

- The Avaya Multimedia Messaging application field name **emailAddress** is mapped using the Attribute Mappings menu to `attr1` in Active Directory.
- The Avaya Multimedia Messaging application field name **SMGR Login Name** is mapped using the Attribute Mappings table to `attr2` in Active Directory.

Important:

The administrator must ensure that the attribute to which the Login Name is mapped in the enterprise directory contains unique values only.

In Microsoft Active Directory, the Login Name is usually mapped to userPrincipalName.

When only attr1 is populated in Active Directory:

The system uses the value of `attr1` returned from an LDAP query to search System Manager for a match on System Manager attributes Login Name, MS Exchange handle, and Other Email handle.

- If the system finds a matching System Manager user, System Manager returns the contact handles.
- If System Manager does not return a match, the only valid contact data for this user is the value of the `attr1` and `msRTCSIP-PrimaryUserAddress` LDAP attributes.

When both attr1 and attr2 are populated in Active Directory:

The system uses the value of `attr2` to search System Manager for a match on the System Manager attribute Login Name.

- If the system finds a matching System Manager user, System Manager returns the contact handles. The handles are returned in a list that contains the union of `attr1` and the set of System Manager handles.
- If System Manager does not return a match, the search is made using `attr1` as in the previous case, when only `attr1` is populated.

Attribute mapping for other LDAP server types

The user must have the `mail` attribute configured in the enterprise directory.

There are no custom attribute mappings available.

The system uses the value of the `mail` attribute returned from an LDAP query to search System Manager for a match on the System Manager Login Name attribute.

- If the system finds a matching System Manager Login Name, System Manager returns a union of the contact handles from the LDAP server and System Manager.
- If the System Manager Login Name does not match any LDAP attributes, the values of Microsoft Exchange or Other Email in the System Manager are used to perform the LDAP search. If a match is found, System Manager returns a union of the contact handles from the LDAP server and System Manager.
- If none of the System Manager attributes match the LDAP attributes, the only valid contact for this user is the value of the `mail` attribute.

Note:

When the SIP domain is different than the email domain and System Manager is synchronised with the LDAP server, the MS Exchange mail, SMGR email, or Other Email attribute must be configured, otherwise the users will be unable to send or receive messages.

Adding the Avaya Multimedia Messaging server as a managed element in System Manager

About this task

The following procedure describes how to add the Avaya Multimedia Messaging server as a managed element in Avaya Aura® System Manager.

Before you begin

Before you configure Avaya Aura® System Manager to work with the Avaya Multimedia Messaging server, ensure that the following requirements are met:

- The FQDN of the Avaya Multimedia Messaging server and the FQDN of the System Manager must have the same subdomain.

  For example: `ammserver.avaya.com` and `smgrserver.avaya.com`.
- The Avaya Multimedia Messaging server must be configured to gain access to System Manager using the System Manager FQDN and not the IP address.
- Ensure that the FQDN of Avaya Multimedia Messaging and System Manager can resolve to each other.

Procedure

1. In the System Manager administration interface, select **Services** > **Inventory** > **Manage Elements**.
2. Click **New**.
3. In the **Type** field, select **Other Applications**.

4. In the **General** field, configure the mandatory fields:
    - The name of the Avaya Multimedia Messaging server
    - The FQDN of the Avaya Multimedia Messaging node
5. In the **Access Profile** field, configure the mandatory fields:
    - Protocol: URI
    - Name
    - Access Profile Type: EMURL
    - Protocol: https
    - Host: the FQDN of the Avaya Multimedia Messaging server
    - Port: 8445
    - Path: /admin
    - Order: 0
6. Click **Save** and then click **Commit**.

    The new element contains a link to the Avaya Multimedia Messaging administration portal.

LDAP server configuration

Avaya Multimedia Messaging uses the LDAP servers for user authentication, user authorization, and retrieving user details.

For a complete list of LDAP settings and attributes, see LDAP Configuration on page 100. This section describes the settings to provide in the LDAP configuration menu during the Avaya Multimedia Messaging installation, but also contains information about the LDAP server attributes.

For a configuration example with Microsoft Active Directory, see Configuration for Microsoft Active Directory on page 136.

User attributes

To be able to use the Avaya Multimedia Messaging features, a user must be defined as follows:

- An object of the *user* type in the LDAP server
- An object of the *user* type in the *active* state, if the LDAP server supports the disabling of users
- An attribute called *mail* for the user object

Note:

The value of the *mail* attribute must not be empty and must contain a valid address, as this is used as the primary email address of the Avaya Multimedia Messaging user.

Optionally, Avaya Multimedia Messaging can retrieve data from the following LDAP attributes:

- The telephone number of the user — telephoneNumber
- The local given name setting — givenName
- The local given surname setting — sn

User management

The following parameters are used by the Avaya Multimedia Messaging User management component:

- Active users search filter string — activeUsersFilter
- Last updated time attribute — lastUpdatedTimeAttr

Global catalog configuration

The Microsoft Active Directory global catalog is a repository that holds data for the entire domain forest.

Each domain in the forest is configured to replicate some of the data to the global catalog. Some attributes are not configured by default to replicate to the global catalog.

For more information about the global catalog, see the Microsoft TechNet website.

Important:

If you set your LDAP configuration on Avaya Multimedia Messaging to point to the global catalog (ports 3268 or 3269), you must ensure that all ‘Directory Field Name’ attributes on the Enterprise Directory Mappings screen are replicated in the global catalog. Otherwise, these attributes are not returned by the LDAP searches.

For example:

By default, the Active Directory attribute ‘employeeID’ is not replicated, so if you need this attribute and you use the global catalog, you must update the schema to replicate that attribute.

For information about adding an attribute to the global catalog, see the Microsoft TechNet website.

Virtual machine and physical server deployment specifications

The following tables describe VMware and physical server deployment specifications.

VMware deployments

Specification	500 users	1000 users	2500 users	5000 users	7500 users	10000 users
vCPUs (at 2.9GHz)	8	8	12	16	20	24
Memory	8 GB	8 GB	16 GB	24 GB	28 GB	32 GB
Storage reservation	0.5 TB	1 TB	2 TB	3 TB	4 TB	5 TB

The storage reservation includes the following:

- The amount of disk space required to install and run Avaya Multimedia Messaging. The amount of disk space does not depend on the number of users in the system. For more information, see *Avaya Multimedia Messaging Reference Configuration*.

- The amount of disk space required to store the user data for the given number of users.

Physical server deployments

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

Resources profile specifications for Avaya Multimedia Messaging on Amazon Web Services

The following table outlines the profiles created by the CloudFormation template generators. You can use the CloudFormation template generation tool to create a template for the required profile. The template contains the computing and networking resources required for the profile.

Profile	Service size	AWS instance type
Profile 2	1000 users	m4.xlarge
Profile 3	5000 users	m4.2xlarge

Networking considerations for Amazon Web Services

There are some limitations for establishing public internet VPNs and direct connections into AWS. For more information about Amazon VPC Limits, see the AWS documentation at http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html.

Important:

Use a direct connection along with a private WAN connection with Service Level Agreement (SLA) measures to ensure that the network quality is appropriate for signaling and voice traffic.

Avaya is not responsible for network connections between AWS and the customer premises.

When you deploy Avaya Multimedia Messaging in an AWS environment, you must also deploy a local LDAP server in AWS. This LDAP server is a replica server that synchronizes content from a master LDAP server within the enterprise. To reduce latency for authentication and directory lookup operations, this LDAP server must be collocated with Avaya Multimedia Messaging in the same AWS region.

Connection types

You can connect applications in a hybrid network on the Virtual Private Cloud (VPC) in the following ways:

Connection type	Resource
VPN connection	For information about VPN connections, see http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html.
Direct connection	For information about AWS direct connections, see https://aws.amazon.com/directconnect/.

Linux alias commands

Linux aliases are defined to make frequently used commands easier to use. When an alias is available for the required operation, you can use the alias instead of typing a long path name and using `sudo`. The path name specification and `sudo` invocation are built into the aliases that Avaya provides.

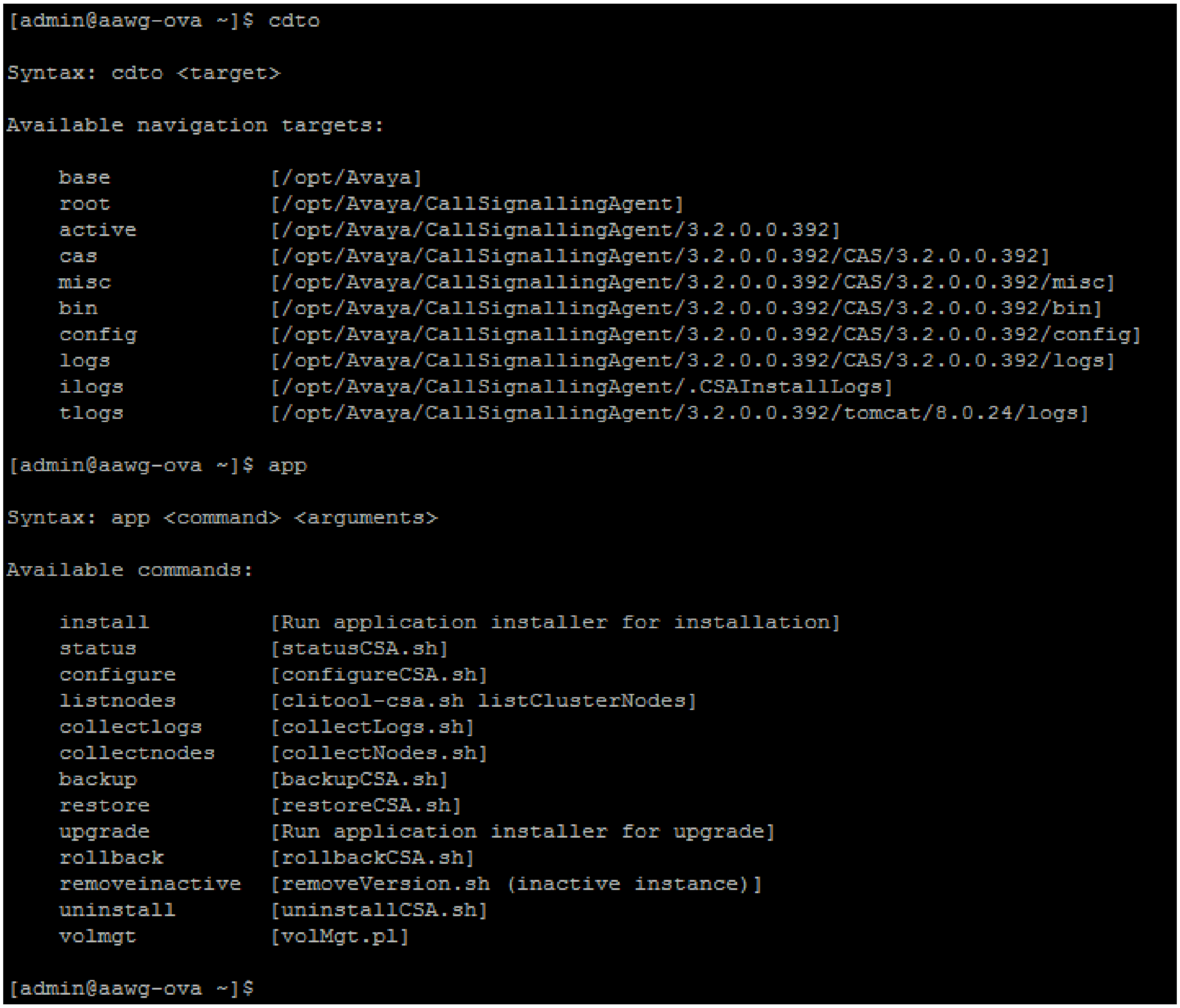
Table 3: Three categories of aliases with their functionality description

Alias	Description
`cdto`	Change to frequently used directories.
`app`	Perform application functions, such as install or backup.
`svc`	Manage the state of application related services.

Some of the alias commands are only available after the application has been installed.

You can type any of the aliases in a Linux shell to list the supported commands.

The following image provides an example of how the aliases are used:



```
[admin@aawg-ova ~]$ cdto

Syntax: cdto <target>

Available navigation targets:

    base            [/opt/Avaya]
    root            [/opt/Avaya/CallSignallingAgent]
    active          [/opt/Avaya/CallSignallingAgent/3.2.0.0.392]
    cas             [/opt/Avaya/CallSignallingAgent/3.2.0.0.392/CAS/3.2.0.0.392]
    misc            [/opt/Avaya/CallSignallingAgent/3.2.0.0.392/CAS/3.2.0.0.392/misc]
    bin             [/opt/Avaya/CallSignallingAgent/3.2.0.0.392/CAS/3.2.0.0.392/bin]
    config          [/opt/Avaya/CallSignallingAgent/3.2.0.0.392/CAS/3.2.0.0.392/config]
    logs            [/opt/Avaya/CallSignallingAgent/3.2.0.0.392/CAS/3.2.0.0.392/logs]
    ilogs           [/opt/Avaya/CallSignallingAgent/.CSAInstallLogs]
    tlogs           [/opt/Avaya/CallSignallingAgent/3.2.0.0.392/tomcat/8.0.24/logs]

[admin@aawg-ova ~]$ app

Syntax: app <command> <arguments>

Available commands:

    install         [Run application installer for installation]
    status          [statusCSA.sh]
    configure       [configureCSA.sh]
    listnodes       [clitool-csa.sh listClusterNodes]
    collectlogs     [collectLogs.sh]
    collectnodes    [collectNodes.sh]
    backup          [backupCSA.sh]
    restore         [restoreCSA.sh]
    upgrade         [Run application installer for upgrade]
    rollback        [rollbackCSA.sh]
    removeinactive  [removeVersion.sh (inactive instance)]
    uninstall       [uninstallCSA.sh]
    volmgt          [volMgt.pl]

[admin@aawg-ova ~]$
```

Each alias category displays the target command, which is in square brackets. The syntax for the command is provided in the procedures outlined in this document. Arguments that you specify after an alias are passed through to the target command.

The system can simultaneously have both an active and inactive installation of the software. For example, after an upgrade, the earlier version becomes inactive, but the new version becomes active. The alias commands operate only on the active installation unless specified.

Table 4: Examples of alias commands to be used in a Linux shell

Alias example	Function provided
`cdto logs`	Changes to the log directory of the active installation on the system.
`app install`	Runs the staged application installer.
`svc telportal restart`	Restarts the telportal service.

Note:

The aliases must be used only from the command line in a Linux shell. Do not use them in a script. You must use the actual target command in a script.

Chapter 4: Initial setup

You can deploy Avaya Multimedia Messaging in the following ways:

- As a software-only application that you can install on your own Red Hat Enterprise Linux (RHEL) 7.3 physical servers or virtual machines.
- In a VMware environment using an Avaya-provided, application-specific RHEL 7.3 OVA.
- In an Amazon Web Services (AWS) environment using an Avaya-provided, application-specific RHEL 7.3 OVA.

Software-only deployments

Avaya Multimedia Messaging can be deployed as a software-only application, using your own physical servers or virtual machines.

For virtual machine installations, Avaya supports the VMware® virtualization environment.

After you deploy your physical servers or virtual machines, use the common installation, configuration, and administration tasks to complete the system deployment.

Software-only deployment checklist

The following checklist outlines the tasks that you must perform when deploying Avaya Multimedia Messaging as a software-only application on your own physical servers or virtual machines.

No.	Task	Notes	✔
1	Install Red Hat Enterprise Linux (RHEL) 7.3 and configure logical disk sizes as required by the Avaya Multimedia Messaging server.	Avaya Multimedia Messaging Release 3.4 requires RHEL 7.3. Avaya also recommends that you install the latest security updates on RHEL.	
2	Create a non-root Linux user and assign sudo permissions to the user.	The installation and administration of the Avaya Multimedia Messaging server is more secure when performed by non-root users with sudo privileges.	

Table continues…

No.	Task	Notes	✔
		Important: The User ID (UID) of the Linux user that performs the installation must be the same on all nodes in the cluster.	
3	Install the required Linux libraries for the Avaya Multimedia Messaging server.	The Linux libraries required for the functioning of the Avaya Multimedia Messaging server are: glibc, libgcc, libstdc++, and dialog. You also need Open JDK 1.8. For the complete list of libraries, see Installing required Linux packages on page 43.	
4	Update OpenSSL	To avoid potential vulnerabilities of the OpenSSL package installed with the operating system, update the OpenSSL package.	
5	Set up your server before installing Avaya Multimedia Messaging.	Before you install Avaya Multimedia Messaging, you must perform the following configuration tasks on the Avaya Multimedia Messaging server: • Disable SELinux. • Add your host name to the `/etc/hosts` file. • Configure DNS. • Configure Network Time Protocol (NTP). • Configure SSH.	
6	Obtain the required components for certificate management.	Avaya Multimedia Messaging certificate management can be done using the Avaya Aura® System Manager trusted certificate, local certificates, or third party CA certificates.	
7	Download the Avaya Multimedia Messaging installation file from PLDS.	None.	
8	Install or restore the application layer as required.	For installation information, see Installing the Avaya Multimedia Messaging server on customer-provided systems on page 48. For initial configuration, see Avaya Multimedia Messaging initial installation configuration on page 73.	

Table continues…

No.	Task	Notes	✔
		If you are configuring a cluster, see Avaya Multimedia Messaging cluster installation on page 80.	
9	Create a new Gluster file system. If you add a new node to a cluster, you must expand the Gluster file system.	For more information, see Creating a Gluster file system on page 91. In a cluster environment, you must deploy all nodes before creating a Gluster file system.	
10	Configure the Avaya Multimedia Messaging using the configuration utility.	The configuration utility starts automatically during installation, after you read and accept the End-User License Agreement (EULA). You can proceed with the configuration immediately or exit and run the configuration utility at a later time. The configuration tasks associated with this utility are described in Avaya Multimedia Messaging server configuration with the configuration utility on page 94.	

Installing the Red Hat Enterprise Linux operating system

About this task

Use this procedure to install the RHEL 7.3 OS on your own physical servers or virtual machines. This procedure enables you to align the OS configuration with the reference configuration for Avaya Multimedia Messaging as described the logical disk specifications in *Avaya Multimedia Messaging Reference Configuration*.

Procedure

1. Mount the Red Hat Enterprise Linux 7.3 ISO image and set the server to boot from this image.

   Note:

   The actual mounting steps vary for physical servers and virtual machines and also depend on the method used to mount the ISO image. For example, the steps vary for using a DVD-ISO mount or an ISO image on a USB device.

2. Turn on the power to boot from the mounted Red Hat Enterprise Linux 7.3 ISO image.
3. Select **Install Red Hat Enterprise Linux 7.3** and then press `Enter`.
4. Press `Enter` to start the installation process.

   The system displays the Red Hat Enterprise Linux installation wizard.
5. Select a language and click **Continue**.
6. Configure the following server settings in the Red Hat Enterprise Linux installer:
   a. Configure **Date & Time**.

   Do not configure the NTP service.

   b. Configure **Keyboard**.

   c. Configure **Language Support**.

7. Do the following to configure network settings using the network data you saved during the preparation procedure:

   a. Select **Network and Hostname**.

   b. Specify a static IPv4 address that you set manually and select **Automatically connect to this network when it is available**.

   c. If the server has multiple network interfaces, configure only one of them.

      Leave the other interfaces set to **Off**.

   d. Configure the DNS server IPs, search domains, netmask, host name, and gateway.

8. Click **Software Selection** and do the following:

   a. For **Base Environment**, select **Minimal Install**.

   b. For **Add-ons for Selected Environment**, select **Compatibility Libraries**.

   c. Leave the other options unselected.

   d. Click **Done**.

9. To select the destination of Red Hat Enterprise Linux 7.3, do the following:

   a. Click **Installation Destination**.

   b. Select all disks that the system displays.

   c. In the Other Storage Options area, select **I will configure partitioning**.

   d. Click **Done**.

10. Do the following to create the `/boot` logical disk:

    a. Click the plus sign (+).

    b. In **Mount Point**, type `/boot`.

    c. In **Desired Capacity**, type `500 MiB`.

       Note:

       The available space for `/boot` might be limited by the disk configuration of the previous system. In this case, allocate as much space as possible, up to 500 MiB.

    d. Click **Add mount point**.

    e. For **Device Type**, select **Standard Partition**.

    f. For **File System**, select **xfs**.

    g. Click **Modify...**.

    h. Ensure that only the first listed disk is selected.

   i. Click **Select**.

11. Do the following to create the `/` logical disk:
    a. Click the plus sign (+).
    b. In **Mount Point**, type `/`.
    c. In **Desired Capacity**, type `50 GiB`.
    d. Click **Add mount point**.
    e. For **Device Type**, select **LVM**.
    f. For **File System**, select **xfs**.
    g. Click **Volume Group** > **Create a new volume group...**, enter a group name, ensure that only the first listed disk is selected, and then click **Save**.

       An example of the volume group name is `disk1_vg`.
    h. In **Name**, type a name for this LVM local disk.

       The standard name is `root`.
12. Do the following to create the `/opt/Avaya` logical disk:
    a. Click the plus sign (+).
    b. In **Mount Point**, type `/opt/Avaya`.
    c. In **Desired Capacity**, type `200 GiB`.
    d. Click **Add mount point**.
    e. For **Device Type**, select **LVM**.
    f. For **File System**, select **xfs**.
    g. Click **Volume Group** and select the new volume group that you created earlier.

       For example, select **disk1_vg**.
    h. In **Name**, type a name for this LVM logical disk.

       The standard name is `application`.
13. Do the following to create the `/home` logical disk:
    a. Click the plus sign (+).
    b. In **Mount Point**, type `/home`.
    c. In **Desired Capacity**, type `10 GiB`.
    d. Click **Add mount point**.
    e. For **Device Type**, select **LVM**.
    f. For **File System**, select **xfs**.
    g. Click **Volume Group** and select the new volume group that you created earlier.

       For example, select **disk1_vg**.

  h. In **Name**, type a name for this LVM logical disk.

     The standard name is `home`.

14. **(Optional)** If you are using disk encryption, do the following to create the `/media/cassandra` logical disk:

    a. Click the plus sign (+).

    b. In **Mount Point**, type `/media/cassandra`.

    c. In **Desired Capacity**, type `10 GiB`.

    d. Click **Add mount point**.

    e. For **Device Type**, select **LVM**.

    f. For **File System**, select **xfs**.

    g. Click **Volume Group** and select the new volume group that you created earlier.

       For example, select **disk1_vg**.

    h. In **Name**, type a name for this LVM logical disk.

       The standard name is `cassandra`.

15. Do the following to create the `swap` logical disk:

    a. Click the plus sign (+).

    b. In **Mount Point**, type `swap`.

    c. In **Desired Capacity**, type `8 GiB`.

    d. Click **Add mount point**.

    e. For **Device Type**, select **LVM**.

    f. For **File System**, select **swap**.

    g. Click **Volume Group** and select the new volume group that you created earlier.

       For example, select **disk1_vg**.

    h. In **Name**, type a name for this LVM logical disk.

       The standard name is `swap`.

16. Do the following to create the `/media/data` logical disk:

    a. Click the plus sign (+).

    b. In **Mount Point**, type `/media/data`.

    c. In **Desired Capacity**, type `1 MiB`.

    d. Click **Add mount point**.

    e. For **Device Type**, select **LVM**.

    f. For **File System**, select **xfs**.

   g. Click **Volume Group** > **Create a new volume group...**, enter a group name, ensure that only the *second* listed disk is selected, and then click **Save**.

      An example of the volume group name is `disk2_vg`.

   h. Select the `/media/data` mount point.

   i. In **Desired Capacity**, enter the actual size of the entire second disk using `MiB` or `GiB` as the unit.

   j. In **Name**, type a name for this LVM logical disk.

      The standard name is `data`.

17. Select each mount point to review the size and settings of each logical disk.

18. **(Optional)** Create the logical disks recommended by the reference configuration for `/tmp`, `/var`, and `/var/log`.

    When creating these disks, select the same dedicated or shared volume group that you selected in the previous steps. The standard names are `tmp` for `/tmp`, `var` for `/var`, and `system_log` for `/var/log`.

19. Do the following to allocate any remaining disk space to any logical disk that you created in the previous steps:

    ! **Important:**

    Do not add additional space to the `/media/data` disk.

   a. In the New Red Hat Linux 7.3 Installation area, select a logical disk that you want to expand.

   b. Click **Modify...**, note the available space that the system displays in the Free column, and then click **Cancel**.

   c. In **Desired Capacity**, enter the new disk size.

      ✱ **Note:**

      - The space you are adding must be less than the total available space.
      - For consistency, specify the disk space unit as `MiB` or `GiB`.

20. Click **Done**.

21. Review the actions that the system displays in the Summary of Changes window.

22. Click **Accept Changes**.

23. Click **Begin Installation**.

24. Click **Root Password** and set a password for the root user.

25. Click **Done**.

26. When the installation is completed, click **Reboot**.

Next steps

Perform post OS installation tasks.

Post OS installation operations

Before you install the Avaya Multimedia Messaging server by running the binary installer, you must configure the OS environment by performing the tasks in this section.

Creating administrative users

About this task

The Avaya Multimedia Messaging deployment must be made by a non-root Linux user with sudo privileges. The User ID (UID) of the Linux user that performs the installation must be the same on all nodes in the cluster.

This procedure describes how to add users and groups. For a clustered deployment of Avaya Multimedia Messaging, perform the steps described in the procedure on every node in the cluster.

The following procedure describes how to add users and groups.

Procedure

1. Log in as the root user.
2. Run the following command to create a group for the administrative user:

   ```
   groupadd -g 4001 <admin_group>
   ```

   In this command, `<admin_group>` is a group name of your choice. For example:

   ```
   groupadd -g 4001 admingrp
   ```

   Important:

   For Group ID (GID), you must use `4001`.
3. Run the following command to add an administrative user in the new administrative group:

   ```
   useradd -g <admin_group> -u 4001 <admin_name>
   ```

   In this command, `<admin_group>` is the name of the group you created in the previous step, and `<admin_name>` is an administrative user name of your choice. For example:

   ```
   useradd -g admingrp -u 4001 ammapp
   ```

   Important:

   For User ID (UID), you must use `4001`.
4. Run the following command to create a password for the new administrative user and then enter the password:

   ```
   passwd <admin_name>
   ```

   In this command, `<admin_name>` is an administrative user name of your choice.
5. Run the following command to create a dedicated group for the software services:

   ```
   groupadd -g 4000 ucgrp
   ```

   Important:

   For GID, you must use `4000`. For the group name, you must use `ucgrp`.

6. Run the following command to add a dedicated user for the software services that has no login privileges:

   ```
   useradd -M -r -s "/sbin/nologin" -g ucgrp -u 4000 ucapp
   ```

   ❗ **Important:**

   You must use the following values:

   - `4000` for GID.
   - `ucgrp` for the group name.
   - `ucapp` for the user name.

7. Run the following command to add the administrative user to the software services group:

   ```
   usermod -a -G ucgrp <admin_name>
   ```

   In this command, `<admin_name>` is the administrative user name. For example:

   ```
   usermod -a -G ucgrp ammapp
   ```

Next steps

Grant sudo permissions to the new administrative user.

Granting sudo permissions to the administrative user

About this task

The administrative user needs sudo rights to install Avaya Multimedia Messaging. For a single-server deployment, perform this task once. For a cluster deployment, perform this task on every node in the cluster.

After performing this procedure, you must always log in to the system as the administrative user, not as the root user. For security reasons, do not use the root user for administrative tasks.

Before you begin

Create an administrative user on every server in the cluster.

Procedure

1. Log in as the root user.
2. Run the following command to open the `/etc/sudoers` file:

   ```
   visudo
   ```

In the following steps, use vi editing commands to edit the `/etc/sudoers` file.

3. Search for the section that contains the following comment: `#Allow root to run any commands anywhere`.
4. Duplicate the line under the comment for the root user and change `root` to the name of the new administrative user in the new line.

   For example:

   ```
   #Allow root to run any commands anywhere
   root        ALL=(ALL)        ALL
   ammapp        ALL=(ALL)        ALL
   ```

5. Do the following to save the /etc/sudoers file and then exit the text editor:
    a. Press Esc.
    b. Enter :wq.
    c. Press Enter.
6. (Optional) Do the following to verify that sudo rights have been assigned to the administrative user:
    a. Run the following command to switch to the administrative user:
       ```
       su - <user_name>
       ```
       The following example shows how to switch to the ammapp user:
       ```
       su - ammapp
       ```
    b. Display a file that requires root access using the sudo command.

       For example:
       ```
       sudo cat /etc/shadow
       ```
    c. Enter the password of the administrative user.

       If the administrative user has sudo access, the content of the file selected in the previous step is displayed in the text console.
    d. **(Optional)** Run the following command to switch back to the root user:
       ```
       exit
       ```

Setting directory ownership

About this task

Use this procedure to assign ownership of /opt/Avaya and /media to ucapp and ucgrp. These directories must be owned by the user and group that are dedicated to the software services.

Before you begin

Create administrative users and groups.

Procedure

1. Log in as the root user.
2. Run the following command to set the user and group owner for /opt/Avaya:
   ```
   chown -R ucapp:ucgrp /opt/Avaya
   ```
3. Run the following command to set the user and group owner for /media:
   ```
   chown -R ucapp:ucgrp /media
   ```
4. Run the following command to set the permissions to /media:
   ```
   chmod 750 /media
   ```

Installing required Linux packages

About this task

This procedure describes how to install the additional Linux packages required by the Avaya Multimedia Messaging server.

You can install the required packages using the yum package manager. For more information about how to enable yum, see the Red Hat yum documentation.

You must use the RHEL 7.3 repository.

Procedure

1. Log in as the root user
2. Run the following commands to install the required RHEL 7.3 packages:

   ```
   yum install libgcc.i686
   yum install libstdc++.i686
   yum install dialog
   yum install java-1.8.0-openjdk
   yum install ntp
   yum install keyutils
   yum install libevent
   yum install nfs-utils
   yum install attr
   yum install psmisc
   yum install perl
   yum install perl-Data-Dumper
   yum install zip
   yum install unzip
   yum install vim
   yum install screen
   yum install wget
   yum install fuse-libs
   yum install fuse
   yum install net-tools
   yum install lsof
   yum install bind-utils
   ```

   For information about applying package updates from the Red Hat network, follow the instructions at the Red Hat customer portal.
3. If you are enabling disk encryption for the media data logical disk, run the following command to install the additional package:

   ```
   yum install cryptsetup
   ```

Disabling SELinux

About this task

The following procedure describes how to disable SELinux prior to the installation of the Avaya Multimedia Messaging server.

Procedure

1. Open the SELinux configuration file using a text editor.

   For example:

   ```
   vim /etc/sysconfig/selinux
   ```

2. Set the value of the `SELINUX` parameter to `disabled`.

   ```
   SELINUX=disabled
   ```

   ⚠ **Warning:**

   Ensure that `disabled` is properly spelled. Misspelling the value of this setting can cause kernel panic issues.

3. Save the file and exit the text editor.
4. Run the following command to restart the server and apply changes:

   ```
   reboot
   ```

5. Do the following to verify the SELinux configuration:
   a. Log in as the root user.
   b. Run the following command:

      ```
      sestatus
      ```

      Ensure that the system displays `disabled`.

Applying security updates

About this task

To minimize impact to the system, Avaya recommends that you restrict RHEL 7 updates to the latest security updates only.

This procedures describes how to install RHEL security updates on your system before you perform the Avaya Multimedia Messaging server installation. You can install security updates using the yum package manager. For more information about how to enable yum, see the Red Hat yum documentation.

Procedure

1. Log in as the root user.
2. Run the following command to install the latest security updates:

   ```
   yum update-minimal --security
   ```

3. Run the following command to update systemd with a critical fix:

   ```
   yum update systemd
   ```

4. Run the following command to restart the server:

   ```
   reboot
   ```

Editing the hosts file

About this task

For the successful installation and configuration of the Avaya Multimedia Messaging server, you must add the Avaya Multimedia Messaging server details in the `/etc/hosts` file before you start the installation.

Procedure

1. Log in as the root user.
2. Open the hosts file using a text editor.

   For example:

   ```
   vim /etc/hosts
   ```

3. Ensure that the following entries are configured in the hosts file:

   ```
   127.0.0.1 localhost.localdomain localhost
   <Machine_IP> <host_FQDN> <host_name>
   ```

   `<Machine_IP>` is the IP address of the Avaya Multimedia Messaging server.

   `<host_FQDN>` is the FQDN of the Avaya Multimedia Messaging server.

   `<host_name>` is the host name of the Avaya Multimedia Messaging server.

   For example:

   ```
   127.0.0.1 localhost.localdomain localhost
   192.168.1.1 myserver.mycompany.com myserver
   ```

Configuring the Network Time Protocol server

About this task

For optimal functioning of the Avaya Multimedia Messaging server, the local system clock must have an accuracy of 100 milliseconds or less.

This procedure describes how to enable the connection to a Network Time Protocol (NTP) server.

Procedure

1. Log in as the root user.
2. Run the following commands to disable the chronyd service:

   ```
   systemctl stop chronyd
   systemctl disable chronyd
   ```

3. Do the following to install an NTP synchronization package that is included in the latest Avaya Multimedia Messaging Release 3.4 binary installer:

   a. Transfer the installer to the home directory of the administrative user using a file transfer program, such as SFTP or SCP.

   b. Run the following commands to move the installer file to the standard staging location and set the required permissions:

   ```
   cp /home<admin-user>/amm-<new-release>.bin /opt/Avaya
   chown ucapp:ucgrp /opt/Avaya/amm-<new-release>.bin
   chmod 750 /opt/Avaya/amm-<new-release>.bin
   ```

   c. Run the following commands to extract and install the NTP synchronization package:

   ```
   cd /root
   /opt/Avaya/amm-<new-release>.bin --tar xf -- ./avaya-ucapp-ntp-
   sync-1.0-1.el7.rpm
   rpm -ivh avaya-ucapp-ntp-sync-1.0-1.el7.rpm
   rm avaya-ucapp-ntp-sync-1.0-1.el7.rpm
   ```

4. Open the `/etc/ntp.conf` file using a text editor.

   For example:

   ```
   vim /etc/ntp.conf
   ```

5. Add a line that contains the FQDN or IP address of the time servers and save the `/etc/ntp.conf` file.

   For example:

   ```
   server ntpserver.example.com iburst
   ```

   Note:

   Avaya recommends using the NTP servers of your organization instead of public NTP servers. Add the pound sign (#) in front of the public servers that are listed by default to disable connecting to these servers.

6. Run the following command to enable the NTP service:

   ```
   systemctl enable ntpd
   ```

7. Run the following command to restart the server:

   ```
   reboot
   ```

8. Log in as the root user.
9. Run the following command to verify that the NTP service is running:

   ```
   systemctl status ntpd
   ```

   Ensure that the system displays `active (running)`.

10. If the NTP service is not running, run the following command:

    ```
    systemctl start ntpd
    ```

11. Run the following command to verify that the system clock is synchronized:

    ```
    ntpstat
    ```

    Ensure that the system displays `synchronized to NTP server`.

Configuring the SSH settings

About this task

This procedure describes how to configure the SSH settings on the Linux server before you install the Avaya Multimedia Messaging server.

The Avaya Multimedia Messaging installation script performs a verification to ensure that the SSH daemon is properly configured before the installation begins.

Note:

Some of the configuration settings are commented using the pound sign (#) in the initial SSH configuration. For the changes to take effect, you must un-comment the settings by deleting the pound sign (#).

Procedure

1. Log in as the root user.
2. Open the SSH configuration file using a text editor.

   For example:

   ```
   vim /etc/ssh/sshd_config
   ```

3. Modify the Protocol, PermitRootLogin, PasswordAuthentication, and ChallengeResponseAuthentication parameters as follows:

   ```
   Protocol 2
   PermitRootLogin no
   PasswordAuthentication no
   ChallengeResponseAuthentication yes
   ```

   Note:

   When the PermitRootLogin setting is set to `no`, you cannot log in directly as root using an SSH console.

   If one or more of the parameters is preceded by the hash character (#), it means that the parameters are commented and you must delete the hash (#) character for the changes to take effect.

   Warning:

   Some of the configuration settings might have a duplicate that is commented with the opposite value. For example:

   ```
   #PasswordAuthentication yes
   PasswordAuthentication no
   ```

   You must ensure that there are no duplicate values uncommented at the same time, otherwise the system will have an unexpected behavior.

4. Configure a time-out of 600 seconds for the SSH sessions by setting the following values:

   ```
   ClientAliveInterval 600
   ClientAliveCountMax 0
   ```

   The time-out can be set from one minute to 24 hours.

5. Run the following command to restart the SSHD service:

   ```
   systemctl restart sshd
   ```

6. Run the following command to verify the SSHD service is running:

   ```
   systemctl status sshd
   ```

   Ensure that the system displays `active (running)`.

7. Log all users out of all current SSH sessions.

   From now on, log in as the administrative user to manage Avaya Multimedia Messaging.

Note:

If you are performing the migration procedure, continue to perform migration tasks for software-only servers as described in *Administering Avaya Multimedia Messaging*.

Installing the Avaya Multimedia Messaging server on customer-provided systems

About this task

Use this procedure to install Avaya Multimedia Messaging on your own physical servers or virtual machines.

The name of the binary file has the following format: `amm-<version_number>.bin`.

For a clustered deployment, you must install every node of the cluster using this procedure.

Before you begin

- If you are installing Avaya Multimedia Messaging on a physical server, ensure that the conditions listed in Software-only deployment checklist on page 33 are met.
- To run the commands in this procedure, you must log in as the administrative user.

Procedure

1. To verify the integrity of the Avaya Multimedia Messaging binary file after a download, perform the following actions:

    a. Run the **`sha256sum`** command on the `amm-<version_number>.bin` file:

    ```
    /usr/bin/sha256sum /opt/Avaya/amm-<version_number>.bin
    ```

    The system displays the SHA-256 hash of the `amm-<version_number>.bin` file.

    For example:

    ```
    e2e1cb0f34bf664de5e3c44563541d6befdf7b422df516f6bb5503df522d429  amm-
    <version_number>.bin
    ```

    b. Compare the alphanumeric string displayed after running the **`sha256sum`** command to the alphanumeric string displayed on the PLDS site, in the **Download Description** field.

    Matching hashes indicate a successful file download. Mismatched hashes indicate a corrupt download; repeat the download and reverify the hashes.

2. (Optional) Run the binary with the `checkOnly` parameter to perform a preliminary check of the prerequisites listed in the *Before you begin* section.

    ```
    sudo /opt/Avaya/amm-<version_number>.bin -- --checkOnly
    ```

    The `checkOnly` parameter lists every prerequisite and whether the prerequisite is present on the system.

    If a prerequisite is missing, the check for the prerequisite and the overall verification fail.

3. Run the binary to install the Avaya Multimedia Messaging server.

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

   The installation process performs a verification of the prerequisites and opens the installation menu if all the requirements are met.

   Important:

   - Do not re-size the SSH console during the installation and configuration of the Avaya Multimedia Messaging server.
   - If the installer aborts and you are prompted to log back in, you must repeat this step.
4. Provide the configuration details listed in the Initial Installation Configuration menu.

   For information about the initial installation configuration settings, see Avaya Multimedia Messaging initial installation configuration on page 73.
5. Select **Continue** and press `Enter`.
6. On each node in the cluster, log out and log in again to enable the required command line aliases for your SSH session.

Next steps

The next option displayed after the initial installation phase related to configuration. You can access these configuration options anytime by running the Avaya Multimedia Messaging configuration utility.

You must also create a Gluster file system.

Related links

Creating a Gluster file system on page 91
Avaya Multimedia Messaging server configuration with the configuration utility on page 94

VMware deployments using Avaya-provided OVAs

You can deploy Avaya Multimedia Messaging in a VMware environment using an optimized Avaya-provided, application-specific OVA. After you deploy the OVA to create a virtual machine instance, you can install the included application software or download the latest available version from the Avaya support site.

After you create a virtual machine, use the common installation, configuration, and administration tasks to complete the system deployment.

VMware deployment process checklist

This checklist describes the high-level deployment process for VMware deployments.

No.	Task	Notes	✔
1	Deploy the Avaya-provided Avaya Multimedia Messaging OVA in a VMware environment using vSphere or vCenter.	For more information, see VMware deployment options on page 50. The Avaya Multimedia Messaging OVA file includes openjdk. Operating system updates for virtual machines include updates for openjdk.	
2	Increase the partitioning volumes.	Detailed information about modifying partitioning topics is available in *Administering Avaya Multimedia Messaging*.	
3	Install or restore the application layer as required.	For installation information, see Installing the Avaya Multimedia Messaging server for Avaya-provided OVAs on page 72. For initial configuration, see Avaya Multimedia Messaging initial installation configuration on page 73. For a cluster environment, see Avaya Multimedia Messaging cluster installation on page 80.	
4	Create a new Gluster file system. If you add a new node to a cluster, you must expand the Gluster file system.	For more information, see Creating a Gluster file system on page 91. In a cluster environment, you must deploy all nodes before creating a Gluster file system.	
5	Configure Avaya Multimedia Messaging using the configuration utility.	The configuration utility starts automatically during installation, after you read and accept the End-User License Agreement (EULA). You can proceed with the configuration immediately or exit and run the configuration utility at a later time. The configuration tasks associated with this utility are described in Avaya Multimedia Messaging server configuration with the configuration utility on page 94.	

VMware deployment options

Use one of the following deployment methods and then proceed to install the Avaya Multimedia Messaging software.

Deploying the Avaya Multimedia Messaging OVA to a vCenter-managed ESXi host

About this task

Use this procedure to deploy the Avaya Multimedia Messaging OVA to an ESXi hypervisor host that is managed by vCenter. System level configuration parameters are provided during the deployment process through the vSphere client.

Before you begin

Download the Avaya Multimedia Messaging OVA file from PLDS.

Procedure

1. Use the vSphere client to connect to the vCenter that hosts the ESXi hypervisor onto which the OVA will be deployed.
2. Navigate to **File** > **Deploy OVF Template**.
3. On the Source page, click **Browse** and then select the OVA file.
4. Verify the information displayed in OVA Template Details and then click **Next**.
5. Review and accept the license agreements (EULAs) and then click **Next**.
6. On the Name and location page, do the following:
   a. Enter a name for the virtual machine.
   b. Select a location.
   c. Click **Next**.
7. Select **Thick Provision Lazy Zeroed** and then click **Next**.
8. Select the network to which the virtual NIC for the virtual machine will be connected, and then click **Next**.
9. Enter the following configuration values for the virtual machine and then click **Next**:
   - IP address to assign to the virtual machine.
   - Netmask to assign to the virtual machine.
   - Short host name to assign to the virtual machine.
   - Domain name to assign to the virtual machine.
   - IP address of your default gateway.
   - One or more IP addresses of your DNS servers.
   - Default search list.
   - IP address or FQDN of the NTP server.
   - Time zone information.
   - Account login name, initial password, and a new group name for the administrative user.

     The administrative user is required to perform installation and any other configuration or administration tasks.

10. Confirm the configuration details, and then click **Finish** to deploy the OVA template.
11. To determine the memory and CPU requirements, and media disk storage reservation requirement, see Virtual machine and physical server deployment specifications on page 28.
12. Update the virtual machine's virtual hardware as required.

    For more information about adjustments, including memory and CPU resource adjustments, see *Administering Avaya Multimedia Messaging*.

    The size of the media disk must also be set to the storage reservation determined in step 11 on page 52.
13. Start the virtual machine and log in.
14. Extend the size of the `/media/data` volume to utilize the remaining space on its host disk.

    For partitioning version specifications, see *Avaya Multimedia Messaging Reference Configuration*. For steps to adjust the size of a disk volume, see *Administering Avaya Multimedia Messaging*.

Next steps

Install the application software.

- To perform a standard, interactive installation, see Installing the Avaya Multimedia Messaging server for Avaya-provided OVAs on page 72.
- To perform a silent installation, see Performing a silent installation on page 79.

Deploying the Avaya Multimedia Messaging OVA to a standalone ESXi host

About this task

Use this procedure to deploy the Avaya Multimedia Messaging OVA to a standalone ESXi hypervisor host. System level configuration parameters are entered in the virtual machine console during the first boot of the virtual machine.

Before you begin

Download the Avaya Multimedia Messaging OVA file from PLDS.

Procedure

1. Use the vSphere interface to connect to the standalone ESXi hypervisor onto which the OVA will be deployed.
2. Perform steps 2 on page 51 to 5 on page 51.
3. On the Name and location page, enter a name for the virtual machine and then click **Next**.
4. Perform steps 7 on page 51 and 8 on page 51.
5. Review the summary and then click **Finish**.
6. Perform steps 11 on page 52 and 12 on page 52.
7. Right click the virtual machine and select **Open Console**.

8. Start the virtual machine from the console.
9. Review each EULA presented and enter `yes` to accept each one.
10. Enter `y` when you receive the prompt `Unable to mount CD-ROM.Do you want to continue?`
11. Enter the following configuration values for this virtual machine.
    - IP address to assign to the virtual machine.
    - Netmask to assign to the virtual machine.
    - Short host name to assign to the virtual machine.
    - Domain name to assign to the virtual machine.
    - IP address of your default gateway.
    - One or more IP addresses of your DNS servers.
    - Default search list.
    - IP address or FQDN of the NTP server.
    - Time zone information.
    - Account login name, initial password, and a new group name for the administrative user.

      The administrative user is required to perform installation and any other configuration or administration tasks.
12. Review the summary and then enter `y` to continue.
13. Extend the size of the `/media/data` volume to utilize the remaining space on its host disk.

    For partitioning version specifications, see *Avaya Multimedia Messaging Reference Configuration*. For steps to adjust the size of a disk volume, see *Administering Avaya Multimedia Messaging*.

Next steps

Install the application software.

- To perform a standard, interactive installation, see Installing the Avaya Multimedia Messaging server for Avaya-provided OVAs on page 72.
- To perform a silent installation, see Performing a silent installation on page 79.

AWS deployments using Avaya-provided OVAs

Amazon Web Services (AWS) is a cloud services platform that enables enterprises to securely run applications on the virtual cloud. The key components of AWS are Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3).

You can deploy Avaya Multimedia Messaging in an AWS environment using an optimized Avaya-provided, application-specific OVA. After you deploy the OVA to create a virtual machine instance, you can install the included application software or download the latest available version from the Avaya support site.

After you create a virtual machine, use the common installation, configuration, and administration tasks to complete the system deployment.

When you deploy Avaya Multimedia Messaging in an AWS environment, you must also deploy a local LDAP server in AWS. This LDAP server is a replica server that synchronizes content from a master LDAP server within the enterprise. To reduce latency for authentication and directory lookup operations, this LDAP server must be collocated with Avaya Multimedia Messaging in the same AWS region.

Use the following sections to deploy Avaya Multimedia Messaging in an AWS environment.

Note:

Use the AWS Command Line Interface (CLI) for managing AWS services from your computer. For more information about setting up the AWS CLI, see https://aws.amazon.com/cli and http://docs.aws.amazon.com/cli/latest/userguide/cli-chap-getting-started.html#cli-quick-configuration.

AWS deployment process checklist

This checklist describes the high-level deployment process for AWS deployments.

No.	Task	Notes	✔
1	Deploy the OVA for AWS environment.	The Avaya Multimedia Messaging OVA file includes openjdk. Operating system updates for virtual machines include updates for openjdk.	
2	Install or restore the application layer as required.	For installation information, see Installing the Avaya Multimedia Messaging server for Avaya-provided OVAs on page 72. For initial configuration, see Avaya Multimedia Messaging initial installation configuration on page 73. For a cluster environment, see Avaya Multimedia Messaging cluster installation on page 80.	
3	Run the S3 configuration script.	For more information, see Configuring the S3 storage on page 71. In a cluster environment, you must run the script on every node.	

Table continues…

No.	Task	Notes	✔
4	Configure Avaya Multimedia Messaging using the configuration utility.	The configuration utility starts automatically during installation, after you read and accept the End-User License Agreement (EULA). You can proceed with the configuration immediately or exit and run the configuration utility at a later time. The configuration tasks associated with this utility are described in Avaya Multimedia Messaging server configuration with the configuration utility on page 94.	

Signing in to the Amazon Web Services Management console

Before you begin

Ensure that you have an AWS account.

Procedure

1. In your web browser, type the URL https://aws.amazon.com/.
2. Click **Sign In to the Console**.

   The system displays the Amazon Web Service page and auto-populates the **Account** field.
3. In the **User Name** field, type the user name or registered email ID.
4. In the **Password** field, type the password.
5. Click **Sign In**.

   The system displays the AWS Management Console page.

Configuring AWS details using the AWS CLI

About this task

The first time that you use the AWS CLI, you must configure the AWS details.

Before you begin

Set up the AWS CLI on a computer with access to AWS. For more information, see http://docs.aws.amazon.com/cli/latest/userguide/cli-chap-welcome.html.

Procedure

1. Start a command line interpreter on the computer with the installed AWS CLI.

Note:

The AWS CLI supports different Windows and Linux command line interpreters, such as PowerShell or Bash.

2. From the command line interpreter, run the command `aws configure`, and do the following:
    a. For **AWS Access Key ID**, type the AWS access key ID.
    b. For **AWS Secret Access Key**, type the AWS secret access key ID.
    c. For **Default region name**, type the region name.

       For example: `us-west-2`.
    d. For **Default output format**, type `text` or `json`.

Creating a key pair

About this task

A key pair is a set of public and private keys. The public key is used to encrypt data, such as the login password. The private key is used to decrypt the encrypted data. You provide this key pair when you create a CloudFormation stack, and use it for SSH access to the Amazon Machine Instances.

Procedure

1. Sign in to the Amazon Web Services Management console.
2. In the left navigation pane, go to **NETWORK & SECURITY**, and click **Key Pairs**.
3. Click **Create Key Pair**.
4. In the Create Key Pair dialog box, in the **Key pair name** field, type a name for the key pair.
5. Click **Create**.

   The system generates a `*.pem` file and prompts you to save the file on your computer. You can also view the created key pair name in the Key pair name column.
6. Save the `*.pem` file.

   Important:

   When you create a key pair, save it. If you lose the key, you cannot retrieve it and you will not be able to access the instance.

OVA to AMI conversion

Creating a bucket for uploading the OVAs for AMI conversion

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Go to **Services** > **Storage**, and click **S3**.

   The system displays the S3 Management Console page.
3. Click **Create bucket**.

   The system displays the Create bucket dialog box.
4. In **Bucket name**, type a unique bucket name.

   Only use lowercase letters for the name.
5. In the **Region** field, click a region for your bucket.

   For more information about creating a bucket and selecting a region, see Amazon S3 Documentation.
6. Click **Create**.

Next steps

Upload the Avaya Multimedia Messaging OVA.

Creating a service role

About this task

Use this procedure to create a role named `vmimport` for importing files into the S3 bucket.

Use the AWS CLI to run the commands in this procedure.

Procedure

1. Start a command line interpreter on a computer with the installed AWS CLI.
2. Run the following command to create a role named `vmimport` and let the AWS image import service assume this role:

   ```
   aws iam create-role --role-name vmimport --assume-role-policy-document <file://
   trust-policy.json>
   ```

   In this command, `<file://trust-policy.json>` is a path to the `trust-policy.json` file. This file is included in the AWS configuration files artifact.
3. Open the `role-policy.json` file, and in each `“Resource”: “arn:aws:s3:::<disk-image-file-bucket>”` string, replace `<disk-image-file_bucket>` with the actual S3 bucket name.

For example:

```
"Resource": "arn:aws:s3:::my-s3-bucket"
```

4. Run the following command to allow the `vmimport` role to perform importing procedures:

   ```
   aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-
   document <file://role-policy.json>
   ```

   In this command, `<file://rule-policy.json>` is a path to the `rule-policy.json` file. This file is included in the AWS configuration files artifact.

Uploading the Avaya Multimedia Messaging OVA

Before you begin

Download the OVAs from the Avaya PLDS website at http://plds.avaya.com/.

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Go to **Services** > **Storage**, and click **S3**.

   The system displays the S3 Management Console page.
3. From the All Buckets area, select a bucket.
4. Click **Upload**.
5. In the dialog box that is displayed, click **Add Files** and upload the Avaya Multimedia Messaging OVA with the `-aws-001-ova` suffix.

Importing the OVA for AMI conversion

About this task

You can use files in the JSON format that are included in the AWS configuration files artifact. The AWS configuration files artifact also contains single-node and multi-node CloudFormation template generators that you use for AWS server deployment. The AWS configuration file contains the following:

- `trust-policy.json`
- `role-policy.json`
- `Single-Node-Cloud-Template-Gen.html`
- `Multi-Node-Cloud-Template-Gen.html`

For more information, see http://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html.

Use the AWS CLI to run the commands in this procedure.

Before you begin

You need the following to convert the OVA file to an Amazon Machine Image (AMI), to deploy the AMI, and configure Avaya Multimedia Messaging:

- Avaya Multimedia Messaging OVAs with the `-aws-001.ova` suffix has been uploaded to an S3 bucket.

Ensure that you also convert the `*.pem` file to the `*.ppk` format and configure PuTTY for establishing an SSH connection.

Ensure that you updated AWS details using the AWS CLI. For more information, see Configuring AWS details using the AWS CLI on page 55.

Procedure

1. Start a command line interpreter on a computer with the installed AWS CLI.
2. Run the following command to check whether the S3 bucket is ready to use:

   ```
   aws s3 ls
   ```

   The system displays the S3 bucket that you created.
3. To view the content of the S3 bucket, run the `aws s3 ls s3://<nameofbucket>` command.
4. To import the ova for conversion, run the following command:

   ```
   >aws ec2 import-image --cli-input-json "{ \"Description\": \"<server.ova>\",
   \"DiskContainers\": [ { \"Description\": \"<text description of task>\",
   \"UserBucket\": { \"S3Bucket\": \"<your_bucket_name>\", \"S3Key\" : \"<server.ova>
   \" } } ]}"
   ```

   The system displays the Status and the ImportTaskId parameters.

   In the following example, when the system converts the CM Simplex OVA, ImportTaskId is `import-ami-ffmanv5x`.

   ```
   {
       "Status": "active",
       "Description": "<version>-aws-001.ova",
       "Progress": "2",
       "SnapshotDetails": [
           {
               "UserBucket": {
                   "S3Bucket": "<version>-dev",
                   "S3Key": "<version>-aws-001.ova"
               },
               "DiskImageSize": 0.0
           }
       ],
       "StatusMessage": "pending",
       "ImportTaskId": "import-ami-fftlelct"
   }
   ```
5. To check the status of the import image, run the following command:

   ```
   aws ec2 describe-import-image-tasks --cli-input-json "{ \"ImportTaskIds\":
   [\"<Your_ImportTaskId>\"], \"NextToken\": \"abc\", \"MaxResults\": 10 } "
   ```

   The conversion process takes up to 30 minutes. You can run the above command repeatedly.

   In the following example, the process is preparing the AMI and is 76% complete:

   ```
   IMPORTIMAGETASKS x86_64 CM-Simplex-07.1.0.0.xxx-aws-001.ova import-ami-ffgji45r
   BYOL Linux 76 active preparing ami
   ```

   The output format varies depending on the selection of the text or JSON format on the AWS CLI configuration.

6. Sign in to the Amazon Web Services Management console.
7. Go to **Services** > **Compute** and then click **EC2**.

   The system displays the EC2 Management Console page.
8. In the left navigation pane, click **IMAGES** > **AMIs**.

   You can search the converted AMI with ImportTaskId. The system displays the newly converted AMI ImageId in the AMI ID column.

Next steps

Create CloudFormation templates, which can be used to create a stack.

Creating CloudFormation templates

About this task

Use CloudFormation templates to create an AWS stack.

Important:

To create CloudFormation templates, use one of the following web browsers:

- Google Chrome
- Mozilla Firefox

Internet Explorer and Microsoft Edge are *not* supported.

Before you begin

Download the compressed artifact that contains the configuration files to your computer. Extract the two CloudFormation generator HTML files from the compressed file.

Procedure

- To create a single-node CloudFormation template, do the following:
  1. In your web browser, run the template generator by opening the `Single-Node-Cloud-Template-Gen.html` file.
  2. In **Product**, select the required application and profile size.
  3. Click **Generate template**.
  4. Save the file to your computer.
- To create a multi-node CloudFormation template, do the following:
  1. In your web browser, run the template generator by opening the `Multi-Node-Cloud-Template-Gen.html` file.
  2. In **Product**, select the required application and profile size.
  3. In **Number of nodes**, set the number of servers required for the cluster.
  4. In **Number of subnets**, set the number of subnets required for the cluster.

You can set two or three subnets.

5. If you want to create new subnets for availability zones, select the **Create subnets** check box.

   Do not select **Create subnets** if you are planning to use existing subnets.
6. If you are planning to use the existing subnets, do not select **Create subnets**.
7. Click **Generate template**.
8. Save the file to your computer.

Next steps

Deploy the CloudFormation stack:

- For a single-node system, see Deploying a single-node CloudFormation stack on page 61.
- For a multi-node system, see Deploying a multi-node CloudFormation stack on page 65.

Deploying a single-node CloudFormation stack

About this task

Use this procedure to deploy a standalone instance by using a single-node CloudFormation template.

Before you begin

- Use standard Amazon Web Services procedures to create the required network setup, including Virtual Private Cloud (VPC) settings and Security Groups.
- Generate a single-node CloudFormation template.
- Ensure that you have network access to the Amazon VPC before deploying an AMI.

Procedure

1. Sign in to the AWS console and navigate to **Services** > **Management Tools** > **CloudFormation**.

   CloudFormation is an AWS service used to create a stack. A stack is a graph of objects such as EC2 instances and EBS volumes inside the Amazon cloud. CloudFormation is used to create the objects required for a single-node Avaya Multimedia Messaging system within a subnet of an existing virtual network.
2. On the CloudFormation page, click **Create Stack**.
3. On the Create Stack page, click **Select Template**.
4. On the Select Template page, in the Choose a template area, click **Choose file**.
5. Select the single-node `yaml` CloudFormation template file that you generated.
6. Click **Next**.
7. On the Specify Details page, in the **Stack name** field, type the stack name.

   The host name for the node is derived from the stack name.

Note:

The stack name must start with a letter and must contain letters, numbers, and dashes.

8. In **Amazon Machine Image ID**, type the Amazon Machine Image ID (AMI ID) of the instance that you created.

   For example, `ami-fda9369d`.

   Tip:

   To obtain the AMI ID of an image, go to **Services** > **EC2** > **Images** > **AMIs**
9. In the Network area, select the required **Virtual Private Cloud** and **Subnet**.
10. Complete the following to determine the required Route table configuration:

    To display details for the subnet to which you are deploying, go to **Services** > **VPC** > **Subnets**.

    a. Click the **Route Table** tab.

    b. In the Target column, in the **Route table** field, do one of the following:

    - Leave this field if it already has a VPC endpoint (VPCE) entry, for example, `vpce-24ade874`.
    - Type the route table ID if this field is empty, so that a VPCE is created.
11. In **DNS domain**, type the name of the private DNS domain to use.

    This domain name represents the domain name that clients use to access service.
12. If the domain is a new domain in this VPC, set **Create domain** to **Y**. Otherwise, set it to **N**.
13. In the Security area, select **SSH key for administrator login**.
14. Click **Next**.
15. **(Optional)** On the Options page, in the Tag area, add tags that can help you find and organize your AWS objects.
16. In the Permissions area, leave the default values for both **IAM Role** and **Enter role arn**.
17. Click **Next**.
18. On the Review page, confirm the stack information.
19. Select **I acknowledge that AWS CloudFormation might create IAM resources**.

    Note:

    Amazon displays this acknowledgement only when creating CloudFormation stacks that include Avaya Multimedia Messaging systems, which use Amazon S3 for data store.
20. Click **Create** to create the stack.

    The system displays the Stacks page, which shows the stack creation status.

21. Wait until the status displays `CREATE_COMPLETE`.

    You can monitor the status of the stack creation and review the properties using the tabs at the bottom of the Stacks page.

22. Click the **Resources** tab.

23. Click the Physical ID of the EC2 instance for the node, for example, `i-0fccb4a222a32dcc9`.

    The system displays the Instances page using a filter that displays the newly created AMI.

24. **(Optional)** Click the **Actions** menu to change the instance state.

    For example, you can start, stop, or reboot the AMI virtual machine.

Next steps

To complete the first-login configuration, log in using `admin@Instance.hostname` or `admin@instance_IP` as the login credentials are not provided. Accept the license agreement and set the password.

AWS cluster deployments

Use the information in the following subsections for multi-node AWS clusters.

For traffic distribution, use the AWS load balancer. A virtual IP address for clusters is not available on AWS.

Creating and applying load balancer certificates

About this task

Load balancers only appear in the private DNS within AWS. Therefore, certificates generated by external certificate authorities might not work. Use this procedure to obtain a certificate from System Manager within AWS.

Procedure

1. On the System Manager web console, navigate to **Home** > **Services** > **Security** > **Certificates** > **Authority**.

2. Click **Add End Entity** and complete the settings in the following fields:

    a. **End Entity Profile**: Type `<INBOUND_OUTBOUND_TLS>`.

    b. **Username**: Type `<FQDN of the load balancer>`.

       The FQDN of the load balancer is the service FQDN of the cluster. This domain name portion of the FQDN represents the domain name that clients use to access service. The FQDN must be the combination of the stack name followed by the domain. For example, if the stack name is `yourStack` and the domain is `your.domain.com`, then the FQDN is `yourStack.your.domain.com`.

Note:

The stack name must start with a letter and must contain only letters, numbers, and dashes. This stack name must be used during multi-node CloudFormation.

c. **Password**: Type your password.

d. **Confirm Password**: Retype your password.

e. **CN, Common name**: Type `<FQDN of the load balancer>`.

f. **Token**: Select the `PEM` file.

Note:

The remaining fields are optional. For more information, see *Administering Avaya Aura® System Manager*.

3. Click **Add**.
4. Navigate to **Home** > **Services** > **Security** > **Certificates** > **Authority** > **Public Web**.

   The system displays the EJBCA public page.
5. Click **Create Keystore**.
6. In **Username**, type the FQDN of the load balancer.
7. In **Password**, type the End Entity password that you created earlier.
8. Click **OK**.

   The system displays the EJBCA Token Certificate Enrollment page.
9. In **Key length**, select the required key length.

   A length of 2048 bits is recommended.
10. Click **Enroll** and select a text editor to view the certificate.
11. Save the `PEM` file to your computer.
12. Sign in to the AWS console and navigate to **Services** > **Security, Identity & Compliance** > **Certificate Manager**.
13. Click **Import a certificate**.

    The system displays a form with three fields: **Certificate Body**, **Certificate private key**, and **Certificate chain**.
14. Open the `PEM` file you saved earlier with a text editor and do the following:

    Note:

    You must include the BEGIN and END labels for each section that you paste into the form.

    a. In the Private Key section, copy the string from `-----BEGIN PRIVATE KEY-----` to `-----END PRIVATE KEY-----` and paste it into the **Certificate private key** field.

b. In the Certificate section, copy the first certificate string from `-----BEGIN CERTIFICATE-----` to `-----END CERTIFICATE-----` and paste it into the **Certificate body** field.

c. In the Certificate section, copy the second certificate string from `-----BEGIN CERTIFICATE-----` to `-----END CERTIFICATE-----` and paste it into the **Certificate chain** field.

15. Click **Review and import**.
16. Click **Import**.

    The system imports the certificate and displays the status and details of the certificate.
17. Copy and save the ARN value in the Details section.

    The ARN is required for the **Load balancer certificate ARN** field during the multi-node CloudFormation deployment.

Deploying a multi-node CloudFormation stack

About this task

Use multi-node CloudFormation to create a cluster.

Note:

You cannot expand an AWS single node into a AWS cluster. You must create AWS clusters from the beginning. However, after an AWS cluster is created it can be expanded. For more information, see Expanding an existing cluster on page 67.

Before you begin

- Use standard Amazon Web Services procedures to create the required network setup, including Virtual Private Cloud (VPC) settings and Security Groups.
- Ensure that you have network access to the Amazon VPC before deploying an AMI.
- Create a multi-node CloudFormation template as described in Creating CloudFormation templates on page 60.
- Create and apply load balancer certificates. The ARN value created during the certificate import is required for this procedure.

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Navigate to **Services** > **Management Tools** > **CloudFormation**.
3. Click **Create Stack**.

   The AWS EC2 Management console displays the first page of the Create stack wizard.
4. On the Select Template page, in the Choose a template area, click **Choose File**.
5. Select the multi-node `yaml` CloudFormation template file that you generated.
6. Click **Next**.

   The system displays the Specify Details page.

7. In **Stack name**, type a name for the stack.

   This stack name must match the stack name portion of the FQDN of the load balancer.

8. In **Amazon Machine Image ID**, type the Amazon Machine Image ID (AMI ID) of the image that you imported.

   For example, `ami-fda9369d`.

   Tip:

   You can obtain the AMI ID of an image from the EC2 AMI page. On a separate browser tab, navigate to **Services** > **EC2** > **Images** > **AMIs**.

9. In Network area, select the required **Virtual Private Cloud**.

10. Do one of the following depending on whether you selected the **Configure subnets** check box in step 2 on page 60 when creating the multi-node CloudFormation template:

    - If you selected the check box, configure the required IPv4 address range in each subnet CIDR block field.

      In CIDR notation, the number of bits in the network portion of the address follows a slash. For example, 10.143.11.192/28. The address range for the subnets must fall within the address range of the VPC and must not overlap any existing subnet within the VPC.

    - If did not select the check box, select the required subnets from each **Subnet** field.

      Note:

      When using existing subnets, each subnet must be in a different availability zone.

      Important:

      If any of the subnets do not have access to a VPC endpoint, enter this subnet route table ID in **Route Table**. To separate multiple IDs, use a comma.

11. In **DNS domain**, type the name of the private DNS domain to use.

    This domain name must match the domain name used in the FQDN of the load balancer.

12. If the domain is a new domain in this VPC, set **Create domain** to **Y**.

    Otherwise, set it to **N**.

13. In the Security area, select **SSH key for administrator login**.

14. Copy the ARN saved in the Details section and paste it into the **Load balancer certificate ARN** field.

    For information on copying the ARN, see Creating and applying load balancer certificates on page 63.

15. Click **Next**.

    The system displays the Options page.

16. **(Optional)** In the Tags area, add tags to help you find and organize your AWS objects.

17. In the Permissions area, keep the default values for both **IAM Role** and **Enter role arn**.
18. Click **Next**.

    The system displays the Review page.
19. Select **I acknowledge that AWS CloudFormation might create IAM resources**.

    Note:

    Amazon displays this acknowledgement only when creating CloudFormation stacks that include Avaya Multimedia Messaging systems, which use Amazon S3 for data store.
20. Click **Create** to create the stack.

    The system displays the Stacks page, which shows the stack creation status.
21. Wait until the status displays `CREATE_COMPLETE`.

    You can monitor the status of the stack creation and review the properties using the tabs at the bottom of the Stacks page.
22. Click the **Resources** tab.
23. Click the Physical ID of the EC2 instance for the node, for example, `i-0fccb4a222a32dcc9`.

    The system displays the Instances page using a filter that displays the newly created AMI.
24. **(Optional)** Click the **Actions** menu to change the instance state.

    For example, you can start, stop, or reboot the AMI virtual machine.

Next steps

- Create a hybrid cloud to provide client access to the servers.
- To complete the first-login configuration, log in using `admin@Instance.hostname` or `admin@instance_IP` as the login credentials are not provided. Accept the license agreement and set the password.

Expanding an existing cluster

About this task

An existing AWS cluster can be expanded with additional nodes by updating the stack that represents the cluster.

Note:

You cannot expand a single AWS node into an AWS cluster. You must create AWS clusters from the beginning.

Procedure

Add nodes to a cluster by updating the CloudFormation stack that represents the cluster.

For information about updating a stack, see the AWS management information in *Administering Avaya Multimedia Messaging*.

Creating a hybrid cloud for client access

About this task

Servers deployed in AWS are contained within a Virtual Private Cloud (VPC). End user clients are present within a separate network but require access to the servers in AWS. You must create a VPN to enable client access.

You must configure VPN gateways at both ends of the tunnel:

- The address range assigned to the VPC must route to the gateway on your side of the tunnel.
- Within AWS, the address range that clients use must route to the AWS-side gateway.

Use this procedure to configure AWS so that the address range that clients use routes to the AWS-side of the gateway.

Before you begin

- Deploy the required EC2 instances.
- Assign an IP address range to the VPC that does not overlap with any subnet in your network.

Procedure

1. Sign in to the AWS console.
2. Navigate to **Services** > **Management Tools** > **CloudFormation** and select the required stack.
3. Click the **Resources** tab.
4. Click the physical ID link for one of the nodes.

   The system displays a page with the details of the node.
5. Copy the value from the **Subnet ID** field of the Description tab. For example, `subnet-99942eff`.
6. Navigate to **Services** > **Networking & Content Delivery** > **VPC** > **Subnets**.
7. Paste the subnet ID into the **Search Subnets** filter.
8. Select the subnet that the system displays.
9. Select the row that contains the previously noted ID in the Route Table ID column.
10. Select the **Route Table** tab.
11. Click the route table ID link that is located next to the **Edit** button. For example, `rtb-bc53a2db`.
12. Select the route that the system displays.
13. Select the Routes tab.
14. Click **Edit**.

15. Click **Add another route** to add each required client address range and do the following:
    a. In the Destination column, enter the address range.
    b. In the Target column, select an AWS-side gateway that can reach the destination.
16. Click **Save**.

Logging in to the EC2 instance

Procedure

Log in to the EC2 instance using the SSH console or PuTTY.

For information about how to use PuTTY, see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html?icmpid=docs_ec2_console.

✱ **Note:**

You must use the key that you specified during stack creation.

Completing the first-login configuration

About this task

The first time you access a newly deployed EC2, you must complete a one-time system procedure to accept the license agreement, configure the OS, and select network preferences.

Before you begin

Access the EC2 instance by logging in using PuTTY or SSH from the command line. Use the Avaya Multimedia Messaging administrator credentials and the EC2 DNS or IP address for the first log in as follows:

```
<admin_name>@<instance_dns_or_ip_address>
```

For example:

```
ammapp@ec2-198-51-100-1.compute-1.internal
```

or

```
ammapp@198.51.100.1
```

Procedure

1. Do the following when you see the license agreement banner, which is displayed when you log in for the first time:
    a. Press `Enter` to display the license agreement.
    b. Press the `Space bar` to navigate through the license agreement.
    c. When prompted, type `yes` to accept the license agreement.
2. Enter a password for the system administrator.

3. To configure the NTP servers, do one of the following:
    - Press `Enter` to accept the default Amazon NTP time servers.
    - Enter one or more comma separated NTP server IP addresses or FQDNs and then press `Enter`.

    Important:

    The NTP servers that you configure must be reachable from this server. The default Amazon NTP time serves are on the Internet and might not be reachable.
4. Select your time zone preferences.
5. Review the summary of your selections and type one of the following:
    - `y` to apply the settings to the system.
    - `n` to make changes to your selections.

Next steps

Install the Avaya Multimedia Messaging application software using the `app install` command as described in Installing the Avaya Multimedia Messaging server for Avaya-provided OVAs on page 72.

Important:

Do *not* install the Gluster file system in an AWS environment.

Complete the required configuration and commissioning procedures after the initial installation. If you are installing a cluster, you must follow the instructions for using an external load balancer.

Configuring on-premise DNS resolution of VPC addresses

About this task

This configuration allows on-premise clients to access the servers hosted in the AWS VPC. Use this procedure to configure your local, on-premise DNS server with a new DNS forwarding zone so that client DNS resolution requests are forwarded to a DNS server located within the VPC. The DNS server located within the VPC then performs the final address resolution to the servers hosted in the AWS VPC.

Before you begin

Ensure that you have:

- Access to your on-premise DNS server so that you can add a new DNS forwarding zone.
- Enabled your corporate firewall to permit outgoing UDP traffic toward the AWS VPC.
- Routes on your AWS VPC VPN gateway that direct UDP port 53 traffic from the enterprise toward the VPC.
- The IP address of the DNS server in the AWS VPC.
- A list of the VPC domains that the on-premise DNS server must resolve to the AWS DNS server. For example, if your VPC servers must resolve `server.example.com` and

server.example.net, then the list of required VPC domains is example.com and example.net.

- A test FQDN that is configured in the VPC DNS.

Procedure

1. Log on to your local on-premises DNS server as an administrator.
2. Add a new “Forward Zone” or “Forward Lookup Zone” DNS by following the instructions provided by your DNS server manufacturer.
3. Add a new forward zone with the following details for each required VPC domain:
    a. A zone name: Use the same name as the domain name. For example, example.com.

    b. The forwarding address: Use the IP address and port of the DNS server in the AWS VPC. For example, 10.1.2.3@53.

    c. Forward First: Enable Forward First if your DNS server supports this feature. This feature causes resolution requests for the zone to be forwarded to the VPC DNS server before attempting to resolve them locally.
4. Enable the DNS server changes by reloading the configuration or restarting the DNS server.
5. Verify that the DNS resolution completes by performing a lookup of the test FQDN using a DNS resolution utility, such as nslookup or dig.

    For example, you can run the following nslookup command:

```
>  nslookup server.example.com
Server:          192.168.0.1
Address:         192.168.0.1#53

Non-authoritative answer:
Name:    server.example.com
Address: 10.1.2.165
```

Configuring the S3 storage

About this task

Avaya Multimedia Messaging uses the Amazon Web Services S3 storage for storing media data. In the current release, you must manually run a script to configure the S3 storage.

Important:

In a cluster configuration, perform this procedure on each node.

Before you begin

Install the Avaya Multimedia Messaging application.

Procedure

1. Log in to an SSH terminal as an administrator.
2. Navigate to the /opt/Avaya/MultimediaMessaging/<build>/CAS/<build>/glusterfs directory.

   ```
   sudo cd /opt/Avaya/MultimediaMessaging/<build>/CAS/<build>/glusterfs
   ```
3. Run the s3config.sh S3 configuration script.

   ```
   sudo ./s3config.sh
   ```
4. Restart Avaya Multimedia Messaging using the svc amm restart command.

Installing the Avaya Multimedia Messaging server for Avaya-provided OVAs

About this task

Use this procedure to install the Avaya Multimedia Messaging software on a virtual machine instance that was deployed using an Avaya-provided OVA. This procedure applies to both the VMware and Amazon Web Services (AWS) virtualization environments.

For more information about installing an Avaya Multimedia Messaging cluster, see Avaya Multimedia Messaging cluster installation on page 80.

Important:

To perform the installation and any other configuration or administration tasks, use the administrative user that you created when deploying the OVA.

Before you begin

Depending on the deployment method, review the process described in either VMware deployment process checklist on page 49 or AWS deployment process checklist on page 54.

Events such as startup and taking or restoring snapshots synchronize time in the guest operating system, so you must ensure that the time of the host operating system is correct. See the VMware Knowledge Base for details and instructions.

Procedure

1. Log in as the non-root administrative user.
2. Run the following command to install the Avaya Multimedia Messaging server:

   ```
   app install
   ```

   Note:

   When you run the app install command without specifying a build, then the system automatically picks up the current build in /opt/Avaya. If you specify a build in the command, such `app install amm-<version>.bin`, then the system looks for that build first in your current directory and then in `/opt/Avaya`.

The installation process performs a verification of the prerequisites and opens the installation menu if all the requirements are met.

Note:

Do not resize the SSH console during the installation and configuration of the Avaya Multimedia Messaging server.

3. Provide the configuration details listed in the Initial Installation Configuration menu.

   For information about the installation configuration settings, see Avaya Multimedia Messaging initial installation configuration on page 73.

4. Select **Continue** and press `Enter`.

Next steps

The next menu displayed after the initial installation phase is the **Configuration** menu.

The **Configuration** menu can also be accessed at a later time by running the Avaya Multimedia Messaging configuration utility.

In the VMware deployment environment, create a Gluster file system.

Important:

Do *not* install the Gluster file system in an AWS environment.

Related links

Creating a Gluster file system on page 91
Avaya Multimedia Messaging server configuration with the configuration utility on page 94

Avaya Multimedia Messaging initial installation configuration

The Initial Installation Configuration menu displayed when you run the binary to install the Avaya Multimedia Messaging server contains the following items:

- Cluster Configuration
- Front-end host, System Manager and Certificate Configuration
- Cassandra Encryption
- Advanced Configuration

This section contains a description of each configuration setting.

Cluster Configuration

The Cluster Configuration section contains the following configuration settings:

Item name	Description	Equivalent properties file parameter
Initial cluster node	The setting to specify if the server where you are performing the installation is the initial node in a cluster. Select `y` (yes) to set the current node as the initial node in the cluster or `n` (no) to set the current node as an additional node. The default value for this setting is `y` (yes). In a standalone installation, set this value to `y` (yes). If you configure this setting to `n` (no), the following settings become visible and must be configured: • The IP address of the initial cluster node • The ID of the Linux user performing the installation on the initial node • The Cassandra database user name for the initial node • The Cassandra database password for the initial node	`INITIAL_NODE` If you configure this setting to `n` (no), you must also configure the following parameters: • `SEED_NODE` • `REMOTE_UID` • `CURRENT_CASSANDRA_USER` • `CURRENT_CASSANDRA_PASSWORD`
Local node IP address	The IP address of the local node.	`CLUSTER_IP_ADDR`

Front-end host, System Manager and Certificate Configuration

The Front-end host, System Manager and Certificate Configuration section contains the following configuration settings:

Table 5: Front-end host, System Manager and Certificate Configuration settings

Item name	Description	Equivalent properties file parameter
Front-end FQDN	The front-end **FQDN** of the Avaya Multimedia Messaging server. For a cluster deployment, you must configure the front-end FQDN as the FQDN of the virtual IP address. If an external load balancer is used, set this value to the FQDN of the load balancer. The front-end FQDN is the address that end-user clients use to access the	`REST_FRONTEND_HOST`

Table continues…

Item name	Description	Equivalent properties file parameter
	services provided by Avaya Multimedia Messaging . The default value depends on the configuration present in the `/etc/hosts` file of the Avaya Multimedia Messaging server. **Note:** If you install the Avaya Multimedia Messaging server with the FQDN as the front-end address, the Message Playback feature must also be accessed using the FQDN of the Avaya Multimedia Messaging server.	
System Manager FQDN	The FQDN of the Avaya Aura® System Manager that signs the Avaya Multimedia Messaging certificates.	`SYSTEM_MGR_IP`
System Manager web admin username	The System Manager web administration portal user name. This field is optional.	`SMGR_USER_NAME`
System Manager web admin password	The System Manager web administration portal password. This field is optional.	`SMGR_USER_PASSWORD`
System Manager web version	The version number of Avaya Aura® System Manager.	`SYSTEM_MGR_VERSION`
System Manager HTTPS Port	The HTTPS port used for the Alarm Agent for the current Avaya Multimedia Messaging server. The default value for this setting is 443.	`SYSTEM_MGR_HTTPS_PORT`
System Manager Enrollment Password	The Avaya Aura® System Manager enrollment password.	`SYSTEM_MGR_PW`
Override port for reverse proxy	Specifies if you use an external reverse proxy server. Enable this setting only if clients will not be connecting directly to the Avaya Multimedia Messaging server, but rather using a proxy server as part of a remote access solution that is configured to receive connections on a port other than default port 443.	`OVERRIDE_FRONTEND_PORT` For the **Front-end port for reverse proxy** setting, the equivalent parameter is `REST_FRONTEND_PORT`.

Table continues…

Item name	Description	Equivalent properties file parameter
	Select `y` (yes) to configure the port for the reverse proxy server or `n` (no) to keep the default configuration that remains disabled. If you select `y` (yes), the menu displays a new setting for the reverse proxy port: **Front-end port for reverse proxy**. **Note:** If this parameter is changed after the installation, all of the nodes in a cluster must be restarted using the `svc amm restart` command to apply the change.	
Use System Manager for certificates	Specifies if the certificates are retrieved from Avaya Aura® System Manager or from imported files. Select `y` (yes) to retrieve certificates from Avaya Aura® System Manager or `n` (no) to retrieve certificates from imported files. If you select `n` (no), the menu displays new settings for configuring the certificate files. To configure the certificate settings, you must provide the complete file path name to the: • REST interface key file • REST interface certificate file • SIP interface key file • SIP interface certificate file • OAM interface key file • OAM interface certificate file • node key file • node certificate file • signing authority certificate file	`USE_SMGR` If the `USE_SMGR` option is set to `n` (no), you must configure the following parameters for importing the certificate files: • `REST_KEY_FILE` • `REST_CRT_FILE` • `SIP_KEY_FILE` • `SIP_CERT_FILE` • `OAM_KEY_FILE` • `OAM_CRT_FILE` • `NODE_KEY_FILE` • `NODE_CRT_FILE` • `CA_CRT_FILE`
Local frontend host	The local FQDN of the node. This FQDN is not used for a client to access services, but is used to access the server within the enterprise, and is bound to the same Ethernet port as the front-end FQDN.	`LOCAL_FRONTEND_HOST`

Table continues…

Item name	Description	Equivalent properties file parameter
	The Avaya Multimedia Messaging configuration utility uses this value to generate certificates for the node. **Important:** In a clustered configuration, the local front-end host is different from one node to the other and is also different from the front-end FQDN. In a non-clustered environment, the local front-end host is usually different from the front-end FQDN to create a clustered configuration from a non-clustered configuration.	
Keystore password	The keystore password for the MSS and Tomcat Avaya Multimedia Messaging certificates. The minimum length for this password is 6 characters. The characters supported for the keystore password are: • a to z • A to Z • 0 to 9 • other supported characters: exclamation point (!), at symbol (@), hash (#), percent sign (%), caret (^), star (*), question mark (?), underscore (_), dot (.)	`KEYSTORE_PW`

Cassandra Encryption

The Cassandra Encryption section contains the following configuration settings:

Item name	Description	Equivalent properties file parameter
Enable inter-node encryption for Cassandra cluster node	The setting to specify if SSL encryption is enabled on the current Avaya Multimedia Messaging server for internode communication between Cassandra cluster nodes. Configure this setting if the certificates are also configured.	`CASS_INTERNODE_ENCRYPTION_FLAG`

Advanced Configuration

The Advanced Configuration section contains the following configuration items:

Item name	Description	Equivalent properties file parameter
Directory for the glusterfs brick	The absolute path to the directory for storing the media files using a Gluster FileSystem (GlusterFS). The Linux user who performs the installation must have access to the GlusterFS directory. The default value for this setting is `/media/data`. ❗ **Important:** Do *not* modify the default value.	`GLUSTER_BRICK_DIR`
Enable Cassandra DB initialization	The setting to initialize the Cassandra Database from the backup used during restore. Select `y` (yes) to enable database initialization from the backup file or `n` (no) to disable database initialization. The default value for this setting is `y` (yes).	`CASSANDRA_INIT_ENABLE`
Run the firewall configuration script	The setting to configure the Linux firewall during the initial installation phase. Select `y` (yes) to enable firewall configuration during the initial installation phase or `n` (no) to disable firewall configuration. If you set this option to `n` (no), you must configure the firewall after the initial installation is completed. If you set this option to `y` (yes) and the firewall is incorrectly configured, the configuration of the next nodes of the cluster might be incorrect. The default value for this setting is `y` (yes).	`RUN_FIREWALL_CONFIG`
Clear database directories and files	The setting to delete existing database directories and files during the installation. Select `y` (yes) to delete the database directories and files during the installation or `n` (no) to preserve the existing database directories and files.	`CLEAR_DB_AT_INSTALL`

Table continues…

Item name	Description	Equivalent properties file parameter
	The default value for this setting is `y` (yes).	
Remove log files from directory	The setting to preserve log files during the install and uninstall phases. Select `n` (no) to preserve the log files or `y` to delete the log files during the install and uninstall phases. The default value for this setting is `n` (no).	`CLEAR_LOGS`

Performing a silent installation

About this task

This procedure describes how to perform a silent installation of the Avaya Multimedia Messaging server.

The silent installation consists of configuring most of the settings in a properties file, instead of using the installation and the configuration menu for every item.

The properties file is called `installation.properties`. It contains the same settings that you configure during the interactive installation. The settings are grouped and the file contains comments that describe the settings.

Note:

The properties file does not contain settings for the following elements:

- The Avaya Multimedia Messaging cluster
- The Gluster file system
- The SSH RSA configuration

You must configure these settings using the configuration utility after the silent installation is complete.

If errors occur after the installation, you can use the configuration utility to re-configure some of the settings.

Procedure

1. Extract the template file from the Avaya Multimedia Messaging binary file.

```
./amm-<version>.bin --tar xf -- ./installation.properties
```

2. Edit the `installation.properties` file and configure the settings as described in the chapter Avaya Multimedia Messaging server configuration with the configuration utility on page 94.

Note:

You can leave some of the settings blank only if you configure them using the configuration utility after the installation is complete.

3. Run the Avaya Multimedia Messaging binary with a parameter that represents the full path to the properties file.

   For example:

   ```
   sudo ./amm-<version>.bin /home/avaya/installation.properties
   ```

4. **(Optional)** To start the Avaya Multimedia Messaging service, run the following command:

   ```
   svc amm start
   ```

5. Run the Avaya Multimedia Messaging configuration utility to configure the remaining items.

Avaya Multimedia Messaging cluster installation

An Avaya Multimedia Messaging cluster requires Avaya Multimedia Messaging servers that belong to the same network, configured as follows:

- One initial node, also known as a seed node.
- One to three additional nodes

The installation of a cluster consists of installing the Avaya Multimedia Messaging server on all the nodes, by following a process similar to the single-server installation, while also configuring cluster-specific details.

The prerequisites for installing an Avaya Multimedia Messaging cluster are the same as for installing an individual Avaya Multimedia Messaging server. For deployments on VMware virtual machines, the only prerequisite is installing the OVA image for every node in the cluster.

Important:

For redundancy, you require multiple nodes and a virtual IP address or an external load balancer. The client applications use the FQDN that resolves to the virtual IP address or the FQDN of the load balancer to gain access to the Avaya Multimedia Messaging server.

If you use the embedded Avaya Multimedia Messaging load balancing mechanism, you must configure a virtual IP master node and a virtual IP backup node. The virtual IP address must be in the same subnet as the Avaya Multimedia Messaging nodes.

- The virtual IP master node is the initial node and handles the Avaya Multimedia Messaging requests by default.
- The virtual IP backup node is an additional node that handles the load balancing functions when the master node is not functioning.

Important:

If Avaya Multimedia Messaging is federated with Presence Services, ensure that there is network connectivity between every Avaya Multimedia Messaging node and the Presence Server.

Warning:

The connection from the Avaya Multimedia Messaging to the remote domain must be established through the virtual IP.

Installing an Avaya Multimedia Messaging cluster

About this task

Use this procedure to install an Avaya Multimedia Messaging cluster.

Before you begin

Ensure that you understand the Avaya Multimedia Messaging prerequisites. The prerequisites for installing an Avaya Multimedia Messaging cluster are the same as for installing an individual Avaya Multimedia Messaging server.

Note:

The Avaya Multimedia Messaging cluster must be installed by a Linux user with sudo privileges, created during the pre-configuration setup. The User ID (UID) of the Linux user that performs the installation must be the same on all the Avaya Multimedia Messaging nodes. After a user is configured, run the following command to display the ID of the user:

```
id -u <user_name>
```

For example:

```
id -u ammapp
```

Procedure

1. Install the initial node.
2. Install one or more additional nodes.

   Important:

   Proceed with the next steps only after installing all the Avaya Multimedia Messaging nodes.

3. After all the required cluster nodes are installed, perform the following actions on the Avaya Multimedia Messaging initial node to configure the SSH/RSA Public/Private keys:

   a. To open the Avaya Multimedia Messaging configuration utility, run the following command:

   ```
   app configure
   ```

   b. Select **Clustering Configuration** > **Cluster Utilities** > **Configure SSH/RSA Public/Private Keys**.

The system displays the other nodes that are configured in the cluster.

c. Ensure that the list of nodes is complete and enter `n` (no).

d. When the system prompts you to enter a user name for a host, enter the Linux user that was used to install the Avaya Multimedia Messaging installation.

e. If the system prompts you to replace the existing keys, enter `y` (yes).

f. If the system displays the following error, enter `y` (yes):

```
The authenticity of the host can't be established.
```

g. When the system prompts you to enter a password for a host, enter the password of the Linux user that was used to install the Avaya Multimedia Messaging installation.

h. When the configuration is complete, press `Enter` and exit the configuration menu.

4. **(Optional)** If your deployment includes Microsoft federation, use the configuration utility to import the Lync or Skype for Business server certificate.

5. **(Optional)** Start every node in the cluster individually.

   Using a Linux shell for each Avaya Multimedia Messaging server in the cluster, run the following command:

```
svc amm start
```

6. **(Optional)** Perform the following actions on every Avaya Multimedia Messaging node to create a cluster of Openfire servers.

   ❗ **Important:**

   A cluster of Openfire servers is required only if Avaya Multimedia Messaging is federated with Presence Services using XMPP configurations.

   a. Run the Avaya Multimedia Messaging configuration utility:

```
app configure
```

   b. Select **Clustering Configuration** > **Cluster Utilities** > **Utility to configure Openfire for cluster operation**.

   ✳ **Note:**

   If the Avaya Multimedia Messaging topology changes in time, you must run the Openfire utility once more on each node, to ensure that the Openfire configuration is updated accordingly.

Related links

Installing the initial cluster node on page 83
Installing an additional cluster node on page 84
Importing the Lync or Skype for Business front-end server certificate into the trust store on page 132
Software-only deployment checklist on page 33

Installing the initial cluster node

About this task

The installation of a cluster consists of installing the Avaya Multimedia Messaging server on all the nodes, by following the same process as for single-server deployments, while also configuring cluster-specific details.

The following procedure describes how to configure the installation settings that are specific to the initial node in a cluster.

Procedure

1. Run the Avaya Multimedia Messaging installer.
2. Select the **Cluster Configuration** menu and ensure that:
   - The **Initial cluster node** option is set to `y` (yes).
   - The **Local Node IP address** option is set to the IP address of the node.
3. Select **Return to Main Menu** and press `Enter` to return to the previous menu.
4. **(Optional)** In the **Cassandra Encryption** menu, enable or disable SSL encryption for internode communication between the database servers on the Avaya Multimedia Messaging nodes.
5. Select the **Front-end host, System Manager and Certificates configuration** menu and configure the settings that are accessible from the menu.

   Use the information provided in the tables in previous sections.

   Important:

   - For a cluster deployment, you must configure the front-end FQDN as the FQDN of the virtual IP address. If an external load balancer is used, set this value to the FQDN of the load balancer.
   - You can also configure the Front-end host, System Manager and certificates settings at a later time, by running the Avaya Multimedia Messaging configuration utility.

     If Cassandra internode encryption is enabled, you must make the configuration settings from this menu during the initial installation phase and not at a later time.
6. Select **Continue** until the Avaya Multimedia Messaging installation starts and accept the End-User License Agreement.

   The installation takes approximately 10 minutes to complete.

   The system displays a new configuration menu for further configuration of the Avaya Multimedia Messaging server.

   The configuration menu is also accessible at a later time, by running the Avaya Multimedia Messaging configuration utility.

7. Perform the LDAP configuration followed by the messaging domain configuration.

   Important:

   The LDAP configuration for the cluster is performed during the installation of the initial node. Additional configuration on each of the additional nodes is not required.

8. Select **Clustering Configuration** > **Virtual IP Configuration** to enable the usage of a virtual IP address.

   Important:

   The virtual IP address is used for redundancy management, which is supported for three or more Avaya Multimedia Messaging nodes.

   If you use an external load balancer, configuring a virtual IP address is not necessary.

   If you use an external load balancer, you must configure the Avaya Multimedia Messaging Front-end host as the FQDN of the load balancer.

   If you set **Enable virtual IP** to `y` (yes), the system displays new configuration options for the virtual IP address.

   Important:

   Write down the virtual IP authentication password. You need this password for configuring the virtual IP backup node.

Next steps

- Install additional cluster nodes.
- Configure the SSH/RSA Public/Private keys.
- Create a cluster of Openfire servers

Related links

Installing the Avaya Multimedia Messaging server on customer-provided systems on page 48
Avaya Multimedia Messaging initial installation configuration on page 73
Configuring the Avaya Multimedia Messaging server using the configuration utility on page 95
Importing the secure LDAP certificate using the configuration utility on page 129
LDAP configuration on page 100
Messaging domains configuration on page 117
Virtual IP configuration options on page 87

Installing an additional cluster node

About this task

The installation of a cluster consists of installing the Avaya Multimedia Messaging server on all the nodes, by following the same process as for single-server deployments, while also configuring cluster-specific details.

The following procedure describes how to configure the installation settings that are specific to an additional node in a cluster.

⚠ **Warning:**

> If you have an existing standalone server or cluster that has been running for more than a few days, and wish to add a new node, the integration of the new node can take much time. The amount of time depends on factors such as the Ethernet connectivity of the system and the amount of existing messaging data in the system. The data transfer from the existing system to the new nodes might reach values such as 5 MB/second if the connectivity is low.
>
> To prevent this issue, see Rebalancing the Gluster file system after adding a new node on page 92.

Before you begin

You must use the Avaya Multimedia Messaging management portal **Cluster Status** page to ensure that all of the cluster nodes are in service.

Procedure

1. Run the Avaya Multimedia Messaging installer.

   For information about installing the Avaya Multimedia Messaging server, see Installing the Avaya Multimedia Messaging server on customer-provided systems on page 48.

   ⚠ **Warning:**

   > You must not configure the LDAP settings on the additional node. The LDAP configuration is automatically configured for the additional nodes.

2. Select **Cluster Configuration** and perform the following actions:

   a. Set the **Initial cluster node** option to `n` (no).

   b. Ensure that the **Local Node IP address** option is set to the IP address of the current node.

   c. Set the **Cluster seed node** to the IP address of the initial node.

   d. Set the **User ID (UID) of product user on seed node** to the ID of the Linux user that was used to install the initial Avaya Multimedia Messaging.

   e. Set the **Cassandra database user name** to the Cassandra user name configured during the installation of the seed node.

   f. Set the **Cassandra database password** to the Cassandra password configured during the installation of the seed node.

3. Select **Return to Main Menu** and press `Enter` to return to the previous menu.

4. **(Optional)** Select **Cassandra Encryption** > **Enable inter-node encryption for Cassandra cluster node** to enable or disable SSL encryption for internode communication between the database servers on the Avaya Multimedia Messaging nodes.

5. Select the **Front-end host, System Manager and Certificates configuration** menu and configure the settings that are accessible from the menu.

You can also configure the Front-end host, System Manager and certificates settings at a later time, by running the Avaya Multimedia Messaging configuration utility.

⚠ **Warning:**

If Cassandra internode encryption is enabled, you must make the configuration settings from this menu during the initial installation phase and not at a later time.

6. Select **Continue** until the Avaya Multimedia Messaging installation starts and accept the End-User License Agreement.

   The installation takes approximately 10 minutes to complete.

   The system displays a new configuration menu for further configuration of the Avaya Multimedia Messaging server.

   The configuration menu is also accessible at a later time by running the Avaya Multimedia Messaging configuration utility.

7. **(Optional)** Select **Clustering Configuration** > **Virtual IP Configuration** > **Enable Virtual IP** menu to enable or disable the usage of a virtual IP address.

   ❗ **Important:**

   The virtual IP address is used for redundancy management, which is supported for three or more Avaya Multimedia Messaging nodes.

   If you use an external load balancer, configuring a virtual IP address is not necessary.

   If you use an external load balancer, you must configure the Avaya Multimedia Messaging Front-end host as the FQDN of the load balancer.

   If you set **Enable virtual IP** to `y` (yes), the system displays new configuration options for the virtual IP address.

   ✱ **Note:**

   The virtual IP address must be enabled only for the two nodes that handle load balancing and you must set “only one of the additional nodes” as a virtual IP backup node.

   The backup node is a node that has **Enable virtual IP** set to `y` (yes) and **Virtual IP master node** set to `n` (no).

   For information about virtual IP configuration values, see Virtual IP configuration options on page 87.

Next steps

- Install other additional nodes, if required
- Configure the SSH/RSA Public/Private keys
- Create a cluster of Openfire servers

For information about rebalancing the Gluster File System, see Rebalancing the Gluster File System after adding a node on page 92.

Virtual IP configuration options

Option	Description
Virtual IP address	The virtual IP address shared by all the cluster nodes.
Virtual IP interface	The network interface used for the virtual IP address. Unless you are using a configuration that has multiple Ethernet interfaces, you must set this value to `eth0` (Ethernet-zero).
Virtual IP master node	Determines if the current node is the virtual IP master node. As the initial node of the cluster is usually designated the virtual IP master, set this value to `n` (no) on the second node.
Virtual IP router ID	An integer with a value from 1 to 255. The value must be the same for both virtual IP master and backup. The default value is 51. This value must be unique across Virtual Router Redundancy Protocol (VRRP) installations.
Virtual IP authentication password	The password that the backup node uses for authentication. This password must be the same as the virtual IP authentication password configured for the initial node.

Adding a new node while performing an Avaya Multimedia Messaging upgrade

About this task

The following procedure summarizes the actions that you must perform if you need to add a new node to a cluster during an upgrade.

Note:

All nodes in the cluster must run the same Avaya Multimedia Messaging version.

Procedure

1. Upgrade all nodes in the cluster to the latest Avaya Multimedia Messaging version.

   For information about upgrading the Avaya Multimedia Messaging server, see *Administering Avaya Multimedia Messaging*.

2. To install the new node using an Avaya-provided OVA, do the following:

   a. Install the Avaya Multimedia Messaging OVA image.

   b. Download the latest Avaya Multimedia Messaging version and use this version for the installation, instead of the binary that is already present on the OVA image.

   c. Install as described in Installing an additional node on page 84.

3. To install a new node on your own RHEL 7.3 physical server or virtual machine, download the latest Avaya Multimedia Messaging binary and install as described in Installing an additional node on page 84.

Changing the Cassandra user name and password

About this task

The following task describes how to change the Cassandra database user name and password after the installation of an Avaya Multimedia Messaging cluster.

Procedure

1. On the seed node, perform the following actions:
    a. Run the Avaya Multimedia Messaging configuration utility.

    ```
    app configure
    ```

    b. Select **Cassandra DB User and Password**.

    c. Select **Current Cassandra Database User Name** and enter the current user name.

    d. Select **Current Cassandra Database Password** and enter the current password.

    e. Select **New Cassandra Database User Name** and enter the new user name.

    f. Select **New Cassandra Database User Password** and enter the new password.

    g. Select **Apply**.

2. On every additional node, perform the following actions:
    a. Run the **`cassandraSetPassword`** command by specifying the new user name and password as parameters.

    ```
    sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/cassandra/
    cassandraSetPassword.sh <new user name> <new password>
    ```

    b. Restart the Avaya Multimedia Messaging service.

    ```
    svc amm restart
    ```

Changing the LDAP parameters after installing an Avaya Multimedia Messaging cluster

About this task

You can change the LDAP configuration by running the Avaya Multimedia Messaging configuration utility or by using the Avaya Multimedia Messaging administration portal.

The LDAP reconfiguration is performed locally on one Avaya Multimedia Messaging node by running a script that synchronizes the LDAP configuration through all the cluster nodes.

The following procedure describes how to change the LDAP parameters after an Avaya Multimedia Messaging cluster is installed.

Procedure

1. Change the LDAP configuration by performing one of the following actions on one of the Avaya Multimedia Messaging cluster nodes:
   - Run the `configureAMM.sh` script and select **LDAP Configuration**.
   - Log in to the administration portal and select **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.
2. Restart each node in the Avaya Multimedia Messaging cluster.

Changing the seed node of a cluster

About this task

Use this procedure to change the seed node only if you need to decommission the seed node. If you are not installing a new node but assigning the seed node function to an existing node, follow the procedure starting with Step 2.

The Gluster File System is unaware of the existence of a seed node. However, you must still configure Gluster for the new seed node and move the data to the new node.

Note:

Before running the `setSeedNode` script, disable the virtual IP on the node so that the new seed node can be set as the virtual IP master afterwards.

Procedure

1. Install the new node as an additional cluster node.
2. Log on to the new node and run the **`setSeedNode.sh`** script.

   For example:

   ```
   sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/misc/setSeedNode.sh
   ```
3. Log on to each of the other cluster nodes and run the **`setSeedNode.sh`** script with the IP address of the new seed node as a parameter.

   For example:

   ```
   sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/misc/setSeedNode.sh
   1.2.3.40
   ```
4. Restart the Avaya Multimedia Messaging service on the new seed node.

   ```
   svc amm restart
   ```
5. Restart the Avaya Multimedia Messaging service on the other cluster nodes.

   ```
   svc amm restart
   ```

Next steps

- Disable the virtual IP on the old seed node.
- Configure the new node to be the virtual IP Master node. The initial node of the cluster is usually designated as the virtual IP master node.

- If required, remove the former seed node.

Related links

Installing an additional cluster node on page 84
Installing the initial cluster node on page 83
Removing a node from an Avaya Multimedia Messaging cluster on page 90

Removing a node from an Avaya Multimedia Messaging cluster

About this task

This procedure describes how to remove a node from an Avaya Multimedia Messaging cluster. You cannot remove a node if the system contains only one node.

The removal of a node involves copying files and reallocating brick replicas onto the remaining nodes. These processes can take several hours depending on the size of the files.

Important:

Although files are copied onto the remaining nodes, they also remain on the node you are removing. Take this into consideration when disposing of hardware.

Procedure

1. Log in to the CLI of an Avaya Multimedia Messaging node that will remain in the cluster.
2. Run the following command:

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

   In this command, `<IP>` is the IP address of the node that must be removed from the cluster.
3. If prompted, enter the SSH and sudo passwords.

   Note:

   You might be prompted for these passwords several times.
4. When you receive the prompt `Removing brick(s) can result in data loss. Do you want to continue? (y/n)` to confirm brick deletion, enter `y`.
5. Log in to the CLI of the Avaya Multimedia Messaging node that you are removing form the cluster.
6. Run the `app uninstall` command.
7. Restart each node that will remain in the cluster using the `svc amm restart` command.

Gluster setup

Creating a Gluster file system

About this task

After installing Avaya Multimedia Messaging, use this procedure to build a new Gluster file system.

Important:

Do *not* install a Gluster file system in an AWS environment.

All **`.sh`** commands in this procedure are located at `/opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/glusterfs`.

Before you begin

- When building a Gluster file system, ensure that all nodes have the same disk size.
- You must deploy all nodes in the cluster before building a Gluster file system.

Procedure

To build a new Gluster file system, run the following command:

```
./glusterInstall.sh <IP1> <IP2>
```

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

For example, `./glusterInstall.sh 10.136.5.211 10.136.5.212 10.136.5.213` constructs a Gluster file system with three nodes.

Note:

`./glusterInstall.sh` can be run from any of the nodes involved.

Expanding a Gluster file system

About this task

This procedure describes how to expand an existing Gluster file system by adding a new node.

All **`.sh`** commands in this procedure are located at `/opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/glusterfs`.

Before you begin

When adding nodes, do not use machines with disk sizes that are smaller than the ones in the existing nodes.

Procedure

1. To add a new node to an existing Gluster file system, run the following command: `./glusterAdd.sh <NewIP> <ExistingIP>`

   In this command, `<NewIP>` is the IP address of the new node, and `<ExistingIP>` is the IP address of any node that is already part of the file system.

   Note:

   `./glusterAdd.sh` must be run from an existing node that is already in the file system. It cannot be run from the new node.

2. When prompted, enter the password that was used to log in.

   While the commands run, they will need the password to perform an operation on a different node.

Next steps

Rebalance the Gluster file system.

Rebalancing the Gluster file system after adding a new node

About this task

As part of adding a new node to an Avaya Multimedia Messaging cluster, messaging data in the Cassandra database is automatically rebalanced to include the new node. After the node installation is complete, the attachment data stored in the Gluster File System can also be rebalanced. Both of these operations can be time-consuming.

To minimize the impact of rebalancing, it is recommended that old conversations be removed prior to adding the new node. Rebalancing the Gluster file system data can be done as a background task after resuming service.

Although the Gluster file system is operational during the process, rebalancing generates a lot of disk traffic, and must be performed when the system is less busy. If several nodes are added, it is more efficient to add them all and then rebalance at the end.

The following commands can be issued from any node in the file system.

Before you begin

After installing a new node to a standalone node or cluster that had existing attachment data, the system places new attachments in a balanced manner on all nodes, but the existing attachment data is not automatically rebalanced onto the new node. The following procedure describes how to balance the attachment data across all nodes.

Procedure

1. To start rebalancing, run the following command:

   ```
   sudo gluster volume rebalance cs_volume start
   ```

2. **(Optional)** To check the rebalancing status, run the following command:

   ```
   sudo gluster volume rebalance cs_volume status
   ```

Uninstalling the Avaya Multimedia Messaging server

About this task

The following procedure describes how to uninstall an Avaya Multimedia Messaging server that can be part of a single-server deployment or part of a cluster.

Important:

If the Avaya Multimedia Messaging was upgraded to a newer version, the following procedure removes the latest version. For information about restoring to a previous version, see *Administering Avaya Multimedia Messaging*.

Before you begin

To uninstall an Avaya Multimedia Messaging cluster, you must decommission the additional nodes first, and the seed node last. For more information about removing an Avaya Multimedia Messaging node from a cluster, see Removing a node from the Avaya Multimedia Messaging cluster on page 90.

Procedure

In the Avaya Multimedia Messaging server CLI, run the following command:

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

Chapter 5: Avaya Multimedia Messaging server configuration with the configuration utility

The following table summarizes the server configuration tasks that you must perform during or after the installation of the Avaya Multimedia Messaging server for each of the deployment models presented.

Table 6: Summary of server configuration tasks

Task	Software-only application		Avaya-provided OVA installations	
	Single server	Cluster	Single server	Cluster
Configure Front-end host, System Manager and certificate configuration Certificates can be: • Managed by System Manager • Local certificates • Intermediate CA certificates Perform the task that corresponds to the certificate type that you use.	If not configured during the initial installation phase.	If not configured during the initial installation phase. Repeat for every node in the cluster.	If not configured during the initial installation phase.	If not configured during the initial installation phase. Repeat for every node in the cluster.
LDAP configuration Messaging domains configuration Cassandra DB username and password	Y	Y — once, on the seed node	Y	Y — once, on the seed node
Clustering Configuration	N	Y Perform tasks as indicated in the Cluster installation section.	N	Y Perform tasks as indicated in the Cluster installation section.

Configuring the Avaya Multimedia Messaging server using the configuration utility

About this task

You can gain access to the configuration menu of the Avaya Multimedia Messaging server during the installation process, after you accept the EULA, or at a later time, if you must update the configuration settings of the Avaya Multimedia Messaging server.

If you perform a silent installation, you need to provide most of the configuration settings in the installation properties file and use the configuration script to configure the cluster, the Gluster File System, and the SSH settings.

Procedure

1. **(Optional)** Run the Avaya Multimedia Messaging configuration utility using the `app configure` command.

   ```
   app configure
   ```

   ❗ **Important:**

   Perform this step only if you run the configuration utility at a later time after the installation.

   During the installation, the configuration menu is displayed after you accept the EULA.

   The script checks the current configuration of the Avaya Multimedia Messaging server and opens the configuration menu.
2. Provide the required configuration settings.
3. Select **Continue** and press **Enter**.

Next steps

The following settings are mandatory for an Avaya Multimedia Messaging installation:

- Front-end host, System Manager and certificate configuration, if not configured during the initial installation phase.
- LDAP authentication parameters.
- Messaging domains configuration.
- Cassandra username and password.
- Cluster configuration, mandatory if you are deploying an Avaya Multimedia Messaging cluster.
- Leave **CORS Configuration** and **Serviceability Agent Configuration** unchanged.

To configure advanced settings, such as certificate warning period, security banner, or re-run the firewall configuration script, select the **Advanced Configuration** menu option.

Important:

After you configure the mandatory settings, you must restart the Avaya Multimedia Messaging service:

```
svc amm restart
```

If there are other settings that you must configure after restarting the Avaya Multimedia Messaging server, you can run the configuration utility as described in *Step 1* and gain access to the required configuration settings.

Front-end host, System Manager, and certificate configuration

Use the following table as an aid for configuring the front-end host, System Manager, and certificate related settings.

If you do not select the **Front-end host, System Manager and Certificate Configuration** option during the installation, then the self-signed certificates are automatically generated. Self-signed certificates are also generated when:

- The **System Manager FQDN** option is not set.
- The **Use System Manager for certificates** option is set to `n`.
- Certificates were not provided for one of the interfaces: REST, OAMP, LYNC, or NODE.

You can modify certificate configuration settings from the administration portal anytime. This is useful if you do not complete the certificate configuration as part of the initial setup process or if you generate certificates at a later time.

For information about managing certificates through the Avaya Multimedia Messaging administration portal, see *Administering Avaya Multimedia Messaging*.

Warning:

Changing the System Manager Server FQDN after the installation will invalidate existing users data in the system, if the FQDN points to a System Manager server that contains a different set of users. You must change the FQDN only when switching to another replicated instance of the current System Manager. For any other situation, you must reinstall the Avaya Multimedia Messaging system.

Table 7: Front-end host, System Manager and Certificate Configuration settings

Item name	Description	Equivalent properties file parameter
Front-end FQDN	The front-end **FQDN** of the Avaya Multimedia Messaging server. For a cluster deployment, you must configure the front-end FQDN as the FQDN of the virtual IP address. If an	`REST_FRONTEND_HOST`

Table continues…

Item name	Description	Equivalent properties file parameter
	external load balancer is used, set this value to the FQDN of the load balancer. The front-end FQDN is the address that end-user clients use to access the services provided by Avaya Multimedia Messaging . The default value depends on the configuration present in the `/etc/hosts` file of the Avaya Multimedia Messaging server. ✱ **Note:** If you install the Avaya Multimedia Messaging server with the FQDN as the front-end address, the Message Playback feature must also be accessed using the FQDN of the Avaya Multimedia Messaging server.	
System Manager FQDN	The FQDN of the Avaya Aura® System Manager that signs the Avaya Multimedia Messaging certificates.	`SYSTEM_MGR_IP`
System Manager web admin username	The System Manager web administration portal user name. This field is optional.	`SMGR_USER_NAME`
System Manager web admin password	The System Manager web administration portal password. This field is optional.	`SMGR_USER_PASSWORD`
System Manager web version	The version number of Avaya Aura® System Manager.	`SYSTEM_MGR_VERSION`
System Manager HTTPS Port	The HTTPS port used for the Alarm Agent for the current Avaya Multimedia Messaging server. The default value for this setting is 443.	`SYSTEM_MGR_HTTPS_PORT`
System Manager Enrollment Password	The Avaya Aura® System Manager enrollment password.	`SYSTEM_MGR_PW`
Override port for reverse proxy	Specifies if you use an external reverse proxy server. Enable this setting only if clients will not be connecting directly to the Avaya Multimedia Messaging server, but rather	`OVERRIDE_FRONTEND_PORT` For the **Front-end port for reverse proxy** setting, the equivalent parameter is `REST_FRONTEND_PORT`.

Table continues…

Item name	Description	Equivalent properties file parameter
	using a proxy server as part of a remote access solution that is configured to receive connections on a port other than default port 443. Select `y` (yes) to configure the port for the reverse proxy server or `n` (no) to keep the default configuration that remains disabled. If you select `y` (yes), the menu displays a new setting for the reverse proxy port: **Front-end port for reverse proxy**. **Note:** If this parameter is changed after the installation, all of the nodes in a cluster must be restarted using the `svc amm restart` command to apply the change.	
Use System Manager for certificates	Specifies if the certificates are retrieved from Avaya Aura® System Manager or from imported files. Select `y` (yes) to retrieve certificates from Avaya Aura® System Manager or `n` (no) to retrieve certificates from imported files. If you select `n` (no), the menu displays new settings for configuring the certificate files. To configure the certificate settings, you must provide the complete file path name to the: • REST interface key file • REST interface certificate file • SIP interface key file • SIP interface certificate file • OAM interface key file • OAM interface certificate file • node key file • node certificate file • signing authority certificate file	`USE_SMGR` If the `USE_SMGR` option is set to `n` (no), you must configure the following parameters for importing the certificate files: • `REST_KEY_FILE` • `REST_CRT_FILE` • `SIP_KEY_FILE` • `SIP_CERT_FILE` • `OAM_KEY_FILE` • `OAM_CRT_FILE` • `NODE_KEY_FILE` • `NODE_CRT_FILE` • `CA_CRT_FILE`
Local frontend host	The local FQDN of the node.	`LOCAL_FRONTEND_HOST`

Table continues…

Item name	Description	Equivalent properties file parameter
	This FQDN is not used for a client to access services, but is used to access the server within the enterprise, and is bound to the same Ethernet port as the front-end FQDN. The Avaya Multimedia Messaging configuration utility uses this value to generate certificates for the node. **Important:** In a clustered configuration, the local front-end host is different from one node to the other and is also different from the front-end FQDN. In a non-clustered environment, the local front-end host is usually different from the front-end FQDN to create a clustered configuration from a non-clustered configuration.	
Keystore password	The keystore password for the MSS and Tomcat Avaya Multimedia Messaging certificates. The minimum length for this password is 6 characters. The characters supported for the keystore password are: • a to z • A to Z • 0 to 9 • other supported characters: exclamation point (!), at symbol (@), hash (#), percent sign (%), caret (^), star (*), question mark (?), underscore (_), dot (.)	`KEYSTORE_PW`

Configuring the Avaya Multimedia Messaging server to connect to a secondary System Manager node

About this task

If a secondary System Manager node is activated, you must configure the Avaya Multimedia Messaging server manually to connect to the second node.

Procedure

1. If Avaya Multimedia Messaging is deployed in a cluster, ensure that all the Avaya Multimedia Messaging server nodes are running.
2. On every Avaya Multimedia Messaging node, run the configuration utility.

   ```
   app configure
   ```

3. Select **Front-end host, System Manager and certificates configuration** and edit the System Manager FQDN and enrollment password.
4. Select **Apply** and then press `Enter`.

LDAP configuration

If you do not complete LDAP configuration during the initial Avaya Multimedia Messaging setup, then you can complete it later using the Avaya Multimedia Messaging administration portal as described in *Administering Avaya Multimedia Messaging*.

⚠ **Warning:**

Changing the LDAP configuration parameters, other than *Bind DN* and *Bind Credential*, when they are configured, might invalidate the existing user data. For example, changing how user roles are found can remove one or more roles from the existing user, which will block the user from accessing the Avaya Multimedia Messaging system. In addition, do not change the server URL unless you need to switch the configuration to another replicated instance of the current LDAP directory. In all the other cases, you must reinstall the Avaya Multimedia Messaging system.

Table 8: LDAP configuration settings

Item name	Description	Equivalent properties file parameter
Load LDAP properties from file	The **Load LDAP properties from file** menu contains an item called **Path to properties file**. You can create a Java properties file that contains the LDAP properties instead of entering the LDAP configuration settings manually. The **Path to properties file** option is for configuring the absolute path to this file. The LDAP properties file must contain the *equivalent properties file parameters* specified in this table. The default value for this setting is `<install_dir>/config/`	pathToLdapPropertiesFile

Table continues…

Item name	Description	Equivalent properties file parameter
	`ldap.properties`, where `<install_dir>` is the Avaya Multimedia Messaging installation directory.	
Import Secure LDAP trusted certificate	The **Import Secure LDAP trusted certificate** menu contains the following items: • **Certificate file**: The path and filename for the LDAP trusted certificate. The certificate file must be in the .PEM format. • **Truststore Password**: The password for Tomcat truststore. ❗ **Important:** Only configure these settings if you need a Secure LDAP connection.	LDAP_TRUSTSTORE_CERTFILE LDAP_TRUSTSTORE_PASSWORD
Directory Type	The LDAP directory type of the enterprise. The supported directory types are the following: • Microsoft Active Directory 2008, 2012, and 2016 • Microsoft Active Directory Lightweight Directory Services (AD-LDS) • IBM Domino Server 7.0 ✳ **Note:** The Domino server must be patched to support TLS, so Avaya Multimedia Messaging can connect to the Domino server through secure LDAP (LDAPS). For a list of supported patch fixes, see https://www-10.lotus.com/ldd/dominowiki.nsf/dx/IBM_Domino_TLS_1.0. • Novell e-Directory 8.8 • OpenLDAP 2.4 • Oracle Directory Server Enterprise Edition 11g Release 1 (11.1.1.7.0)	ldapType

Table continues…

Item name	Description	Equivalent properties file parameter
	For detailed information about supported product releases, see the Avaya Compatibility Matrix.	

URL for LDAP server	The URL for gaining access to the LDAP server. This is a mandatory setting.
	The URL must have the following format:
	`<protocol>://<LDAP server FQDN or IP address>:<port>`
	For example:
	`ldap://myserver.mycompany.com:3268`
	`ldaps://myserver.mycompany.com:3269`
	The protocol can be LDAP or LDAPS, depending on the LDAP server type.
	For Microsoft Active Directory, use the catalog LDAP ports.
	The default global catalog LDAP port values are 3268 for LDAP and 3269 for LDAPS.
	The default domain LDAP ports values are 389 for LDAP and 636 for LDAPS.
	Note:
	If an FQDN is used to specify the LDAP server, the enterprise might map the FQDN to multiple, replicated LDAP servers using the DNS round-robin mechanism as an attempt for load-balance and for redundancy purpose. Sporadic authentication failures can occur if one of the LDAP servers is offline and the DNS round-robin mechanism resolves the FQDN to the IP of the LDAP server that is offline.
	If this outcome cannot be tolerated, a more reliable load-balancing mechanism, such as a dedicated load-balancer in front of the LDAP servers, will be needed.
	For Active Directory, use the *Global Catalog service port* instead of the default LDAP/LDAPS ports.
		ldapUrl

Table continues…

Item name	Description	Equivalent properties file parameter
Bind DN	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. **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.	bindDN
Bind Credential	The password that the Avaya Multimedia Messaging server requires for the LDAP bind operation. This is a mandatory setting.	bindCredential **Important:** If you configure the LDAP settings using the properties file, you must enter the Bind Credential manually by running the **`configureAMM.sh`** script.
UID Attribute ID	The User ID attribute name, as determined by the LDAP server configuration. This is a mandatory setting. This parameter is used for searching users in the LDAP server. For example: `sAMAccountName`	uidAttrID
Base Context DN	The DN of the context used for LDAP authentication. For example: `ou=ammsusers,dc=example,dc=com`	baseCtxDN
Administrator Role	The list of LDAP roles that match the Avaya Multimedia Messaging Administrator role. For example:	adminRole

Table continues…

Item name	Description	Equivalent properties file parameter
	If the role is configured as `AMMAdmin,AMMxyz`, any user whose list of roles contains `AMMAdmin` or `AMMxyz` is mapped to the Avaya Multimedia Messaging Administrator role. **Note:** The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user in order for the mapping of the LDAP roles to the Avaya Multimedia Messaging application roles to succeed. **Important:** To avoid situations when potential loss of credentials could impact the administration tasks, Avaya recommends creating more than one user account with administrator privileges.	
Security Administrator Role	The list of LDAP roles that match the Avaya Multimedia Messaging Security Administrator role. For example: If the role is configured as `AMMSecurityAdmin,AMMxyz`, any user whose list of roles contains `AMMSecurityAdmin` or `AMMxyz` is mapped to the Avaya Multimedia Messaging Security Administrator role. **Note:** The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the role name found for a user in order for the mapping of the LDAP roles to the Avaya Multimedia Messaging application roles to succeed.	securityAdminRole
Auditor Role	The list of LDAP roles that match the Avaya Multimedia Messaging Auditor role.	auditorRole

Table continues…

Item name	Description	Equivalent properties file parameter
	For example: If the Auditor role is configured as `AMMAuditor,AMMxyz`, any user whose list of roles contains the `AMMAuditor` or `AMMxyz` role is mapped to the Avaya Multimedia Messaging AUDITOR role. ✱ **Note:** The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user in order for the mapping of the LDAP roles to the Avaya Multimedia Messaging application roles to succeed.	
User Role	The list of LDAP roles that match the Avaya Multimedia Messaging User role. For example: If the User role is configured as `AAMMUser,AMMxyz`, any user whose list of roles contains the `AAMMUser` or `AMMxyz` role is mapped to the Avaya Multimedia Messaging USER role. ✱ **Note:** The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user for the mapping of the LDAP roles to the Avaya Multimedia Messaging application roles to succeed.	usersRole
Services Administrator Role	The list of LDAP roles that match the Services Administrator role. For example: If the User role is configured as `AAMMUser,AMMxyz`, any user whose list of roles contains the `AAMMUser` or `AMMxyz` role is mapped to the Avaya Multimedia Messaging Services Administrator role.	serviceAdminRole

Table continues…

Item name	Description	Equivalent properties file parameter
	Note: The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user for the mapping of the LDAP roles to the Avaya Multimedia Messaging application roles to succeed.	
Maintenance and Support Role	The list of LDAP roles that match the Maintenance and Support role. For example: If the User role is configured as `AAMMUser,AMMxyz`, any user whose list of roles contains the `AAMMUser` or `AMMxyz` role is mapped to the Avaya Multimedia Messaging Maintenance and Support role. **Note:** The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user for the mapping of the LDAP roles to the Avaya Multimedia Messaging application roles to succeed.	serviceMaintenanceRole
Advanced LDAP parameters	The menu that contains advanced LDAP parameters to configure depending on the structure of the LDAP server.	
Test User	If you select testUser and select **Apply**, this option is used to validate the following LDAP settings: • Verifies that the user is searchable with a given base DN and search filter. • Lists the group to which the user belongs — user, administrator, or auditor. • Validates the values for Role Attribute ID and Role Name Attribute. • Verifies the Last Updated Time attribute, role filter syntax, and active users search filter syntax.	testUser

Table continues…

Item name	Description	Equivalent properties file parameter
	The configuration is not saved if any of these validations fail. The testUser parameter is optional. If you do not specify a value, the system skips validation and directly saves the configuration in the database.	

Table 9: Advanced LDAP attributes

The following table contains the LDAP configuration settings accessible through the **Advanced LDAP attributes** menu:

Item name	Description	Equivalent properties file parameter
Role Filter	The string to use for role filtering. The format of the string depends on the LDAP server configuration. For example: `(&(objectClass=group)(member={1}))`	`roleFilter`
Role Attribute ID	The Role Attribute ID parameter has a different meaning, depending on the value of RoleAttributeIsDN: • If RoleAttributeIsDN is true, this is the attribute that contains the DN used to find the object that contains the role name. • If RoleAttributeIsDN is false, this is the name of the attribute that contains the role name. For example: `memberOf`	`roleAttrID`
Roles Context DN	The Roles Context DN to use for searching roles. The roles search in LDAP is performed by using the Roles Context DN in combination with the Role Filter. For example: `ou=ammsusers,dc=example,dc=com`	`rolesCtxDN`

Table continues…

Item name	Description	Equivalent properties file parameter
Role Name Attribute	This parameter has a different meaning, depending on the value of RoleAttributeIsDN: • If RoleAttributeIsDN is true, the value of the attribute set in RoleAttributeID is used to find the object that contains the role and this parameter stores the name of the attribute that contains the role name. • If RoleAttributeIsDN is false, this parameter is ignored. For example: `cn`	`roleNameAttrID`
Role Attribute is DN (true/false)	The setting to determine if the role attribute is stored in the DN or in another object. If you set this parameter to `true`, the role is stored in the attribute defined by the *Role Name Attribute* parameter. If you set this parameter to `false`, the role attribute of the user contains the name of the role.	`roleAttrIsDN`
Role Recursion (0 - 10)	The setting to define the depth of role recursion. If the LDAP configuration contains nested groups, searching through LDAP structures is recursive. Set a value from `0` to `10` to define the depth of recursion, where: • 0 is for disabling recursive search • 10 is for searching through 10 levels in the LDAP structure to find the object that defines the user role to use for Avaya Multimedia Messaging authentication For example: the user jsmith can be in the Sales group, which can	`roleRecursion`

Table continues…

Item name	Description	Equivalent properties file parameter
	be in the AMM users group. In this case, Role Recursion must be set to *at least* 2 for jsmith to be recognized as a member of the AMM users group.	
Allow Empty Passwords (true/false)	The setting to determine if empty passwords are allowed in the LDAP directory.	`allowEmptyPasswords`
Search Scope (0 - 2)	The setting to determine the scope of the role search. The role search starts from the *Role Context DN* and uses the *Role Filter*. The search scope determines the depth of the search as follows: • Level 0, also named OBJECT_SCOPE, indicates that the search is performed only on the named role context. • Level 1, also named ONELEVEL_SCOPE, indicates that the search is performed directly under the named role context. • Level 2, also named SUBTREE_SCOPE, indicates that the search is performed at the named role context and in the sub-tree rooted at the named role context.	`searchScope`
Language used in Directory	The language used in the LDAP directory. The following languages are supported: • Russian • German • Spanish • English • Korean • French • Portuguese	`language`

Table continues…

Item name	Description	Equivalent properties file parameter
	• Simplified Chinese • Japanese • Italian	
Active users search filter	The search filter string used to identify active users. If the LDAP server supports a method of determining whether a user is active, this setting must contain the attribute that determines if a user is active. If this setting is not configured, the Avaya Multimedia Messaging User Management component handles all the users as active users. For example: `(&(objectClass=user)(objectCategory=Person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))`.	`activeUsersFilter`
Last updated time attribute	The attribute indicating the last time an LDAP object was modified, in the ASN.1 Generalized Time Notation. The Avaya Multimedia Messaging User Management component uses this attribute to identify updated users when synchronizing the user data with the LDAP server. If this parameter is not configured, the User Management component compares the data of every user to the data that exists in the LDAP server. **Note:** Configuring this parameter improves the efficiency of the user synchronization process and reduces the	`lastUpdatedTimeAttr`

Table continues…

Item name	Description	Equivalent properties file parameter
	traffic between the Avaya Multimedia Messaging server and the LDAP server during user synchronization.	
Load parameter defaults	The script to load the default values for the parameters.	—

Advanced configuration

Table 10: Advanced configuration settings

Item name	Description	Equivalent properties file parameter
Certificate Warning Period	The number of days before the expiry date of a certificate causes the system to raise an alarm.	`CERT_WARNING_PERIOD`
Maximum Message Count	The maximum message count that the system can return per conversation, when a user performs a database a query to view a conversation. If you set the **Maximum message count in a query** value to NULL, the system uses the default value in the database initialization settings.	`MAX_MESSAGE_COUNT`
OS Security Utility	The menu for configuring the firewall automatically on the current node. Select **Run the firewall configuration script** and press Enter to run the firewall configuration script. Avaya recommends that you run this script to configure the firewall automatically and not perform a manual configuration. ⚠ **Warning:** The firewall configuration script replaces the current configuration of the firewall on the server where you are performing the installation, so you must open any other ports	`RUN_FIREWALL_CONFIG` If you set this parameter to y (yes), the firewall configuration script is run during the silent installation.

Table continues…

Item name	Description	Equivalent properties file parameter
	required for your server manually after you run this script.	
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.	`AVAYA_REQUEST_TIMEOUT`
Configure Host IP for SNMP management	The menu that contains the **IP address for managing this server** setting for configuring the IP address of the Network Interface to use for SNMP.	`SNMP_IP_ADDR`
Security Banner File	The menu for configuring security banner settings. The **Security Banner File** setting must contain the path to the security banner file. The security banner file is a text file that contains the security warnings displayed when a user or administrator logs in to the administration portal or using an SSH console.	`SECURITY_BANNER_PATH`
From Forking Configuration	The option that specifies how the server handles messages for users that use both Avaya Multimedia Messaging and federated Avaya Aura® Presence Services clients. • If you select **true**, messages sent from a client will be available on both clients. • If you select **false**, messages sent from a client will only be available on that client.	—

Table continues…

Item name	Description	Equivalent properties file parameter
Import Presence Services trusted certificate	The menu for downloading a Presence Services certificate that is required to federate Avaya Multimedia Messaging with Presence Services. Usually, you can download Presence Services certificates from Presence Services System Manager.	—
Import Microsoft Lync trusted certificate	The menu for downloading a Microsoft Lync certificate that is required to federate Avaya Multimedia Messaging with Microsoft Lync.	—
Change Application JAVA_HOME setting	The menu for configuring a path to a directory containing the Java Runtime Environment. The default value is `/etc/alternatives/jre`.	—

Configuring the Avaya Multimedia Messaging server firewall

About this task

Use this procedure to reset the firewall settings back to the defaults, or to allow additional ports through the server firewall.

Procedure

1. **(Optional)** Add the required ports to the firewall configuration file `/opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/os/security/firewall.conf`.
2. Run the Avaya Multimedia Messaging configuration utility using the `app configure` command.
3. Select **Advanced Configuration** > **OS Security Utility** > **Run the firewall configuration script**.

   The firewall is configured automatically.

Configuring the Avaya Multimedia Messaging server From Forking

Procedure

1. Run the Avaya Multimedia Messaging configuration utility using the `app configure` command.

2. Click **From Forking Configuration** and choose one of the following:
    - **True**: To enable the configuration.
    - **False**: To disable the configuration.
3. Select **Apply** to finish the configuration.
4. Check the configuration utility log files to ensure that the System Manager configuration is done successfully.

Clustering configuration

The Cluster Configuration menu contains the tools and settings that you must use for configuring the Avaya Multimedia Messaging nodes in a clustered environment.

The Cluster Configuration menu contains the following submenus:

- Cluster Configuration
- Cluster Utilities
- Virtual IP Configuration Settings

Table 11: Cluster Configuration settings

Item name	Description	Equivalent properties file parameter
Enable inter-node encryption for Cassandra cluster node	The setting to enable or disable SSL encryption on this node for internode communication between Cassandra cluster nodes. **Note:** You must perform this configuration step only after the initial installation and configurations complete for the new node, by running the configuration script from the Avaya Multimedia Messaging installation directory.	`CASS_INTERNODE_ENCRYPTION_FLAG`

Table 12: Cluster Utilities

Item name	Description	Equivalent properties file parameter
Utility to configure Openfire for cluster operation	The *Utility to configure Openfire for cluster operation* utility configures a cluster of Openfire servers.	This setting does not have an equivalent parameter in the installation.properties file.

Table continues…

Item name	Description	Equivalent properties file parameter
	You must run this utility on every Avaya Multimedia Messaging server in the cluster.	You must configure the cluster using the configuration tool after the silent installation is complete.
Configure SSH RSA Public/ Private Keys	The *Configure SSH RSA Public/Private Keys* utility configures the SSH RSA keys for SSH login configuration. You must run this utility from the seed node, after installing the other nodes in the cluster.	This setting does not have an equivalent parameter in the installation.properties file. You must configure the cluster using the configuration tool after the silent installation is complete.
Propagate REST and OAMP certificates to cluster	The Propagate REST and OAMP certificates to cluster utility provides REST and OAMP certificates for each node in a cluster. You must run this utility from the seed node, after installing the other nodes in the cluster.	This setting does not have an equivalent parameter in the installation.properties file.

The virtual IP address is necessary in a clustered environment, so that all the nodes in the cluster can be accessed using the same IP address.

Table 13: Virtual IP Configuration Settings

Item name	Description	Equivalent properties file parameter
Enable virtual IP	The setting to enable the usage of a virtual IP address. If you select `n` (no), the configuration script does not configure the virtual IP address. If you select `y` (yes), new configuration settings for the virtual IP address are displayed in the configuration menu: • Virtual IP address: the virtual IP address to be shared by the current node • Virtual IP interface: the network interface to use for the virtual IP. The form of this interface must be `eth0`. • Virtual IP master node: the setting to determine if the current node is the master node in the cluster • Virtual IP router ID: An integer with a value from 1 to 255. The value must be the same for both virtual IP master and backup. The default value is 51.	`KA_ENABLED` If you set this parameter to `y` (yes), you must also configure the following parameters: • `KA_VIRTUAL_IP` • `KA_INTERFACE` • `KA_MASTER_YN` • `KA_AUTHENTICATION_PASSWORD` • `KA_ROUTER_ID`

Item name	Description	Equivalent properties file parameter
	This value must be unique across Virtual Router Redundancy Protocol (VRRP) installations and it is limited to cluster deployments. • Virtual IP authentication password: the password to use for virtual IP authentication.	

Cassandra DB user and password

When you configure the Avaya Multimedia Messaging server, you must change the default Cassandra database credentials to ensure a secured connection to the Cassandra database server.

Table 14: Cassandra database settings

Item name	Description	Equivalent properties file parameter
Current Cassandra Database User Name	The current user name for gaining access to the Cassandra database server. This setting is automatically filled in when you install the Avaya Multimedia Messaging server.	`CURRENT_CASSANDRA_USER`
Current Cassandra Database Password	The current password for gaining access to the Cassandra database server. This setting is automatically filled in when you install the Avaya Multimedia Messaging server.	`CURRENT_CASSANDRA_PASSWORD`
New Cassandra Database User Name	The new user name for gaining access to the Cassandra database server.	`NEW_CASSANDRA_USER`
New Cassandra Database Password	The new password for gaining access to the Cassandra database server.	`NEW_CASSANDRA_PW`

Messaging domains configuration

Table 15: Messaging domains configuration settings

Item name	Description	Equivalent properties file parameter
Messaging Domains	The setting to configure the messaging domains that can send and receive messages using the Avaya Multimedia Messaging server. The domains listed in the **Messaging Domains** configuration setting must be separated by the space character ( ).	`MSG_DOMAINS`

Chapter 6: Avaya Multimedia Messaging certificate configuration

The Avaya Multimedia Messaging server has multiple options for certificate management, which include:

- Importing local or public certificates.
- Importing local certificates that are signed by an intermediate Certificate Authority.
- Viewing the details for a certificate.

The following sections outline the manual command line and configuration utility processes for setting up certificates during the Avaya Multimedia Messaging installation process. After you import a certificate, you must restart Avaya Multimedia Messaging for the changes to take effect.

You can also manage and update certificates using the Avaya Multimedia Messaging web administration portal. For more information about working with the web administration portal, see *Administering Avaya Multimedia Messaging*.

✱ **Note:**

The web administration portal is the preferred method for managing certificates. Use the configuration utility process to configure certificates during a new installation or for troubleshooting purposes, but after this is done, perform certificate management from the web administration portal when possible.

For information about managing the Avaya Multimedia Messaging root certificate and for managing identity certificates, see *Administering Avaya Aura® System Manager*.

For details about adding CA signed certificate used by Lync or Skype for Business edge server and updating the TLS certificate through Session Manager, see *Avaya Aura® Presence Services Snap-in Reference*.

If you do not use Avaya Aura® System Manager certificates, the Avaya Multimedia Messaging server requires four PEM certificates and their corresponding key files:

- The REST interface certificate is used for the communication with the clients.
- The SIP interface certificate is used for SIP communication for integration with Lync or Skype for Business.
- The OAMP interface certificate is used for the OAMP GUI.
- The node certificate is used for internode communication such as cluster notifications. The node certificate is also used for encrypting database traffic.

Avaya Multimedia Messaging supports PKS12-format certificates. The signing authority certificate file is also required.

Important:

- All certificates must contain Subject Alternate Names for the FQDN of the Avaya Multimedia Messaging server and the FQDN of the local Avaya Multimedia Messaging node.
- The Common Name of the Node certificate must contain the FQDN of the local Avaya Multimedia Messaging node. In a cluster, every Avaya Multimedia Messaging node has a different FQDN.

Command for viewing certificate details

You can view certificate details by running `displayCertificate.sh` under the `misc` directory.

```
sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<vesion>/misc/displayCertificates.sh
<cert-type>
```

You can enter one of the following `<cert-type>` values:

- `oam`
- `rest`
- `sip`
- `node`
- `ca`
- `licensing`
- `ldap`
- `psng`

Example

The following is an example output of the command:

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 2945238310718265506 (0x28df96a3993bd8a2)
Signature Algorithm: sha256WithRSAEncryption
Issuer: CN=default, OU=MGMT, O=AVAYA
Validity
Not Before: Apr 13 19:04:48 2016 GMT
Not After : Apr 13 20:04:48 2018 GMT
Subject: CN=ott-253-20.cnda.avaya.com, O=Avaya, C=US
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (1024 bit)
Modulus:
00:86:a6:bc:0a:88:0e:5a:b7:c4:c7:e7:07:b5:80:
3b:b7:c9:99:a4:d8:79:94:0c:58:01:ca:bd:a3:07:
```

```
41:c6:0e:1a:8b:dc:81:ae:d4:44:9e:78:19:a9:b6:
fa:90:bd:36:53:60:b0:ab:60:0e:c6:8e:0f:92:49:
21:8c:a0:63:82:2c:79:00:65:2a:63:9a:51:f2:9a:
09:8c:95:58:69:82:eb:bf:4e:4a:55:8c:54:7d:cf:
60:c7:aa:69:ec:6c:a1:83:7d:d6:35:38:18:1e:e3:
35:cb:48:04:24:a3:a8:4c:5b:97:7b:18:5a:b4:0e:
95:af:25:9b:4d:f6:79:3f:0f
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Alternative Name:
DNS:ott-253-20.cnda.avaya.com
X509v3 Subject Key Identifier:
69:12:BB:43:87:FE:39:33:A1:E6:5A:5B:E0:0D:DD:36:BD:AF:68:1E
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Authority Key Identifier:
keyid:5C:6F:06:43:55:4D:BF:B0:8C:C8:CE:24:0D:E5:AD:53:E4:98:E7:E4
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Key Usage: critical
Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement
Signature Algorithm: sha256WithRSAEncryption
1e:7d:03:a1:b9:d8:0c:48:e6:de:8f:4f:c5:47:88:25:8b:33:
ba:ac:32:a2:9f:5c:8b:5d:9a:25:99:14:11:c5:5f:17:77:65:
de:1b:f4:7f:9b:b5:69:9f:1d:ec:2e:a2:9d:ad:b7:0c:46:ae:
f5:51:1c:71:0b:6b:53:9f:c0:9f:55:44:c2:d3:b9:7c:6a:60:
03:10:64:c5:96:6b:40:53:16:77:2f:7c:2d:7b:38:ff:7d:fd:
f0:b7:4f:13:f9:13:30:83:29:10:86:f8:60:b5:d9:71:d0:39:
2d:65:52:a6:d1:5c:5d:08:ad:a8:5f:71:d9:b7:ef:ae:3e:81:
f7:3c
SHA1 Fingerprint=CA:FF:95:12:F3:C2:4F:37:CA:CE:32:D2:7F:89:0D:2C:B8:99:9A:9D
```

Importing the Avaya Aura® System Manager trusted certificate

About this task

If you use Avaya Aura® System Manager for certificate management, you must configure the System Manager connection details, enable using System Manager for certificate management, and enter the enrollment password.

The following procedure describes how to configure the Avaya Multimedia Messaging server for certificate management using Avaya Aura® System Manager.

Procedure

1. Run the Avaya Multimedia Messaging configuration utility using the `app configure` command.
2. Select **Front-end host, System Manager and Certificate Configuration**.
3. Set **Use System Manager** to `y` (yes).
4. Configure the System Manager connection details:
    - **System Manager FQDN**

- **System Manager HTTPS Port** or the **Front-end port for reverse proxy**, if applicable

  To configure the reverse proxy port number, you must first set the **Override port for reverse proxy** setting to `y` (yes).

5. Configure the **System Manager Enrollment Password** and **Keystore password** options.

   These options are used for adding the certificates to the trust store of the client applications.

6. After you finish configuring the Avaya Multimedia Messaging server, check the configuration utility log files to ensure that the System Manager configuration was made successfully.

7. Restart Avaya Multimedia Messaging after adding certificates for the changes to take effect.

Generating Certificate Signing Requests

About this task

Use this procedure to generate a Certificate Signing Request (CSR).

Important:

You must use this procedure if you are not using System Manager as the only Certificate Authority (CA) to sign certificates for all solution components.

Before you begin

Ensure that Avaya Multimedia Messaging is successfully installed with System Manager signed certificates. This is the default setting for installation.

Procedure

1. Run the following command:

   ```
   sudo mkdir /opt/Avaya/AMMportalCerts
   sudo chmod 770 /opt/Avaya/AMMportalCerts
   ```

   The system creates an `AMMportalCerts` directory in `/opt/Avaya/` for the output of the script that will generate the CSRs.

2. Run the following command to navigate to the directory containing the script:

   ```
   cdto misc
   ```

3. To generate a CSR, run the following command:

   ```
   sudo ./createCSR.sh /opt/Avaya/AMMportalCerts frontEndFQDN localFQDN
   organizationName organizationUnit locality stateOrProvince countryCode
   emailAddress
   ```

Important:

This command is a single Linux command and must be entered as a single line even if it appears as several lines in the document.

The parameters for this script are:

- `frontendFQDN`: For a cluster installation, this is the FQDN of the Virtual IP or external load balancer. For simple, non-clustered installations, this is the FQDN of the server where Avaya Multimedia Messaging is installed.
- `localFQDN`: The FQDN of the server.
- `orgnizationName`: The name of the organization.
- `organizationUnit`: The name of the unit or sub-organization. For example, “Design”.
- `locality`: The name of the city or town.
- `state`: The two-digit state or province code.
- `countryCode`: The two-digit country code.
- `emailAddress`: The administrator email address.

4. Verify that `/opt/Avaya/AMMportalCerts` contains the `.key` and `.csr` files for front-end, node, OAMP, and SIP.

   Note:

   Use `.csr` and `.key` files for front-end and OAMP to generate certificates. You can ignore `.csr` and `.key` files for node and SIP.

Getting certificates signed by the third-party CA

About this task

Avaya Multimedia Messaging accepts certificates in either the PEM or PKCS12 formats.

Note:

- PEM is a Base64 encoded ASCII format. The certificate data is prefixed with the `-----BEGIN CERTIFICATE-----` line and followed by the `-----END CERTIFICATE-----` line. The most common file name extensions are `.pem`, `crt`, and `cer`.
- PKCS12 is a binary format that contains the server certificate, intermediate certificates and the private key in a single encryptable file. The file name extensions for this format are `.pfx` and `.p12`.

Before you begin

- Ensure that the CA is configured to include extendedKeyUsage for both the client and the server in the generated certificates.

- Open the Linux shell using the Linux administrator account credentials.

Procedure

1. Transfer the required `.csr` files from Avaya Multimedia Messaging so that they can be used during signed certificate generation process on your third-party CA.
2. Transfer certificates to Avaya Multimedia Messaging.

   For more information about importing certificates, see Importing third party CA signed certificates on page 123.

   a. Transfer the signed certificate file in the PEM or PKCS12 format to the Avaya Multimedia Messaging server, and rename it according to the CSR file name.

      For example, if you used the `frontEnd.csr` file to generate a certificate, and you received a signed certificate with the `signed_certificate.crt` file name, rename the certificate to `frontEnd.crt`. You must keep the signed certificate file extension unchanged.

   b. Transfer the third-party root CA certificate to the Avaya Multimedia Messaging server, and name it `rootCA.<extension>`.

      For example, use `rootCA.crt` if you received the third-party root CA certificate with the `.crt` extension. You must keep the root CA certificate extension unchanged.

   c. Transfer any third-party intermediary CA certificates to the Avaya Multimedia Messaging server, and name them `intermediary1.<extension>`, `intermediary2.<extension>`, and so on in ascending order of the certificate chain until the root CA.

      For example, use `intermediary1.crt` and so on if you received third-party intermediary CA certificates with the `.crt` extension. You must keep the root CA certificate extension unchanged.

Importing third party CA signed certificates

About this task

If you do not use Avaya Aura® System Manager for certificate management, Avaya Multimedia Messaging provides you with the possibility of using certificates that are specific to your organization and have the certificates signed by a local or public certificate authority.

The following procedure describes how to import the certificate files and the corresponding key files using the configuration utility.

Before you begin

Import third party root and all intermediate CAs into the following trust stores in order:

- The trust stores of each server that interacts with Avaya Multimedia Messaging, including Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Session Border Controller, and the Equinox Management server.

- The Avaya Multimedia Messaging trust store. This is required for intra-cluster communications where the Avaya Multimedia Messaging identity certificate is presented to other servers within the cluster.

Important:

You must perform the importing in order. Otherwise, loss of service can occur because Avaya Multimedia Messaging cannot communicate with some or all of the mentioned servers.

Procedure

1. Run the Avaya Multimedia Messaging configuration utility using the `app configure` command.
2. Select **Front-end host, System Manager and Certificate Configuration**.
3. Configure the System Manager connection details:
   - **System Manager FQDN**
   - **System Manager HTTPS Port** or the **Front-end port for reverse proxy**, if applicable

     To configure the reverse proxy port number, you must first set the **Override port for reverse proxy** setting to `y` (yes).
4. Configure the **System Manager Enrollment Password** option.

   The System Manager enrollment password is used for adding the certificates to the trust store of the client applications.
5. Set **Use System Manager** to `n` (no).

   The menu displays options for importing individual certificate files and the corresponding key files.
6. Configure the following options to provide the paths to the certificate and key files:
   - REST interface key file
   - REST interface certificate file
   - SIP interface key file
   - SIP interface certificate file
   - OAM interface key file
   - OAM interface certificate file
   - node key file
   - node certificate file
   - signing authority certificate file

   a. When prompted, specify whether the certificate file is in PKCS12 format.

   b. If the certificate file is in the PEM format, specify paths to the key file and to the PEM file.

   Both the certificate and the corresponding key file must be present on the server when they are imported. If one pair of files is not imported because one or both files are missing, the other files may still be imported, so that you can selectively replace individual certificates. You can also generate certificates using Avaya Aura® System Manager and replace individual certificates, such as the front-end certificates.

7. Configure the path to the Lync or Skype for Business certificate file under **Advanced Configuration** > **Import Microsoft Lync trusted certificate**.
8. Configure the **Keystore password** option.

   This password is used for adding the certificates to the trust store of the client applications. The role of the keystore password is similar to the role of the Avaya Aura® System Manager enrollment password in the configurations that use the Avaya Aura® System Manager root certificate.
9. Restart Avaya Multimedia Messaging and check the configuration utility log files to ensure that the certificates were imported successfully.

Adding third-party root and intermediate CA certificates to Avaya Multimedia Messaging

About this task

Use this procedure to trust additional root and intermediate CAs. For example, you can add the:

- LDAP root CA certificate if you are using a secure LDAP connection.
- Lync CA certificate if Session Manager has certificates signed by the Lync CA.

You can manage truststore certificates by using the Avaya Multimedia Messaging administration portal as described in *Administering Avaya Multimedia Messaging*.

Do not use this procedure to add the System Manager root CA certificate, which was already added during the installation process.

Note:

Avaya Multimedia Messaging does *not* support PEM certificate chains.

Procedure

1. Run the Avaya Multimedia Messaging configuration utility using the `app configure` command.
2. Select **Add a Certificate to the TrustStore**.
3. To add a certificate, select **Certificate file** and specify the path to the file.
4. Select **Apply**.

Creating a Certificate Signing Request (CSR) using OpenSSL

About this task

Use this procedure to generate a CSR using OpenSSL.

You can also generate a CSR using the Avaya Multimedia Messaging web administration portal or Generating Certificate Signing Requests on page 121.

Before you begin

Ensure that you have the OpenSSL utility.

Procedure

1. Create an OpenSSL configuration file.

   For example:

   ```
   [ req ]
   req_extensions = v3_req
   distinguished_name = req_distinguished_name

   [req_distinguished_name]

   [ v3_req ]
   basicConstraints = CA:FALSE
   keyUsage = nonRepudiation, digitalSignature, keyEncipherment
   subjectAltName = @alt_names

   [alt_names]
   DNS.1 = dnsserver10927.company.com
   DNS.2 = dnsserver10938.company.com
   DNS.3 = dnsserver10955.company.com
   ```

   The `alt_names` section defines the Subject Alternative Names list and must contain FQDNs of all nodes in the cluster.

2. Run the following command:

   ```
   openssl req -out <CSR_request_file>.csr -newkey rsa:2048 -nodes -keyout
   <CSR_key_file>.key -config <configuration_file>
   ```

   In this command:

   - `<CSR_request_file>.csr` specifies a CSR file name.
   - `<CSR_key_file>.key` specifies a file containing a private key that is used to add the signed certificate to the system.
   - `<configuration_file>` specifies the OpenSSL configuration file that was created in the previous step.

   For example:

   ```
   openssl req -out createCSR.csr -newkey rsa:2048 -nodes -keyout keyCSR.key -config
   configCSR.config
   ```

Signing identity certificates for Avaya Multimedia Messaging using third-party CA certificates

About this task

You can use the following procedure to sign identity certificates for Avaya Multimedia Messaging using third-party CA certificates.

Note:

In the following procedure, the third-party CA certificate can be a public CA or an internal private CA.

Before you begin

- Create a CSR with the following X509 extensions:
  - keyUsage = nonRepudiation, digitalSignature, keyEncipherment
  - extendedKeyUsage = serverAuth, clientAuth
- Ensure that the CSR contains the following:
  - If the certificate is only used on the Avaya SBCE, the request contains the subjectAltName extension that lists the cluster FQDN in the SAN.
  - If the certificate is used on both Avaya SBCE and the Avaya Multimedia Messaging server, the request contains the subjectAltName extension that lists the cluster FQDN as well as the FQDN of each cluster member in the SAN.

    Note:

    From the security perspective, Avaya recommends that you generate separate certificates for each node, including the cluster FQDN and the individual cluster node FQDN in subjectAltName.
- Do not provide the password for a key because password protected keys are not supported.
- Ensure that the key generated along with the CSR is stored safely.
- Ensure that once the certificate is generated, you have received the identity certificate, root CA certificate, and all intermediate CA certificates in the `.PEM` format from the certification authority. If these certificates are not in the `.PEM` format, you can convert these certificates using the OpenSSL tool.
- Generate the identity certificate chain.

Procedure

1. Log on to Avaya Multimedia Messaging using your SSH credentials.
2. Import the intermediate CA certificate and the root CA certificate to the Avaya SBCE trust store if you are using reverse proxy on the Avaya SBCE to Avaya Multimedia Messaging.
3. Run the Avaya Multimedia Messaging configuration utility using the `app configure` command.

4. Do the following to import intermediate CA certificates to Avaya Multimedia Messaging:
    a. Select **Add a Certificate to the TrustStore**.
    b. Click **Select**.
    c. Enter the path to the certificate file and then click **OK**.
    d. Click **Apply** to import the certificate.
    e. Repeat these steps for all intermediate CA certificates.
5. Click **Front-end host, System Manager and Certificate Configuration**.
6. Click **Use System Manager for Certificates** and type `n` to not use System Manager for certificates.
7. Click **REST Interface certificate configuration**. If the certificate is not in the PKCS12 format, type `n` on the REST Interface certificate configuration screen.
8. Add the key file to the REST interface PEM key file and the certificate chain to the REST interface PEM certificate file.
9. Click **Signing authority certificate configuration** on the Front-end host, System Manager and Certificate Configuration screen.
10. If the CA root certificate is not in the PKCS12 format, type `n`.
11. Click **Signing Authority PEM certificate file** and add the signing authority CA certificate.
12. Click **Return to previous menu**.
13. Click **Apply**.

Configuring System Manager to trust third-party root CA certificates

Procedure

1. Log on to the System Manager web console.
2. Click **Home** > **Services** > **Inventory** > **Manage Elements** .
3. Select System Manager from the **Elements**.
4. Click **Configure Trusted Certificates** in the **More Actions** list.
5. Click **Add** and select **Import from file**.
6. Click **Choose File** and browse to the third-party root CA certificate.
7. Click **Commit**.

8. Restart the System Manager JBOSS™ process.

   From the SSH session on the System Manager, run the following command as a root user:

   ```
   service jboss restart
   ```

   Note:

   The **`service jboss restart`** command affects the service for the System Manager.

LDAP certificates

By default, Avaya Multimedia Messaging uses an unsecured LDAP connection. For secure connectivity, you must import an LDAP certificate file to the Tomcat trust store.

You can import the certificate using the configuration utility or the web administration portal. This section describes the configuration utility procedure. For information about importing the certificate from the web administration portal, see *Administering Avaya Multimedia Messaging*.

Importing the secure LDAP certificate using the configuration utility

Before you begin

- Ensure that the certificate file is in the `.PEM` format. If it uses a different format, such as `.DER`, you must first convert the file to the `.PEM` format using the **`openssl`** command in the Avaya Multimedia Messaging CLI.

  For example:

  ```
  openssl  x509 -inform DER -outform PEM -in certificate.der -out certificate.pem
  ```

- Ensure that the FQDN that is configured as the address of the LDAP source is defined in the LDAP certificate in one of the following places:
  - The Common Name in the Subject field.
  - Subject Alternative Name.

  You can use the following command to verify the certificate content:

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

Procedure

1. Run the Avaya Multimedia Messaging configuration utility using the `app configure` command.
2. Select **LDAP Configuration** > **Import Secure LDAP trusted certificate**.

3. In the **Trusted LDAP certificate settings** menu, configure the following settings:
   - **Certificate file**: The path and file name for the LDAP trusted certificate. This file must be in the PEM format.
   - **Truststore password**: The password for the Tomcat trust store. This is the same password as the *MSS/Tomcat keystore password* configured in the **Front-end host, System Manager and Certificate Configuration** menu.

   ✱ **Note:**

   If you perform a silent installation, the equivalent parameters that you must configure in the `installation.properties` file are the following:

   - `LDAP_TRUSTSTORE_CERTFILE`
   - `LDAP_TRUSTSTORE_PASSWORD`

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, 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.

Default Lync or Skype for Business server certificate to put in the trust store for each Avaya Multimedia Messaging node

You must obtain a certificate for Avaya Multimedia Messaging and Session Manager to communicate with the Lync or Skype for Business servers.

Methods for obtaining the certificate

Use one of the following methods to obtain the certificate:

- Get the certificate from the Certificate Authority (CA). This is the recommended method.
- Copy the default certificate from the Lync or Skype for Business server to each node.

Getting the certificate from the Certificate Authority

About this task

You can obtain the certificate for communicating with the Lync or Skype for Business servers using one of two methods. This procedure describes the first method, which is recommended.

Procedure

1. In a browser, enter the URL of the Certificate Authority (CA).

   The URL is usually `https://<server-name>/certsrv/` .
2. When prompted, enter your login credentials.
3. Click **Download a CA certificate, certificate chain, or CRL**.
4. Select **Base 64** as the encoding method.
5. Click **Download CA certificate chain**.
6. Click **Save** to download the certificate file.

Copying the default certificate from the Lync or Skype for Business server to the node

About this task

You can obtain the certificate for communicating with the Lync or Skype for Business servers using one of two methods.This procedure describes the second method, which involves copying the certificate from the Lync or Skype for Business server into the trust store for each Avaya Multimedia Messaging node. If you use this method, then you must get the certificate for Avaya Multimedia Messaging from the Lync or Skype for Business front-end server, and the certificate for Session Manager from the Lync or Skype for Business Edge server.

Procedure

1. Use Remote Desktop to connect to the Lync or Skype for Business front-end server.
2. Run the Lync Deployment Wizard.
3. Click **Install or Update Lync Server System**.
4. In the Request, Install or Assign Certificates section, click **Run Again**.
5. Ensure that **Default certificate** is selected and click **View**.
6. In the View Certificate screen, click **View certificate details**.
7. In the Details tab, click **Copy to File**.
8. In the Certificate Export Wizard, click **Next**.
9. Select **No, do not export the private key** and then click **Next**.
10. Select **Base-64 encoded X.509 (.CER)** as the format and then click **Next**.
11. Enter a name for the file.
12. **(Optional)** To check the location for the saved certificate, click **Browse**.
13. Click **Next** and then click **Finish**.

Importing the Lync or Skype for Business front-end server certificate into the trust store

About this task

Use this procedure to import Lync or Skype for Business certificates into the Avaya Multimedia Messaging trusted store.

Tip:

If you experience problems with the import in a cluster environment, see information about uploading the certificate on and Avaya Multimedia Messaging cluster in *Troubleshooting Avaya Multimedia Messaging*.

Before you begin

Obtain the certificate. For more information, see Methods for obtaining the certificate on page 131.

Procedure

1. Start the Avaya Multimedia Messaging configuration utility.
2. Select **Advanced Configuration**.
3. Select **Import Microsoft Lync trusted certificate**.
4. Enter the full path to the file name of the Lync or Skype for Business certificate and select **OK**.

   The file must be in `per` or `der` format.

5. Select **Apply**.

Chapter 7: Messaging domains configuration

The list of reachable domains consists of a union of all domains to which Avaya Multimedia Messaging can route messages. This includes the federated remote domains defined for any messaging adaptors as well as a list of messaging domains that applies only to Avaya Multimedia Messaging messages.

For more information about reachable domains, see DNS configuration on page 22.

Configuring the messaging domains using the configuration utility

About this task

The following procedure describes how to configure the messaging domains using the Avaya Multimedia Messaging configuration utility.

Procedure

1. Run the Avaya Multimedia Messaging configuration utility using the `app configure` command.
2. Select **Messaging Domains Configuration**.
3. Select the **Messaging Domains Configuration** menu option, type the messaging domains separated by the space character ( ) and press Enter.

   For example:

   ```
   ammdomain1.avaya.com ammdomain2.avaya.com
   ```

Configuring the messaging domains using the administration portal

About this task

The following procedure describes how to configure the messaging domains using the Avaya Multimedia Messaging administration portal.

Procedure

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

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

   ❗ **Important:**

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

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

2. Select **Client Administration** > **Client Settings**.
3. In the **Messaging Domains** field, type the messaging domain and click **Add To List**.
4. To delete a messaging domain from the list, select the corresponding check box in the **Messaging Domains List** table and click **Delete Selected**.
5. Click **Save**.

Chapter 8: LDAP settings configuration

Avaya Multimedia Messaging uses the LDAP servers for user authentication, user authorization, and retrieving user details.

The following sections provide tasks and configuration examples for the LDAP settings.

The LDAP settings configuration is performed during the Avaya Multimedia Messaging installation and there are no additional actions required after the installation is complete.

will follow referrals in LDAP in case the returned host is known. It will work if the bind credentials are valid in the referred to server.

LDAP configuration for Microsoft Active Directory

The following sections describe how to configure the LDAP server for Microsoft Active Directory (AD).

The following sections use the example below to provide tasks follow the LDAP configuration example provided in this section, to provide a comprehensive view of how to perform the LDAP configuration.

LDAP secure configuration

By default, Avaya Multimedia Messaging uses an unsecured LDAP connection. For secured connectivity, you must import an LDAP certificate to the Tomcat trust store.

Important:

The FQDN that is configured as the address of the LDAP source must be defined in the LDAP certificate in one of the following places:

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

For more information about enabling a secure connection, see https://support.microsoft.com/en-us/help/931351/how-to-add-a-subject-alternative-name-to-a-secure-ldap-certificate and https://support.microsoft.com/en-us/help/931351/how-to-add-a-subject-alternative-name-to-a-secure-ldap-certificate.

For more information about installing LDAP certificates on Avaya Multimedia Messaging, see LDAP certificates on page 129.

LDAP configuration example

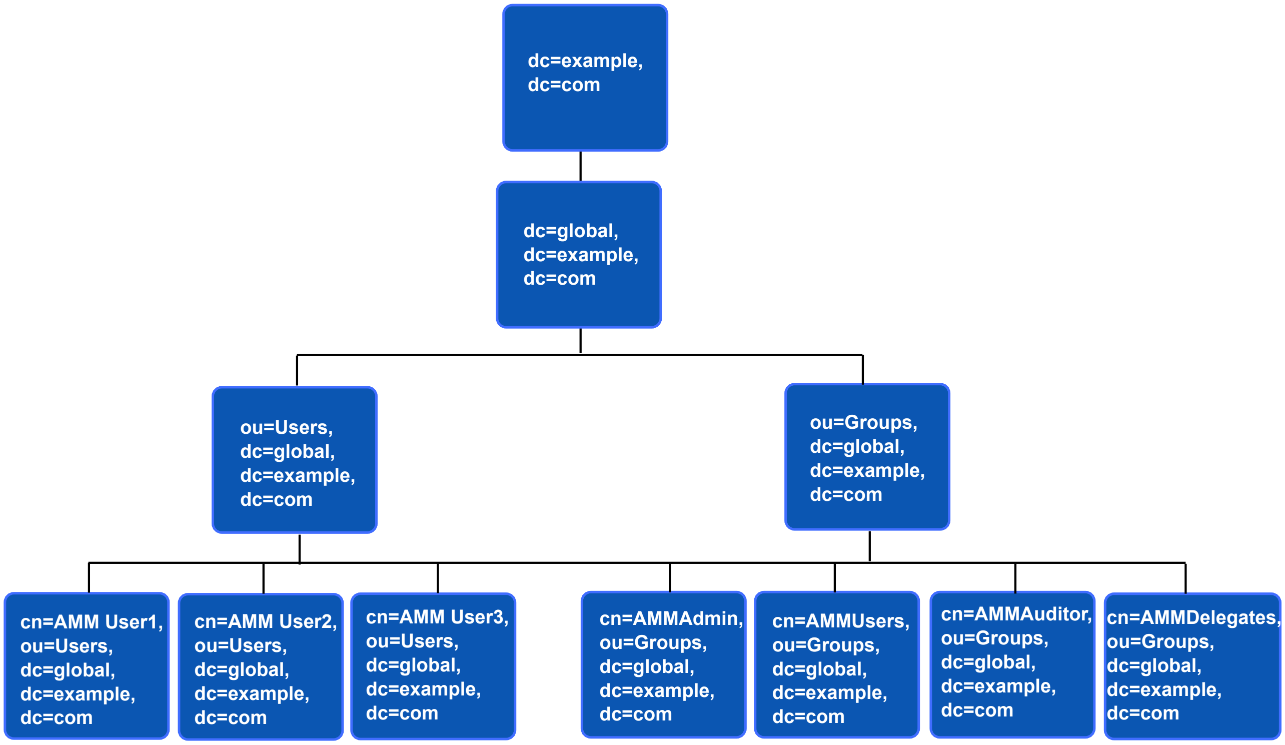

dc=example, dc=com
dc=global, dc=example, dc=com
ou=Users, dc=global, dc=example, dc=com
ou=Groups, dc=global, dc=example, dc=com
cn=AMM User1, ou=Users, dc=global, dc=example, dc=com
cn=AMM User2, ou=Users, dc=global, dc=example, dc=com
cn=AMM User3, ou=Users, dc=global, dc=example, dc=com
cn=AMMAdmin, ou=Groups, dc=global, dc=example, dc=com
cn=AMMUsers, ou=Groups, dc=global, dc=example, dc=com
cn=AMMAuditor, ou=Groups, dc=global, dc=example, dc=com
cn=AMMDelegates, ou=Groups, dc=global, dc=example, dc=com

Figure 2: LDAP configuration example

- Company DNS domain: example.com
- Domain: GLOBAL
- Active Directory FQDN: gdc.global.example.com. This FQDN could be mapped to more than one replicated AD servers with different IPs.
- The Active Directory provides both LDAP and LDAPS (LDAP over TLS) accesses to the Active Directory Global Catalog (see http://technet.microsoft.com/en-us/library/cc728188(v=ws.10).aspx for details on what is Global Catalog) through ports 3268 and 3269, respectively.
- The user that has privileges to read and search the Active Directory (User: AMMAssistant, Password: admin123).
- Domain users.

  Note:

  If the mapping EmailAddress is set to “mail”, the LDAP attribute “mail” must be set as its value is used as the unique identifier for an AMM User.

  - AMM User 1 which has the following attributes:
    - sAMAccountName=ammuser1
    - userPrincipalName=ammuser1@global.example.com
    - mail=ammuser1@example.com

        - givenName=User1
        - sn=AMM
    - AMM User 2 which has the following attributes:
        - sAMAccountName=ammuser2
        - userPrincipalName=ammuser2@global.example.com
        - mail=ammuser2@example.com
        - givenName=User2
        - sn=AMM
    - AMM Admin which has the following attributes:
        - sAMAccountName=ammadmin
        - userPrincipalName=ammadmin@global.example.com
        - mail=ammadmin@example.com
        - givenName=Admin
        - sn=AMM
- Groups:
    - “AMMAdmin” contains the users that can access the AMM OAMP GUI. In this example, this group contains the DN (Distinguished Name) of the user “AMM Admin” as the value of its “member” attributes.
    - “AMMUsers” contains the users that can access the AMM REST interface. In this example, this group contains the DN of the user “AMM User1” and the group “AMMDelegates” as the value of its “member” attributes.
    - “AMMAuditor” contains the users that have read-only access to the OAMP GUI. In this example, this group contains the DN of the users “AMM User1” and “AMM User2” as the values of its “member” attribute.
    - “AMMDelegates” is a subgroup of “AMMUsers”. So the users in this group should also have access to AMM REST interface. In this example, this group contains the DN of the user “AMM User 2” as the value of its “member” attributes.

Configuring the binding parameters

About this task

This procedure describes how to configure the LDAP binding parameters when Microsoft Active Directory (AD) is used.

Procedure

1. Run the Avaya Multimedia Messaging configuration utility using the `app configure` command.
2. Select **LDAP Configuration**.

3. Configure the following settings:

Parameter	Description	Example
URL for LDAP Server	The URL used to locate the Active Directory server. Avaya Multimedia Messaging uses the AD Global Catalog instead of the Avaya Multimedia Messaging LDAP interface. The Global Catalog contains the replicated copies of data in all of the enterprise domains. This avoids the need for delegated searches by following references in the LDAP to other AD domain controllers. ✱ **Note:** Microsoft Active Directory uses a Secure LDAP connection. For the LDAPS connection, a CA (Certificate Authority) certificate for the CA that signed the AD server certificate needs to be imported into the Avaya Multimedia Messaging trust store before the LDAP configuration can be made.	ldaps://gdc.global.example.com:3269
Bind User	The user that has read and search access to Active Directory.	global \AMMAssistant
Bind Credential	The password for the Bind User.	admin123

Configuring the authentication parameters

About this task

This procedure describes how to configure the LDAP authentication parameters when Microsoft Active Directory (AD) is used.

Procedure

1. Run the Avaya Multimedia Messaging configuration utility using the `app configure` command.
2. Select **LDAP Configuration** and configure the following settings:

Parameter	Description	Example
UID Attribute ID	The LDAP attribute that contains the user ID used for authentication. For AD, there are usually two types of userID: Domain user ID or User Principal Names. Avaya Multimedia	sAMAccoutName userPrincipalName

Table continues…

Parameter	Description	Example
	Messaging also supports authentication using the email address of a user. • For Domain user ID authentication, the “UID Attribute ID” must be set to “sAMAccoutName”. See MultipleActiveDirectorydomains for how to set this up in an AD forest • For authentication using User Principal Name, “UID Attribute ID” must be set to “userPrincipalName”. ✱ **Note:** For Microsoft Active Directory, “userPrincipalName” is an optional attribute. So if authentication using User Principal Name (or UPN) is used, ensure that each user has the “userPrincipalName” attribute set.	
Base Context DN	The base DN where the search for the user must start. Usually, the base DN is the root DN for the AD domain.	dc=global,dc=examp le,dc=com

3. Select **LDAP Configuration** > **Advanced LDAP parameters** and configure the following settings:

Parameter	Description	Example
Allow Empty Passwords	The setting to enable user authentication without a password. Microsoft Active Directory does not allow users to authenticate without a password, so you must set the *Allow Empty Passwords* setting to false.	false

Configuring the role search parameters

About this task

This procedure describes how to configure the LDAP role search parameters when Microsoft Active Directory (AD) is used.

Role search for Avaya Multimedia Messaging users are really about finding the associated “role” strings for a user in LDAP. For AD, this is about the user group names that a user belongs to.

In Microsoft Active Directory, the DNs of the groups that a user belongs to are stored in the “memberOf” attribute of a user. The “memberOf” attribute also stores the Exchange mailing lists that a user belongs to. Conversely, the group objects that the user belongs to contain a “member” attribute that stores the DNs of all of the users and sub-groups that are members of this group.

Procedure

1. Run the Avaya Multimedia Messaging configuration utility using the `app configure` command.

2. Select **LDAP Configuration** > **Advanced LDAP parameters**.
3. Configure the parameter settings as described in Parameter settings on page 143.
4. Configure the attributes as described in Role configuration on page 145.

Configuring the internationalization parameters

About this task

The internationalization parameters specify how a user’s given name and surname are stored in Microsoft Active Directory (AD), as well as the language used to store these names. Optionally, for non-Latin script languages, two of the parameters also specify how the ASCII transliteration of these names is stored.

The following procedure describes how to configure the LDAP internationalization parameters when AD is used.

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. Configure the language setting:

Parameter	Description	Default value
Language used in Directory	The language code of one of the languages supported by Avaya Multimedia Messaging.	en

3. Click **Save**.
4. Click **Modify Attribute Mappings**.
5. Configure the following settings:

Parameter	Description	Default value
NativeFirstName	The attribute that stores the “given name” of the user in the language of the LDAP server.	givenName
NativeSurName	The attribute that stores the “surname” of the user in the language of the LDAP server.	sn
GivenName	This is only applicable if the language in AD is one of the non-Latin script based ones.	
SurName	This is only applicable if the language in AD is one of the non-Latin script based ones.	

   The NativeFirstName and NativeSurName parameters allow the user to identify the LDAP attributes used to store the user's native language given name and surname. These are mandatory parameters with defaults of givenName and sn.

The GivenName and SurName parameters allows the user to identify the LDAP attributes used to store the ASCII transliteration of the user's given name and surname, respectively. These are optional parameters and only used only if the Language used in Directory parameter is set to one of the non-Latin script languages.

The internationalization of the names must be done using the language tags specified in RFC 3866.

To configure internationalization for Microsoft Active Directory, you must configure custom attributes for the native and the ASCII transliterations of the names, if both types of names are needed.

6. Click **Save** to apply changes and restart Avaya Multimedia Messaging.

Configuring the user management parameters

About this task

Microsoft Active Directory (AD) users can be disabled by Administrators. The active state is tracked using one bit in the value of the attribute “userAccountControl”. The “whenChanged” attribute in AD is updated with the timestamp of the last time the object is updated.

This procedure describes how to configure the user management parameters for Microsoft Active Directory.

Procedure

1. Run the Avaya Multimedia Messaging configuration utility using the `app configure` command.
2. Select **LDAP Configuration** > **Advanced LDAP parameters**.
3. Configure the following settings:

Parameter	Description	Example
Active users search filter string	The active users search filter string contains the following elements: • objectClass: because the object needs to be of the “user” object class as this is the object class that AD uses to store AD user data. • objectCategory: because AD also uses the “user” object class for objects other than AD users. Notably, the “Computer” object is also of “user” object class. Adding this condition ensures that the object found is an AD user object. • userAccountControl: The string “1.2.840.113556.1.4.803” specifies a bitwise AND filter to check the second lowest bit in the value of “userAccountControl”, which is “1” if the	(&(objectClass=user)(objectCategory=Person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))

Table continues…

Parameter	Description	Example
	user is disabled. Negating this filter using the "!" operator results in filtering for users that are NOT disabled. For details on bitwise filters and an example of using it to locate disabled users in AD, see: http://support.microsoft.com/kb/269181	
Last updated time attribute	The value for AD is "whenChanged".	whenChanged

Multiple authentication and authorization domains

Before Release 3.4, you could configure multiple LDAPs and have multiple base contexts on each LDAP, but you could only use one of them for authorization and authentication. With the single authentication and authorization domain restriction in place, users had to be provisioned multiple times so they existed in the authentication and authorization domain and in the other LDAPs used for search.

As of Release 3.4, the multiple authentication and authorization feature removes the requirement for a single domain for authentication and authorization and facilitates the following deployments:

- A single LDAP infrastructure belonging to a single organization with multiple configured domains.
- Two distinct LDAP infrastructures belonging to two separate organizations.

Avaya Multimedia Messaging supports up to ten LDAP authentication and authorization domains.

When multiple directories are enabled for authentication, you must provide your FQDN to log in. For example: `username@avaya.com`. A short user name is not supported. If you do not have proper data in user name attributes, such as mail and userPrincipalName, you can assign a custom attribute that is used for the UID mapping of user names. All values in the custom attribute must be a fully qualified user name of the form `username@domain`, where `domain` must match one of the base context DNs defined for the LDAP.

During the initial Avaya Multimedia Messaging installation procedure, you can configure only one LDAP server. If you want to add more LDAP servers, use the web administration portal. For more information, see "Adding a new enterprise LDAP server" in *Administering Avaya Multimedia Messaging*.

LDAP parameter descriptions

Parameter settings

The following table describes the parameter settings according to the search mechanism that you choose:

Parameter	**Search mechanism #1:** **Find the user, extract the group DNs from the "memberOf" attribute, and get the role strings from each of the group objects**		**Search mechanism #2:** **Find the groups that the user belongs to and extract the role string from one of the attributes**	
	Example	**Description**	**Example**	**Description**
Role Filter	(&(objectClass=user)(objectCategory=Person)(<UID attribute ID>={0}))	<UID Attribute ID> is the value of the "UID Attribute ID" parameter. "{0}" is the placeholder that will be replaced by the authenticating user ID.	(&(objectClass=group)(member={1}))	"{1}" is the placeholder to be replaced by the DN of the user object. The DN is identified during the authentication process. This filter looks for a group object whose "member" attribute contains a value of the authenticating user DN.
Role Context DN	ou=Users,dc=global,dc=example,dc=com	The purpose of the search is to find the user and then extract the role objects from the "memberOf" user attribute.	ou=Groups,dc=global,dc=example,dc=com	The purpose of the search is to find the roles whose "member" attribute contains the user.
Role Attribute ID	"memberOf"	This attribute contains the list of DNs of the groups to which the user belongs to.	CN	This contains the group's name (e.g. "AMMAdmin", etc.)
Role Attribute is DN	true	The "memberOf" values are the DNs of the group/mailing list objects.	false	The "Role Attribute ID" already contains the "role" string name.
Role Name Attribute	CN	The attribute defined by Role Name Attribute contains the group name. For example: AMMAdmin		Leave this empty because "Role Attribute is DN" is false.
Role Recursion	0	This configuration does not allow recursive search.	1 or higher	You must set this value to 0 if there are no subgroups or a value from 1 to 10

Table continues…

Parameter	Search mechanism #1: Find the user, extract the group DNs from the “memberOf” attribute, and get the role strings from each of the group objects		Search mechanism #2: Find the groups that the user belongs to and extract the role string from one of the attributes	
	Example	**Description**	**Example**	**Description**
		Note: Using this configuration, the users under the “AMMDelegates” group will not be able to use Avaya Multimedia Messaging so this is not the recommended configuration for this example.		to support searches of users that are in subgroups. In this example, the recursive search is needed to find the user in the “AMMDelegates” group, so this value must be set to at least 1.

Role configuration

To search the role base context and under it, set **Search Scope** to `2` or `SUBTREE_SCOPE` . The configuration of the following roles is the same, regardless of the configured search mechanism:

Role	Description	Example
Administrator Role	This role specifies the list of the “role” string extracted from LDAP that would be mapped to the Avaya Multimedia Messaging server ADMIN application role.	AMMAdmin
User Role	This role specifies the list of the “role” string extracted from LDAP that would be mapped to the Avaya Multimedia Messaging server USERS application role.	AMMUsers
Auditor Role	This role specifies the list of the “role” string extracted from LDAP that would be mapped to the Avaya Multimedia Messaging server AUDITOR application role.	AMMAuditor
Service Administrator Role	Avaya Multimedia Messaging does not currently use this role. Leave this setting blank.	
Services Maintenance and Support Role	Avaya Multimedia Messaging does not currently use this role. Leave this setting blank.	
Security Administrator Role	This role is for updating web certificates from the web administration portal.	AMMSecurityAdmin

LDAP attribute mapping

Attribute mapping consists of associating the Avaya Multimedia Messaging Application fields with attributes from the LDAP server configuration, depending on the organization requirement.

You can configure attribute mapping using the **Attribute Mapping** menu on the Avaya Multimedia Messaging administration portal.

Configuration and data mapping use cases

Avaya Multimedia Messaging uses Avaya Aura® Device Services to validate addresses. Avaya Aura® Device Services brings the address information or handle data from Enterprise Directory and System Manager.

Enterprise Directory query

The query used is based on a URI from the Avaya Multimedia Messaging side, which should not contain a schema. Avaya Aura® Device Services uses the LDAP attribute mapping from the configuration to build the filter to query the LDAP. The filter can use the attributes mapped to EmailAddress, EmailAddress-1, IMHandle, IMHandle-1, or LyncAddress, and it is intended for the SMTP, SIP, and XMPP schema.

The following are sample default mappings:

Application Field Name	Directory Field Name
Email address	mail
EmailAddress-1	<not mapped>
IMHandle	<not mapped>
IMHandle-1	<not mapped>
LyncAddress	msrtcsip-primaryuseraddress
SMGRLoginname	userPrincipalName

If the Avaya Multimedia Messaging sends a validation request to Avaya Aura® Device Services for address j.doe@company.com, the Avaya Aura® Device Services will set the filter as follows:

```
OR: 8 items
Filter: (mail=j.doe@company.com)
Filter: (mail=sip:j.doe@company.com)
Filter: (mail=xmpp:j.doe@company.com)
Filter: (mail=smtp:j.doe@company.com)
Filter: (msrtcsip-primaryuseraddress=j.doe@company.com)
Filter: (msrtcsip-primaryuseraddress=sip:j.doe@company.com)
Filter: (msrtcsip-primaryuseraddress=xmpp:j.doe@company.com)
Filter: (msrtcsip-primaryuseraddress=smtp:j.doe@company.com)
```

Leave the IMHandle and IMHandle-1 attributes unmapped. Avaya Multimedia Messaging uses the EmailAddress value as the internal contact. When the EmailAddress and IMHandle mapping return different attribute values, the validation might fail.

System Manager query

Avaya Multimedia Messaging sends a query to Avaya Aura® Device Services, which first queries LDAP, brings back the information, and extracts the values returned for EmailAddress and SMGRLoginname. Avaya Aura® Device Services then queries System Manager using SMGRLoginName, and if that fails, then it uses EmailAddress.

Application Field Name	System Manager Field Name
SMGRLoginName	Login Name
Email address	Login Name, OR Microsoft Exchange Communication Address, OR Other Email Communication Address

The user information is available in both Enterprise Directory and System Manager

If Avaya Aura® Device Services is able to retrieve data from both Enterprise Directory and System Manager, it merges these two data sets, and sends this information back to the Avaya Multimedia Messaging server.

If Avaya Aura® Device Services queries the System Manager data, and if it does not find any related information from System Manager, it sends back the data only from Enterprise Directory.

The user information is available on System Manager but not on Enterprise Directory

The Avaya Multimedia Messaging server sends a query to Avaya Aura® Device Services. If the relevant user is not available on Enterprise Directory, the query is redirected to System Manager. Avaya Aura® Device Services attempts to use the received URI from Avaya Multimedia Messaging to match the System Manager, Login Name, Microsoft Exchange Communication Address, or Other Email Communication Address.

If a match is found, then Avaya Aura® Device Services extracts the SMGRLoginName, creates a query filter with the SMGRLoginName, and then sends another query to the Enterprise Directory.

The fetched data is merged with System Manager data and sent back to Avaya Multimedia Messaging. If the second query to Enterprise Directory fails to bring back data because no relevant data exists, then only System Manager data is sent back to the Avaya Multimedia Messaging server.

User in Enterprise Directory and System Manger

Table 16: Avaya Multimedia Messaging server mappings

Application Field Name	Directory Field Name
Email address	mail
EmailAddress-1	<not mapped>
IMHandle	<not mapped>
IMHandle-1	<not mapped>
LyncAddress	msrtcsip-primaryuseraddress
SMGRLoginname	userPrincipalName

Table 17: Enterprise Directory mappings

Enterprise Directory Field	Value
mail	j.doe@company.com
userPrincipalName	j.doe@north.company.com

Table 18: System Manager mappings

System Manager Field	Value
Login Name	j.doe@north.company.com
Avaya SIP handle	2001@sip.company.com
Avaya Presence/IM handle	j.doe@pres.north.company.com

Avaya Multimedia Messaging sends a validation request for j.doe@company.com to Avaya Aura® Device Services, which then sends a query to Enterprise Directory with the filter shown in Enterprise Directory querySystem Manager queryThe user information is available in both Enterprise Directory and System Manager on page 146.

```
OR: 8 items
Filter: (mail=j.doe@company.com)
Filter: (mail=sip:j.doe@company.com)
Filter: (mail=xmpp:j.doe@company.com)
Filter: (mail=smtp:j.doe@company.com)
Filter: (msrtcsip-primaryuseraddress=j.doe@company.com)
Filter: (msrtcsip-primaryuseraddress=sip:j.doe@company.com)
Filter: (msrtcsip-primaryuseraddress=xmpp:j.doe@company.com)
Filter: (msrtcsip-primaryuseraddress=smtp:j.doe@company.com)
```

When Enterprise Directory gets a match for mail=j.doe@company.com, it returns:

```
mail=j.doe@company.com
userPrincipalName=j.doe@north.company.com
```

Avaya Aura® Device Services sends the following query to System Manager:

```
Filter: Login Name=j.doe@north.company.com
```

When System Manager gets a match on Login Name, it returns the Avaya SIP handle and the Avaya Presence or IM Handle.

Avaya Aura® Device Services merges the information and returns handles to Avaya Multimedia Messaging:

```
Contact = j.doe@company.com
SIP Handle= 2001@sip.company.com
XMPP Handle=j.doe@pres.company.com
```

Attribute mapping use case: changing the address attribute

About this task

The following task provides a use case for attribute mapping when the Directory Service Response contains `address` as `postalCode`, instead of `StreetAddress`.

By default, the `address` application field in the directory service response contains the `streetAddress` LDAP attribute value of the user.

To configure the `address` application field to contain the postal address, perform the following actions:

Procedure

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

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

   ❗ **Important:**

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

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

2. Select **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.
3. Click **Modify Attribute Mappings**.
4. Find the `address` application field.
5. In the combo box next to the `address` application field, select `postalCode`.
6. Click **Save**.
7. To apply the changes immediately, click **Force LDAP Sync** on the Enterprise Directory page.

Attribute mapping use case: adding the language to the directory service response

About this task

The following task provides a use case for attribute mapping when the Directory Service Response contains the language of the user.

The attribute used for determining the language of a user depends on each organization.

By default, the `language` field does not have a default attribute mapping. The `preferredLanguage` attribute used in the following example is not a pre-loaded attribute. You must type the `preferredLanguage` name in the custom attribute field.

Important:

Before you type the name of a custom attribute, ensure that the attribute is available in your Directory configuration and that the attribute is available or part of the global catalogue.

The following procedure describes how to map the `preferredLanguage` attribute to the `language` application field by using the custom attribute field.

Procedure

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

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

   Important:

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

   To gain access to the web-based administration portal, you must use an account that has the Administrator role defined in the LDAP server configuration.
2. Select **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.
3. Click **Modify Attribute Mappings**.
4. Find the `language` application field.
5. In the **Custom Attribute Field** column that corresponds to the `language` application field, click the cell and type `preferredLanguage`.
6. Click **Save**.
7. To apply the changes immediately, click **Force LDAP Sync** on the Enterprise Directory page.

Chapter 9: Avaya Multimedia Messaging federation configuration

Avaya Multimedia Messaging supports federation with:

- Avaya Aura® Presence Services
- Microsft Lync or Skype for Business

Only one type of federation is supported for each Avaya Multimedia Messaging server.

You can configure federation with a standalone server or with a cluster of servers.

Federation with Presence Services

The following sections describe the Presence Services and Avaya Multimedia Messaging configuration required to set up federation with Presence Services.

As of Release 3.3, Avaya Multimedia Messaging no longer supports Presence Services Release 6.x. You must use Presence Services Release 7.x. and configure the HTTPS REST adaptor. The XMPP adaptor is no longer supported. For information about migrating to the 7.x REST environment, see *Administering Avaya Multimedia Messaging*.

For more information about how to configure Breeze or Openfire to interoperate with Avaya Multimedia Messaging, see *Avaya Aura® Presence Services Snap-in Reference*.

Configuring Presence Services Release 7.x for Avaya Multimedia Messaging federation

About this task

The following procedure describes how to configure Avaya Multimedia Messaging federation with Presence Services Release 7.x. You must repeat this procedure on every node in the cluster.

Before you begin

Before you configure the Avaya Multimedia Messaging–Presence Services federation, you must ensure that:

- The Avaya Multimedia Messaging server is reachable.

- The DNS server contains:
  - An SRV record of the Avaya Multimedia Messaging domain.
  - An SRV record for each Presence domain.

Procedure

1. From the System Manager web interface, navigate to **Elements** > **Avaya Breeze**.
2. Navigate to the Attributes Configuration page.
3. Click the **Service Clusters** tab and then do the following:
   a. Select the correct cluster.
   b. From the **Service** drop-down menu, select **PresenceServices**.
4. Click ▼ if necessary to expand the Avaya Multimedia Messaging items.
5. Select the **Override Default** check box for each item and set the following values:
   a. Set **AMM Integration enabled** to **True**.
   b. Enter the web service path for the Avaya Multimedia Messaging server. For example, `aem/xmpp/stanza`.
   c. Enter all trusted Avaya Multimedia Messaging host names using a comma-separated list.

LDAP attribute mapping for XMPP adaptors

You can use the IMHandle and IMHandle-1 LDAP attribute mappings to validate in-directory XMPP addresses. After you set the mapping using the LDAP Configuration Modify Attribute Mappings feature, ensure that the XMPP domains are listed in **Remote Domain(s)** for the particular adaptor.

Configuring the HTTPS REST interface in Avaya Multimedia Messaging for federation with Presence Services

About this task

This procedure describes how to provision the HTTPS REST interface for interoperability between the Avaya Multimedia Messaging server and Presence Services.

Avaya Multimedia Messaging can interoperate with Presence Services using either the XEP-0033 or XEP-0045 protocol, or both of them. When communicating with Avaya one-X® Communicator clients hosted on Presence Services, use the XEP-0033 adaptor. Otherwise, use the XEP-0045 adaptor for XMPP clients federated on Presence Services with external XMPP servers, such as Openfire or Cisco Jabber. With the XEP-0045 adaptor, Avaya Multimedia Messaging federates with external XMPP servers using the multi-user chat protocol. With this configuration, Avaya Multimedia Messaging acts as a host for the chat room, inviting both Avaya Multimedia Messaging users and external users into the chat room. Avaya Multimedia Messaging users can also be invited into a chat room hosted on an external XMPP server. External XMPP addresses must be added to the Domains without Directory Access table after the XEP-0045 adaptor is created.

Important:

For federation with external XMPP servers, Avaya Multimedia Messaging does *not* support shared users that have both an Avaya Multimedia Messaging address and an XMPP address in an XEP-0045 domain. Avaya Multimedia Messaging users should *not* have XMPP addresses in either System Manager or LDAP in any external XEP-0045 domains. Otherwise, the system might not work as expected. For example, shared users might be unexpectedly kicked out of a conversation.

The old Groupchat 1.0 protocol that an XMPP client might send to join an Avaya Multimedia Messaging chat room is not supported and is ignored by Avaya Multimedia Messaging.

External XMPP chat room URIs must be included in the list of federated domains under the XMPP Federation table in System Manager Avaya Breeze Attributes Configuration for the appropriate service cluster hosting Presence Services.

DNS SRV records are required for the XEP-0045 adaptor. For more information about records that must be created to interoperate with an external XMPP server, see the multi-user chat information of *Avaya Aura® Presence Services Snap-in Reference*. By default, the multi-user chat URI that is used by Avaya Multimedia Messaging is the front-end FQDN as configured on the Avaya Multimedia Messaging server.

For the configuration needed on the Avaya Aura® Presence Services side, see *Avaya Aura® Presence Services Snap-in Reference*.

Note:

After upgrading to Release 3.4, you must delete any existing XEP-0045 adaptors and then re-add them.

Procedure

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

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

   Important:

   - For the hostname, always use the same Avaya Multimedia Messaging server FQDN that you use for generating certificates. You will be redirected to the Login page if you use the IP address instead of the FQDN.
   - If both the XEP-0033 and XEP-0045 adaptors are enabled, then in the System Manager communication profile you must set **IM Gateway** to Avaya Multimedia Messaging for all users, including users that only use Presence Services IM clients. This allows Avaya Multimedia Messaging to mediate XEP-0033 and XEP-0045 interactions.

   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. In **HTTPS REST to Avaya Presence Services Adaptors**, do one of the following:
    - To add a new adaptor, click **Add**.
    - To edit an existing adaptor, select the adaptor and click **Edit**.
4. Do the following to edit adaptor settings:
    a. Select a protocol.

        ✱ **Note:**

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

    b. Select the **Adaptor Enabled** check box.

    c. In the **Name** field, type a name, such as `HTTP1`.

    d. In the **Address** field, enter the IP address or the FQDN of your Presence Services server.

    e. **(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.

    f. Select the **Send Domain Ping** check box.

    g. In **Add Remote Domain**, add the Avaya Multimedia Messaging users' Presence or IM handle domains in the communication profile in System Manager, and then click **Add**.

        This field is required for both XEP-0033 and XEP-0045 protocols.

        ✱ **Note:**

        The Remote Domains are mutually exclusive across the REST adaptors.

    h. If you are creating an XEP-0045 adaptor, in the **Add Local Domain(s)** field, provide the Avaya Multimedia Messaging users' XMPP domain, which corresponds to their Presence or IM domains in System Manager, and then click **Add**.

    i. Click **Save**.
5. Do the following to add a domain without directory access from the network of a different enterprise and to enable message exchange between users:
    a. In **Domains without Directory Access**, select the adaptor and click **Edit**

    b. In **Add Domain**, type the domain name.

        For XEP-0045, this can also be the XMPP domain name of the external XMPP server, such as OpenFire or Cisco.

    c. Click **Add**.

    d. Click **Save**.

    All users from the domain are considered valid.
6. Ensure the adaptor status is `CONNECTED`.

If all the domains are connected, then the status is `CONNECTED`. If all the domains are disconnected, then the status is `DISCONNECTED`. If any of the domains is disconnected, then the status is `PARTIAL`.

Supported external chat room configurations

Most XMPP servers allow clients to customize their chat rooms. Depending on the configuration type, an Avaya Multimedia Messaging user acting as a participant in the chat room might not have an acceptable user experience. For example, the user might see the incorrect participant list or might not exchange messages with other users. Currently, Avaya Multimedia Messaging does not support but allows you to use the following room configurations:

- Members-only rooms. These type of rooms require participants to be on a list in order to participate in the chat room. Avaya Multimedia Messaging ignores invitations from an XMPP server. Avaya Multimedia Messaging accepts invitations from clients, but adding additional users from the Avaya Multimedia Messaging client will not work correctly.
- Moderated rooms. In this type of room, a participant must request the ability to chat with other users before sending any messages. If an Avaya Multimedia Messaging user is invited into a moderated room, external XMPP clients will not see messages sent by this user.
- Password-protected rooms. To enter a room, users must provide the correct password. If an Avaya Multimedia Messaging user is invited into this type of room, the XMPP client that sent the invitation might not see any response or might see that Avaya Multimedia Messaging declined the invitation.

XMPP can also forbid changing the subject of a room. While this is enforced by XMPP clients, Avaya Multimedia Messaging users can still change the subject. All other Avaya Multimedia Messaging users will see the changed subject, but the XMPP users will see the original subject. This behavior does not affect exchanging of messages.

Avaya Multimedia Messaging does not handle presence state changes. When Avaya Equinox® users update their presence state, XMPP clients might not reflect these changes.

Concept of identity in external chat rooms

XMPP servers can send the full Jabber ID of each participant in a chat room to all other participants. Chat rooms that use this feature are also known as non-anonymous rooms.

Important:

Avaya Multimedia Messaging requires that this feature to be enabled for all external chat rooms.

Consider the following example:

- An Avaya Multimedia Messaging user has an XMPP contact Joe User with the joeuser@somedomain.com address on the Avaya Equinox® client.
- The XMPP user with the full Jabber ID joeuser@somedomain.com logs into a client using the nickname just_joe.

The Avaya Multimedia Messaging user is invited into an external chat room that is configured to send full Jabber IDs of each participant. The Avaya Multimedia Messaging user adds Joe User to the conversation from the contact list. In this case, the Avaya Multimedia Messaging user will see “Joe User” in the participant list, but all other XMPP clients will see that XMPP user’s nickname, just_joe. Using the full Jabber ID allows the Avaya Multimedia Messaging client to match joeuser@somedomain.com with their contact list entry and know that they are the same person.

If the room is not configured to send full Jabber IDs, the Avaya Multimedia Messaging user will see an additional participant just_joe in the participant list. If the room does not send full Jabber IDs, Avaya Multimedia Messaging cannot determine that the two addresses belong to the same person. Users can still exchange messages, but the Avaya Multimedia Messaging user will see that messages are sent by just_joe, and not by Joe User.

XMPP users can change nicknames during the chat.

- If the room is configured to send full Jabber IDs, then Avaya Multimedia Messaging will not see that an XMPP user’s nickname has changed.
- If the room does not send full Jabber IDs, then, if an XMPP user changes their nickname, the Avaya Multimedia Messaging user will see that the XMPP user left the conversation and then rejoined with a new name.

Avaya Multimedia Messaging users cannot change their nicknames during the chat. If an Avaya Multimedia Messaging user is invited to a remote chat, and there is a nickname conflict, then the Avaya Multimedia Messaging user cannot join the room. In this case, XMPP users will see that the Avaya Multimedia Messaging user entered the room and immediately left.

Important:

When a chat is initiated by Avaya Multimedia Messaging and an Avaya Multimedia Messaging user invites external XMPP users into the conversation, Avaya Multimedia Messaging does not allow the XMPP users to change their nicknames. The reason is that Avaya Multimedia Messaging always uses the node@domain address when adding a participant to the conversation to support contact matching.

Expected behavior when an Avaya Multimedia Messaging user cannot enter an external chat room

There are several scenarios where an Avaya Multimedia Messaging user is invited into an external chat room, but cannot enter the room. Examples of why this can occur include the following:

- Chat room nickname conflict.
- Avaya Multimedia Messaging user is on a banned users list.
- Chat room reached its maximum number of participants.

In such cases, the Avaya Multimedia Messaging will never enter the external chat room.

If an Avaya Multimedia Messaging user invites another Avaya Multimedia Messaging user into a chat room, and the invited user cannot enter the room due to any of the reasons above, then the user will see that the invited user joined the conversation and then immediately left.

Expected behavior when all Avaya Multimedia Messaging users leave a conference

Consider the following example:

An Avaya Multimedia Messaging user invites external XMPP users whose domains are on the list of domains without directory access into a conference. At some point later, *all* Avaya Multimedia Messaging users leave the conference, so that only external XMPP users are still in the conference.

In this case, all external XMPP users see that they were kicked out of the conference by Avaya Multimedia Messaging, and they cannot exchange messages.

Expected behavior when adding a banned user to a conference

When a user is banned from a conference, this user can be invited back to the conference, but cannot participate in it. If an Avaya Multimedia Messaging user tries to add a banned XMPP user to the conference, the banned XMPP user might receive a `403 Forbidden` error, but Avaya Multimedia Messaging might not receive any response from the XMPP server. In this case, Avaya Multimedia Messaging users participating in the conference see that the banned XMPP user joined the conference and left it in five minutes, when the Avaya Multimedia Messaging invite timer expired. The user is then removed from the conference. XMPP users participating in the conference do not see the banned user on their participant lists.

A banned Avaya Multimedia Messaging user never joins the conference. If the banned Avaya Multimedia Messaging user accepts the invitation, Avaya Multimedia Messaging users see that the banned user joined the conference and then was immediately removed.

Expected behavior when a user joins or leaves a point-to-point chat

If an XMPP user starts a chat with an Avaya Multimedia Messaging user, it is a point-to-point or one-to-one chat. If another participant joins a point-to-point chat, it becomes a multi-user chat. The XMPP user receives an invitation to an Avaya Multimedia Messaging conference in a new chat window, and if the XMPP user accepts the invitation, the multi-user chat continues in this new window. To provide continuity between point-to-point and multi-user chats, an identifier called threadid is used.

Some XMPP clients, such as Pandion, do not send the threadid by default, but will start sending it when the other party communicates using the threadid. In this case, the Avaya Multimedia Messaging user must reply to the initial message to continue the same conversation. Otherwise, if the client sends another message, it will be opened in a new conversation window.

Some XMPP clients, such as Pidgin, do not support threadid. This does not affect multi-user chats. However, with point-to-point chats, these XMPP clients will open a new conversation window every time the client sends a message to Avaya Multimedia Messaging users.

Some XMPP clients, such as Spark, always use threadid. These clients will not have any issues with point-to-point or multi-user chats.

Expected behavior when a user leaves a point-to-point chat

When an Avaya Multimedia Messaging user leaves a point-to-point chat, an XMPP user can still send messages to the Avaya Multimedia Messaging user and the chat continues.

When an XMPP user leaves a point-to-point chat, the Avaya Multimedia Messaging user might not see that the XMPP user left the conversation depending on the external client. If the Avaya Multimedia Messaging user sends a message, the XMPP client will open a new conversation window.

Expected behavior when an Avaya Multimedia Messaging user sends a file to an external XMPP user

When an Avaya Multimedia Messaging user participates in a conversation with an external XMPP user and sends an attachment to that user, the XMPP user cannot receive the attachment. The XMPP user receives the URL link to the attachment, but the XMPP user cannot be authenticated on the Avaya Multimedia Messaging server and therefore cannot log in and view the attachment.

Federation with Microsoft Lync or Skype for Business

The following sections describe how to configure Avaya Multimedia Messaging to interoperate with Lync or Skype for Business.

The Avaya Multimedia Messaging server can be federated with a Lync Standard Edition or Skype for Business installation using SIP. The Avaya Multimedia Messaging server can be federated directly to the Lync or Skype for Business front end in the case of an intra-enterprise deployment, or via the Avaya Aura® Session Manager to the Lync or Skype for Business edge server in the case of an inter-enterprise deployment.

The federation with Lync or Skype for Business is also referred to as “Microsoft federation” in the Avaya Multimedia Messaging documentation.

For information about Microsoft federation limitations, see “Caveats and limitations” in *Avaya Multimedia Messaging Reference Configuration*.

Microsoft federation checklist

The following checklist outlines the tasks you must perform to configure Avaya Multimedia Messaging federation with Microsoft Lync or Skype for Business.

No.	Task	✔
1	Administer Microsoft Federation. For more information, see *Avaya Aura® Presence Services Snap-in Reference*.	
2	Obtain the default Lync or Skype for Business server certificate to put in the trust store for each Avaya Multimedia Messaging node. Review the sections under Default Lync or Skype for Business server certificate to put in the trust store for each Avaya Multimedia Messaging node on page 131.	
3	Perform the required configuration in System Manager.	
4	Configure Active Directory users using the information in Configuring Avaya Aura System Manager for LDAP synchronization on page 23.	
5	Configure the Avaya Multimedia Messaging server for Microsoft federation.	
6	Enable Presence Services updates for Microsoft federation.	
7	Configure the Lync or Skype for Business server for an internal or external domain as required.	
8	Perform DNS configuration for Lync and Skype for Business and for the Avaya Multimedia Messaging server.	
9	Configure Avaya Multimedia Messaging clusters to interoperate with Lync and Skype for Business.	
10	Configure users.	

System Manager configuration

System Manager configuration checklist

The following checklist outlines the tasks you must perform in System Manager to configure Avaya Multimedia Messaging interoperability with Microsoft Lync or Skype for Business within the same domain:

No.	Task	✔
1	Add the default server certificate to the System Manager trust store.	
2	Complete the Local Host Resolution Table.	
3	Configure SIP entities and set the IM Gateway SIP entity for each user for an Avaya Multimedia Messaging cluster entity.	
4	Use the Application Editor to set application media attributes, so media types used for IM are sequenced through Communication Manager.	
5	Configure application media attributes.	

Table continues…

No.	Task	✔
6	Configure domains.	
7	Configure users.	
8	Configure routing policies and expressions.	
9	Configure the Lync or Skype for Business Edge server. **Note:** This task is only required for external domain federation to an Edge server.	

Adding the Lync or Skype for Business certificate to System Manager

About this task

Use this procedure only if System Manager and Lync or Skype for Business are using different certificate authorities.

Repeat this procedure for each Session Manager that has an Entity link to the Lync or Skype for Business Edge server.

Procedure

1. In the System Manager web interface, navigate to **Services** > **Inventory** > **Manage Elements**.
2. Select the Session Manager to upgrade with the new certificate.
3. From the **More actions** drop-down menu, click **Manage Trusted Certificates**.
4. Click **Add**.
5. Select **SECURITY_MODULE_SIP** from the drop-down menu.
6. Select the appropriate option for your situation and enter the required information.
7. Click **Retrieve Certificates** or **Commit**, depending on which option is used.
8. Verify the certificate information on the screen and then click **Commit**.

   The certificate is now installed.

Adding Avaya Multimedia Messaging nodes to the Local Host Resolution Table

About this task

Use this procedure to enter the IP address of each Avaya Multimedia Messaging node in the cluster into the Local Host Resolution Table for the IM entity.

Note:

You can add nodes for front-end and federation relay SIP entities.

- For more information about front-end entities, see Front-end SIP entity on page 161.

- For more information about relay entities, see Federation Relay SIP entity on page 161.

Procedure

1. In System Manager, navigate to **Elements** > **Session Manager** > **Network Configuration** > **Local Host Name Resolution**.
2. For the front-end entity, do the following for each Avaya Multimedia Messaging node in the cluster:
   a. In **Host Name (FQDN)**, type the Avaya Multimedia Messaging front end FQDN.
   b. Enter the node IP address as the **IP Address**.
   c. Enter `5061` in the **Port** field for all nodes.
   d. To balance the load equally between all nodes in the cluster, enter the same values in **Priority** and **Weight** fields for each node.
   e. Ensure that **Transport** is set to **TLS**.

   The front-end FQDN is the name entered through the configuration utility, in the **Front-end host** > **System Manager and Certificates configuration** menu.
3. Click **Commit** to save your changes.

SIP entities

You can add SIP entities in System Manager by navigating to **Elements** > **Routing** > **SIP Entities**.

Tip:

For a single node system, you can use the Front-End FQDN of Avaya Multimedia Messaging for the entity's FQDN because no load balancing is required.

Front-end SIP entity

The front-end IM entity is used as the IM Gateway in the Presence Services profile of each Avaya Multimedia Messaging user. This entity handles IM requests for the entire cluster. The entity FQDN must be the same as the one configured for the front-end FQDN in the Avaya Multimedia Messaging Configuration form.

Federation Relay SIP entity

The Presence federation Relay SIP entity handles the SIP messages from the Microsoft front-end server as described in *Avaya Aura® Presence Services Snap-in Reference*. To support Microsoft multi-user chat for Avaya Multimedia Messaging, the LyncAdapter adaptation must be applied to this entity.

Summary of SIP entity values

The following tables summarize the required values when you configure SIP entities:

Table 19: General fields

Field name	Value for front-end SIP entity
Name	Enter any value.
FQDN	Same as Avaya Multimedia Messaging front-end FQDN value that resolves to Avaya Multimedia Messaging VIP for cluster, or local node for single node deployment.
Type	Select **Other**.
Adaptation	Leave this blank.

Table 20: Entity links

You must configure Entity links between Avaya Aura® Session Manager and the front-end SIP entity of Avaya Multimedia Messaging.

Entity link field	Value for front-end SIP entity
Name	Enter any value.
SIP Entity 1	Session Manager SIP Entity.
SIP Entity 2	Avaya Multimedia Messaging front-end SIP Entity.
Protocol	Select **TLS**
Port for the Session Manager side	Same as the administered port for the Session Manager SIP adaptor. This port is usually set to 5061.
Port for the Avaya Multimedia Messaging side	Always set to 5061.

Setting the IM Gateway SIP entity for a user in an Avaya Multimedia Messaging

About this task

Repeat this procedure for each Avaya Multimedia Messaging user.

Procedure

1. Log in to the Avaya Aura® System Manager administration portal.
2. Select **User Management** > **Manage Users**.
3. In the Users table, select a user and click **Edit**.
4. Click the **Presence Profile** tab.
5. In the **IM Gateway SIP Entity** field, select the SIP entity for the Avaya Multimedia Messaging.
6. Click **Commit** or **Commit and Continue** to save the changes.

Setting application media attributes

About this task

The application that handles Communication Manager application sequencing must be configured to allow the media types used for IM to sequence through Communication Manager.

Procedure

1. In the System Manager web interface, navigate to **Elements** > **Session Manager** > **Application Configuration** > **Applications** .
2. Ensure that the **Enable Media Filtering** checkbox is selected.
3. Select the following values from the drop-down menus in the Application Media Attributes section:
    a. For **Audio**, select **Yes**.
    b. For **Video**, select **Yes**.
    c. For **Text**, select **NOT_ONLY**.
    d. For **Match Type**, select **NOT_EXACT**.
    e. For **If SDP Missing**, select **ALLOW**.
4. Click **Commit** to save your changes.

Domain configuration

In System Manager, you must add any domain used in a Lync or Skype for Business address. You can add a new domain by navigating to **Elements** > **Routing** > **Domains**.

The Session Manager must be authoritative in a domain to allow users to be configured in that domain. For external domains, you must use a regular expression for your routing. However, if the Lync or Skype for Business Edge server is set up in DNS as the handler for a domain, then no regular expression is needed in that domain.

User profile configuration in System Manager

You must configure a Presence and IM handle for each Avaya Multimedia Messaging user from System Manager. You must set the IM Gateway SIP Entity to the Front End Entity.

The users can be of the following types:

- Lync or Skype for Business only
- Avaya Multimedia Messaging only

Note:

Avaya Multimedia Messaging does not support dual users.

Routing policies and regular expressions

You must set a routing policy to the Avaya Multimedia Messaging SIP entity. You must do this in System Manager by navigating to **Elements** > **Routing** > **Routing policies**. The regular expression pattern corresponding to each routing policy for IM is the front-end FQDN, which is set during the front-end configuration. This FQDN is part of the URI in all the requests from Lync or Skype for Business to the Avaya Multimedia Messaging front-end SIP entity.

Example

The following regular expression example is for an Avaya Multimedia Messaging front-end FQDN of mycompany.com:

```
.*amm\.frontEnd\.fqdn@.+
```

Lync or Skype for Business edge server configuration

You must configure SIP entities, routing policies, and regular expressions for routing to the Lync or Skype for Business edge server. You can perform this configuration in System Manager by navigating to the following locations:

- For SIP entity configuration: **Elements** > **Routing** > **SIP Entities**
- For routing policy configuration: **Elements** > **Routing** > **Routing policies**
- For regular expression configuration: **Elements** > **Routing** > **Regular Expressions**

Summary of configuration values for Lync edge

The following tables summarize the required values to configure the Lync or Skype for Business edge server:

SIP entity values

Table 21: SIP entity general fields

Field name	Value for Lync or Skype for Business edge server SIP entity
Name	Enter any value.
FQDN	Enter same value as Lync or Skype for Business edge.
Type	Select **Other**.
Adaptation	Select **LyncAdaptation**.

Table 22: Entity link fields

Field name	Value for Lync or Skype for Business edge server SIP entity
Name	Enter any value.
SIP Entity 1 is the Session Manager entity and **SIP Entity 2** is the Front-end SIP entity.	Select from the drop-down list. SIP entity 1 is for the Session Manager side, and SIP entity 2 is for the Lync or Skype for Business Edge server.
Protocol	Select **TLS**
Port for the Session Manager side	Same as the administered port for the Session Manager SIP adaptor. This port is usually set to 5061.
Port for the Avaya Multimedia Messaging side	Port for the Lync or Skype for Business Edge server, **Lync Edge SIP TLS port**. This port is usually set to 5061.

Routing policies for Lync edge server

Table 23: General fields

Field name	Value for Lync or Skype for Business edge server
Name	Enter any value.
SIP Entity	SIP Entity of Lync or Skype for Business Edge

You can select a destination from several SIP entities and also modify the time of day for the corresponding routing policies.

Routing regular expression details

Table 24: General fields

Field name	Value for Lync or Skype for Business edge server
Pattern	Enter the routing expression, for example: `example.*@lyncdomain.example.com`
Rank order	Enter any value.
Routing Policy	Select routing policy from above.

Avaya Multimedia Messaging server configuration

Avaya Multimedia Messaging server configuration checklist

Use this checklist to complete the Avaya Multimedia Messaging server configuration for Microsoft federation. This checklist does not describe standard Avaya Multimedia Messaging configuration.

No.	Task	✔
1	Ensure that the host name is set correctly.	
2	Import the Lync or Skype for Business front-end server certificate. For more information, see Importing the Lync or Skype for Business front-end server certificate into the trust store on page 132.	
3	Verify LDAP and System Manager setup in the Avaya Multimedia Messaging administration portal. You can also force updates.	
4	Configure SIP adaptors.	

Avaya Multimedia Messaging server host name setup

The host name for each Avaya Multimedia Messaging server node and the front-end FQDN of a cluster must be resolvable to the Lync or Skype for Business server. The reverse lookup of the IP address of each node and the virtual IP address must also be resolvable to the node FQDN, and respectively to the front-end FQDN.

LDAP and System Manager setup on the Avaya Multimedia Messaging server

Active Directory setup is typically performed before you install the Avaya Multimedia Messaging. For more information, see LDAP server configuration on page 27.

You can view the Active Directory configuration in the Avaya Multimedia Messaging administration portal under **Server Connections**. When user information is changed in System Manager, you can use the **Force LDAP Sync** button on this page. Data synchronization can take a few minutes.

Configuring SIP adaptors

About this task

You must create two SIP adaptors for Microsoft federation: one for Session Manager and the other for Microsoft Lync or Skype for Business.

Procedure

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

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

   Important:

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

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

2. In the left panel, select **Server Connections** > **Federation Configuration**.

Repeat steps 3 on page 166 and 4 on page 166 for each SIP adaptor.

3. Click **Add** to add each SIP adaptor.

4. On the new adaptor page:

   a. Set **Select Type** to **Avaya Session Manager** for the first SIP adaptor, and to **Microsoft Lync** for the second SIP adaptor.

   b. Select the **Adaptor Enabled** check box.

   c. In the **Name** field, type a name.

   d. In the **Address** field, enter the address of the adaptor.

   e. Set the port for **SIP over TLS port**.

      The default value is 5061.

   f. To monitor the adaptor, select **Monitor Adaptor Status** and update the interval value if required.

      The interval value is in seconds.

g. In **Add Remote Domain**, add a Remote domain.

   The Remote domain is the Avaya Multimedia Messaging server domain.

h. In **Add From Domain**, add a From domain.

i. Click **Save**.

5. After both SIP adaptors are added, restart the system.

   A restart is required to use the newly enabled adaptors.

6. Ensure the adaptor status is `CONNECTED`.

   If all the domains are connected, then the status is `CONNECTED`. If all the domains are disconnected, then the status is `DISCONNECTED`. If any of the domains is disconnected, then the status is `PARTIAL`.

Lync or Skype for Business server configuration for an internal domain

The following sections describe the Lync or Skype for Business server internal domain configuration required for Microsoft federation.

Lync or Skype for Business server internal domain configuration checklist

Use this checklist to complete the Lync or Skype for Business server configuration for an internal domain.

No	Task	✔
1	Configure Session Manager routing. In order for Session Manager to route to an address in a particular domain, the domain must be administered in System Manager. For more information, see Domain configuration on page 163.	
2	Check that the Avaya Aura® System Manager and Avaya Aura® Session Manager use the same domain recognized by Lync or Skype for Business. For more information, see Domain configuration on page 163.	
3	Configure Avaya Multimedia Messaging as a Lync or Skype for Business trusted server. For details, see Configuration of Avaya Multimedia Messaging as a Lync or Skype for Business trusted server on page 168.	
4	Get a Lync or Skype for Business certificate with both client and server authentication. For details, see Getting a certificate with client and server authentication on page 173.	
5	Place the System Manager CA certificate into the Lync or Skype for Business Trust Store. For details, see Placing the System Manager CA certificate into the Lync or Skype for Business Trust Store on page 176.	

Configuration of Avaya Multimedia Messaging as a Lync or Skype for Business trusted server

The following configuration allows an Avaya Multimedia Messaging SIP application to register to the server and function as a Lync or Skype for Business user device in multiple instances, without requiring user credentials.

Ensuring that port 5061 is enabled on the Lync or Skype for Business server

Before you begin

If you have users in the domain used by Lync or Skype for Business, then ensure that Avaya Aura® System Manager and Avaya Aura® Session Manager list this domain as a recognized domain.

Procedure

1. Open a terminal window on the Lync or Skype for Business front end and Lync or Skype for Business edge servers.
2. Run the command: `netstat -an | grep 5061 .`

   Note:

   From a Linux server, to check the running certificates, you can use the command: `openssl s_client -showcerts —connect <lync_server_ip>:5061`
3. Look for an entry that shows that the server is listening on port 5061 for TCP.

   For example, the result might be:

   ```
   TCP    1.2.3.4:5061      lync2013-example.example.com:0  LISTENING
   ```

Result

If the commands produce no errors, the port is enabled for TLS.

Adding each server node and front-end FQDN to Lync or Skype for Business as a trusted application

Adding each Avaya Multimedia Messaging server node and front-end FQDN as a trusted application to Lync or Skype for Business Standard Edition

About this task

Use the following procedure to add each Avaya Multimedia Messaging server node and the front-end FQDN to Lync or Skype for Business as a Trusted Application using Microsoft scripts.

Note:

The Microsoft scripts used might display warnings when they create a new application pool or static route entry. These warnings can be ignored.

Procedure

1. Log in to the Lync or Skype for Business front-end server.
2. Go to **Start** > **Lync Server Management Shell**.

3. Obtain the value for the SiteID attribute by entering the following command:

   ```
   Get-CsSite
   ```

   This value is usually 1.

4. Obtain the value for the Registrar Identity attribute by entering the following command:

   ```
   Get-CsService -Registrar
   ```

   The following `New-CsTrustedApplicationPool` invocation uses this value.

5. Create a single server Trusted Application Pool by entering the following command:

   ```
   New-CsTrustedApplicationPool -Identity <pool_fqdn> -Registrar
   <Registrar_Identity> -site <Site_identity> -ComputerFqdn <front_end_fqdn> -
   ThrottleAsServer $true -TreatAsAuthenticated $true -RequiresReplication $false
   ```

   ❗ **Important:**

   Ensure that the values for `ComputerFqdn` and the SIP application server's certificate Common Name (CN) are the same. Otherwise, an error will appear in the Lync or Skype for Business logs.

   If the Trusted Application Pool is created, Lync or Skype for Business might display a warning, which you can ignore. The following is an example of the warning message:

   ```
   WARNING: Machine amm.yourdomain.com from the topology you are
   publishing was not found in Active Directory and will result in
   errors during Enable-CsTopology as it tries to prepare Active
   Directory entries for the topology machines. If you choose to
   publish this topology, you must run Enable-CsTopology again after
   you join the missing machines to the domain.
   ```

6. Create the Trusted Application representing your SIP application and assign it to the Pool you created by entering the following command:

   ```
   New-CsTrustedApplication -ApplicationID <Any_AppId_You_Want. -
   TrustedApplicationPoolFqdn <TrustAppPool_fqdn> -Port 5061
   ```

   ✱ **Note:**

   The ApplicationID can have any value.

7. Enable the newly created topology by entering the following command:

   ```
   Enable-CsTopology
   ```

8. To change the default 0.0.0.0 IP address for the trusted application servers with the appropriate values, perform the following:

   a. Export the topology to an XML formatted file by entering the following command:

      ```
      Get-CsTopology -AsXml | Out-File C:\topology.xml
      ```

   b. Edit the topology XML file by changing the IP address, in the section *Cluster Fqdn="amm_server_node_fqdn"*, from 0.0.0.0 to the IP address of *amm_server_node_fqdn*.

   c. Import the topology from the modified XML file with the following command:

      ```
      Publish-CsTopology –FileName C:\topology.xml
      ```

9. Save the topology in a file.

   ⚠ **Warning:**

   If you do not save the topology and an earlier version of the topology is loaded, the topology will either fail or your work will be deleted.

Adding each Avaya Multimedia Messaging server node and front-end FQDN as a trusted application for Lync or Skype for Business Enterprise Edition

About this task

Use the following procedure to add each Avaya Multimedia Messaging server node and the front-end FQDN to Lync or Skype for Business as a Trusted Application using Microsoft scripts.

You can use Topology Builder.

Note:

The Microsoft scripts used might display warnings when they create a new application pool or static route entry. These warnings can be ignored.

Procedure

1. Run the Lync Topology Builder and select one of the available options.

   The **Download Topology from existing deployment** option is usually selected.

2. Click **OK**.
3. Type a name for the topology and click **Save**.
4. In the Topology Builder window, expand the left tab.
5. Right-click on **Trusted application servers**.
6. Click **New Trusted Application Pool**.
7. Select **Multiple computer pool**.

   Tip:

   You can select **Multiple computer pool** even if your application pool contains only one computer. This option allows later expansion.

8. Enter the Avaya Multimedia Messaging front-end address in **Pool FQDN**.
9. Add the FQDN for each Avaya Multimedia Messaging node, one at a time, and then click **Add**.

   The FQDN appears in the list.

10. After you add all the nodes, click **Next**.
11. Select the **Associate next hop pool** checkbox and then choose the pool from the drop down list.
12. Click **Finish**.
13. Return to the main screen.

14. Click **Action** > **Topology** > **Publish**.
15. Click **Next**.

    A pop-up window displays the status of the action.

    Note:

    If the Avaya Multimedia Messaging nodes are not in Active Directory, you might see a Missing Computer dialog box. If you see this dialog box, click **Yes to All**.
16. When the full status is displayed, click **Finish**.
17. Create the Trusted Application representing your SIP application and assign it to the Pool you created by entering the following command:

    ```
    New-CsTrustedApplication -ApplicationID <Any_AppId_You_Want. -
    TrustedApplicationPoolFqdn <TrustAppPool_fqdn> -Port 5061
    ```

    Note:

    The ApplicationID can have any value.
18. From Topology Builder, save the topology in a file.

    Warning:

    If you do not save the topology and an earlier version of the topology is loaded, the topology will either fail or your work will be deleted.

Adding the Avaya Multimedia Messaging root signing certificate to the Lync or Skype for Business server

About this task

Use this procedure to allow the Lync or Skype for Business server to trust the Avaya Multimedia Messaging SIP application certificate. This certificate is usually the System Manager CA certificate. For more information, see Placing the System Manager CA certificate into the Lync or Skype for Business Trust Store on page 176.

Procedure

1. Log in to the Lync or Skype for Business front-end server.
2. Start the Microsoft Management Console, `mmc.exe`.
3. Click **File** > **Add/Remove Snap-in**.
4. Click **Certificates** and then **Add**.
5. Click **Computer account** and then click **Next**.
6. Keep **Local Computer** selected, click **Finish**, and then **OK**.
7. Expand **Certificates (Local Computer)** and **Trusted Root Certification Authorities**.
8. Right-click **Certificates** and then click **All Tasks** > **Import**.
9. Import the SIP application server root CA certificate, which is usually the System Manager CA..

10. If you configured a Lync or Skype for Business Edge server, repeat the procedure from the start.

Ensuring that each Avaya Multimedia Messaging server node is in DNS

About this task

Repeat this procedure on each Avaya Multimedia Messaging node.

Procedure

1. Log in to the Lync or Skype for Business front-end server.
2. Open a terminal window and enter the following command:

   ```
   nslookup <FQDN_of_amm_server>
   ```

   If the command resolves the SIP application server FQDN, no further action is required on the current node. You must check the next Avaya Multimedia Messaging node.

Perform the following steps if the comment did not resolve the SIP application server FQDN.

3. Connect to the DNS server by navigating to **Start** > **DNS**.
4. In **Forward Looking Zones**, locate an entry that matches the domain of the FQDN.

   If you do not find an appropriate entry, add a new zone.
5. Right-click the entry and do the following:
   a. Select **New host**.
   b. Type the full host name.
   c. Type the IP address for the Avaya Multimedia Messaging server node.
   d. Select the **Create associated pointer (PTR) record** check box.
   e. Click **Add Host**.

Adding the Avaya Multimedia Messaging domain as a SIP federated provider

Procedure

1. Log in to the Lync or Skype for Business Server control panel.
2. Navigate to **Federation and External Access** > **SIP Federated Domains**.
3. Click **New** to add a new entry for the Avaya Multimedia Messaging domain and do the following:
   a. Select **Allowed Domain**.
   b. In **Domain Name**, enter the Avaya Multimedia Messaging domain.
   c. Leave **Access edge server** blank.
   d. Click **Commit**.
   e. To ensure that the users policy has access to **Federated User Access**, go to **Federation and External Access** > **External Access Policy** and verify that the corresponding check box is selected for that policy.

Restarting services on the Lync or Skype for Business front-end servers

About this task

Use this procedure when you first add certificates into Lync or Skype for Business. Subsequent changes, such as adding a new trusted host or changing the static route, do not require a restart.

Procedure

1. Log in to the Lync or Skype for Business front-end server.
2. Do one of the following:
   - On most Windows operating systems, click **Start** > **Programs** > **Administrative Tools** > **Office Communications Server 2007 R2**.
   - On Windows Server 2008, click **Control Panel** > **Administrative Tools** > **Services** .
3. Right-click the FQDN of the Standard Edition server or Enterprise Edition front-end server and click **Stop**.
4. After the services stop, right-click the FQDN of the Standard Edition server or Enterprise Edition front-end server and click **Start**.

Getting a certificate with client and server authentication

About this task

This procedure describes how to obtain a certificate with both client and server authentication using an existing certificate template. If an existing certificate template is not available, then you must create a new one.

Procedure

1. Log in to the Active Directory machine with the certificate authority.
2. Start the Microsoft Management Console, `mmc.exe`.
3. Click **File** > **Add/Remove Snap-in**.
4. Click **Certificate Templates** and then do the following:
   a. Click **Add**.
   b. Click **OK**.
5. Find a template that displays “Client Authentication, Server Authentication” in **Intended Purposes**.

   If an existing template is not available, see Creating a certificate template with client and server authentication on page 174.
6. Return to the main Management Console window.
7. Click **File** > **Add/Remove Snap-in**.
8. Click **Certificate Authority** and then click **Add**.

9. In the Certification Authorities screen, do the following:
    1. Select **Local Computer**.
    2. Click **Finish**.
    3. Click **OK**.
10. Expand **Certification Authority (Local)**.
11. Right-click **Certificate Templates**.
12. If the template you identified in step 5 on page 173 is not available, do the following:

    Note:

    If the template is available in the list, then skip this step.

    1. Click **New** > **Certificate Template to Issue**.
    2. From the list, select the certificate template to enable.
    3. Click **OK**.

Next steps

On the Lync or Skype for Business front-end server, assign the certificate.

Creating a certificate template with client and server authentication

Procedure

1. Log in to the Active Directory machine with the certificate authority.
2. Start the Microsoft Management Console, `mmc.exe`.
3. Click **File** > **Add/Remove Snap-in**.
4. Click **Certificate Authority** and then click **Add**.
5. In the Certification Authorities screen, do the following:
    1. Select **Local Computer**.
    2. Click **Finish**.
    3. Click **OK**.
6. Expand **Certification Authority (Local)**.
7. Right-click **Certificate Templates**.
8. Click **Manage**.
9. To base a new template on an existing template, right-click the existing web server template and then click **Duplicate Template**.
10. Provide the following information in the General tab:
    1. In **Template Display Name**, enter a value such as `Lync Server`.
    2. In **Template Name**, enter a short name, such as `LyncServer`.

11. Click the **Extensions** tab and do the following:

    a. Click **Application Policies** and then click **Edit**.

    b. In the Edit Application Policies Extension screen, click **Add**.

    c. Select **Client Authentication** as the application policy.

    d. Click **OK**.

    The template must support both client and server authentication. You can repeat this process if required.

12. Close the Certificate Templates Console.
13. Right-click **Certificate Templates**.
14. Click **New** > **Certificate Template to Issue**.
15. Select the new template created in steps 9 on page 174 to 11 on page 175.
16. Click **OK**.

Next steps

On the Lync or Skype for Business front-end server, assign the certificate.

Assigning the certificate to the Lync or Skype for Business front-end server

Procedure

1. Log in to the Lync or Skype for Business front-end server and do the following:

    a. Run the following command:

    ```
    Request-CsCertificate -New -Type Default -Output filename -ClientEku $true -
    Template template-chosen-above
    ```

    b. Copy the file created to the Active Directory machine.

2. In a Console Root window on the Active Directory machine, under **Certification Authority (Local)**, right-click the certificate root authority and then click **All Tasks** > **Submit new request**.
3. Select the file you copied in step 1.b on page 175 and click **Open**.
4. Choose a name for the certificate file and click **Save**.
5. Copy the certificate file to the Lync or Skype for Business front-end server.
6. Go to **Start** > **Lync Server Management Shell**.
7. Run the following command:

    ```
    Import-CsCertificate -Path path-to-certificate-file -PrivateKeyExportable $true
    ```

8. Run the Lync Server Deployment Wizard.
9. Click **Install or Update Lync Server System**.
10. Click **Request, Install or Assign Certificates**.
11. In the Certificate Wizard window, select the default certificate and click **Assign**.

12. In the Certificate Assignment window, click **Next**.
13. In the Certificate Store area, select the imported certificate and click **Next**.
14. In the Certificate Assignment Summary area, click **Next**.
15. In the Executing Commands window, wait for the task status to be completed and then click **Finish**.
16. Close the Certificate Wizard window.
17. Exit the Deployment Wizard.

Multiple domains for Avaya Multimedia Messaging users

The Avaya Multimedia Messaging users might be in one or multiple different domains than the Lync or Skype for Business users. Lync or Skype for Business recognizes one domain as local and any other domain must be federated. If the Avaya Multimedia Messaging and the Lync or Skype for Business users are part of two different domains of the same enterprise, then you can set up the domain as a static route instead of configuring a Lync edge server. You must also add this domain to the SIP federated domains list, without entering the Edge server details, in the Lync or Skype for Business front-end server control panel, in **Federation and External Access** > **SIP Federated Domains**.

Placing the System Manager CA certificate into the Lync or Skype for Business Trust Store

Procedure

1. Obtain the certificate file from System Manager
   a. In the System Manager web interface, navigate to **Services** > **Security** > **Certificates** > **Authority** > **CA structure and CRLs**.
   b. Click **Download pem file**.
2. Place the certificate in the Lync edge server.

Microsoft federation with external domains

Microsoft federation with external domains requires Avaya Session Border Controller for Enterprise (Avaya SBCE). A SIP entity link between Session Manager and the Lync or Skype Edge servers is no longer supported. Avaya SBCE modifies the SIP messages that are destined for the Edge servers. For information about Microsoft federation with external domains, see *Avaya Aura® Presence Services Snap-in Reference*. On Avaya SBCE, you must also add the following headers in the Global Profiles/Topology Hiding area for the topology from or to the Session Manager from Edge:

- **Request-Line**: Overwrite with the Avaya Aura® domain.
- **To**: Overwrite with the Avaya Aura® domain.
- **From**: Overwrite with the Skype or external domain.

For domain policies, when creating the end point policy group in Avaya SBCE, select **No-Content-Type-Checks** for Avaya Multimedia Messaging instead of the default signaling rules that are mentioned in *Avaya Aura® Presence Services Snap-in Reference*.

Enabling Presence Services updates for Microsoft federation

About this task

Use this procedure to allow for Presence updates to Microsoft federation.

Procedure

1. From the System Manager web interface, navigate to **Elements** > **Avaya Breeze**.
2. Navigate to **Configuration** > **Attributes**.
3. Click the **Service Clusters** tab and then do the following:
    a. Select the correct cluster.

    b. From the **Service** drop-down menu, select **PresenceServices**.
4. Do one of the following:
    - If using Lync, click the arrow ▼ to expand the Lync federation items.
    - If using Skype for Business, Click the arrow ▼ to expand the Microsoft federation items.
5. If you are using Lync federation, select the **Override Default** check box for each item and set the following values:
    a. Set **Lync Federation Enabled** to **True**.

    b. In **Lync Domain Name List**, use a comma-separated list to enter the federated Lync domains.

    This list is used for External Domains.

    c. In **Lync Shared Domain List**, use a comma-separated list to enter the URLs of the federated Lync domains that are accessible through the Lync front-end server.

    This list is used for Internal Domains.
6. If you are using Skype for Business, select the **Override Default** check box for each item and set the following values:
    a. Set **Microsoft Federation Enabled** to **True**.

    b. In **External Microsoft Domain List**, use a comma-separated list to enter the domains handled by Microsoft that are external to the enterprise where Presence Services are deployed.

    c. In **Microsoft Shared Domain List**, use a comma-separated list to enter the domains handled by Microsoft that are internal to the enterprise where Presence Services are deployed.

DNS configuration

DNS configuration for Lync or Skype for Business

Servers that Lync or Skype for Business communicates with using SIP must have an FQDN that is accessible through the DNS lookup service. Lync or Skype for Business cannot communicate with an external server that is identified by only an IP address. The Lync or Skype for Business edge server is designed for external communication. The Lync or Skype for Business front-end server can only handle SIP messages that:

- Have the Lync or Skype for Business domain in the request URI.
- Do not have a route header.

Use the following type of DNS entry for inter-domain access in all domains that are federated through the Lync or Skype for Business edge server:

```
_sipfederationtls._tcp.<remote.domain>
```

SRV records for Lync or Skype for Business client DNS processing

Lync or Skype for Business clients use DNS to discover services. For information about determining the DNS requirements for your Lync or Skype for Business server, see https://technet.microsoft.com/en-us/library/gg398758.aspx.

The following SRV records are queried and returned in this order during DNS lookup for all Lync or Skype for Business clients, except for the Lync Windows Store application:

SRV record	Description
`lyncdiscoverinternal.<domain>`	A host record for the Automatic discovery service on the internal Web service.
`lyncdiscover.<domain>`	A host record for the Automatic discovery service on the external Web service.
`_sipinternaltls._tcp.<domain>`	SRV service locator record for internal TLS connections.
`_sipinternal._tcp.<domain>`	SRV service locator record for internal TCP connections. This is only performed if TCP is allowed.
`l_sip._tls.<domain>`	SRV service locator record for external TLS connections.
`lsipinternal.<domain>`	A host record for the front-end pool or directory, resolvable only on the internal network.
`sip.<domain>`	A host record for the front-end pool or directory on the internal network, or the Access Edge service when the client is external.
`sipexternal.<domain>`	A host record for the Access Edge service when the client is external.

DNS configuration for the Avaya Multimedia Messaging server

The SIP adaptor for the Avaya Multimedia Messaging server can handle communication with servers identified by either an FQDN or an IP address. Avaya Multimedia Messaging relies on the SRV DNS records when it is set up to spread traffic across multiple Session Manager servers. Instead of setting up a SIP adaptor for each Session Manager, Avaya Multimedia Messaging queries for the following pattern in the SRV records:

```
_amm-sm._tcp.DOMAIN
```

`DOMAIN` can be one of the following domains administered on Avaya Multimedia Messaging:

- Message domains
- Remote domains
- External domains

Avaya Multimedia Messaging cluster configuration with Lync or Skype for Business interoperability

The following sections describe how to set up an Avaya Multimedia Messaging cluster with Microsoft federation. Start with a normal Avaya Multimedia Messaging cluster and then add Lync or Skype for Business interoperability.

Avaya Multimedia Messaging cluster with Lync or Skype for Business checklist

The following checklist outlines the tasks you must perform to configure an Avaya Multimedia Messaging cluster with Lync or Skype for Business.

No.	Task	Reference	✔
1	Configure a normal Avaya Multimedia Messaging cluster.	Clustering configuration on page 114	
2	Make each nodal IP a trusted node on Lync or Skype for Business, and ensure that the Lync or Skype for Business server can resolve the node's FQDN. You must do the following: • Add each Avaya Multimedia Messaging server node to Lync or Skype for Business as a trusted application. • Ensure that each Avaya Multimedia Messaging server node is in DNS.	Configuration of Avaya Multimedia Messaging as a Lync or Skype for Business trusted server on page 168	

Table continues…

No.	Task	Reference	✔
3	Make the virtual IP a trusted node on Lync or Skype for Business, and ensure that the Lync or Skype for Business server can resolve the cluster's FQDN.	Adding each Avaya Multimedia Messaging server node and front-end FQDN as a trusted application to Lync or Skype for Business Standard Edition on page 168 Adding each Avaya Multimedia Messaging server node and front-end FQDN as a trusted application for Lync or Skype for Business Enterprise Edition on page 170	
4	Configure SIP entities in System Manager.	SIP entities on page 161	
5	Complete the Local Host Resolution Table in System Manager.	Adding Avaya Multimedia Messaging nodes to the Local Host Resolution Table on page 160	
6	Set the IM Gateway SIP entity for a user in an Avaya Multimedia Messaging cluster.	Setting the IM Gateway SIP entity for a user in an Avaya Multimedia Messaging on page 162	

User configuration

The following types of Lync or Skype for Business and Avaya Multimedia Messaging users exist:

- Lync or Skype for Business only
- Avaya Multimedia Messaging only

Note:

Avaya Multimedia Messaging does not support dual users.

User configuration checklist

The following checklist outlines the tasks that you must perform to configure Lync or Skype for Business and Avaya Multimedia Messaging users.

No.	Task	✔
1	Add Lync or Skype for Business users to the Lync or Skype for Business server.	
2	Administer Avaya Equinox® on System Manager as a SIP endpoint with the appropriate profiles. The presence profile must be set up with Avaya Multimedia Messaging as the IM Gateway.	

Table continues…

No.	Task	✔
	For information about configuring Avaya Equinox® settings, see *Using Avaya Equinox® for Android, iOS, Mac, and Windows*.	
3	Configure Lync or Skype for Business-only and Avaya Multimedia Messaging-only users.	

Adding Lync or Skype for Business users to the Lync or Skype for Business server

Procedure

1. Open the Lync or Skype for Business Server Control Panel and log in as the domain administrator.
2. Click the **Users** tab on the left.
3. Click **Enable users** on the right.
4. Click **Add**.
5. Type the name of the user to add in the Search window and click **Find**.
6. Click **OK**.
7. From the **Assign users to a pool** drop-down menu:
    a. Select the desired pool.
    b. Click **Enable**.

    The user you selected is added to the list of users and is marked as *Enabled*.

Configuration of Lync or Skype for Business-only and Avaya Aura®-only users

In an Avaya Aura® environment, Avaya Multimedia Messaging must use an LDAP attribute for the primary contact. The attribute must have the same value as the user's presence or IM handle in System Manager.

Attributes for configuring users

The following attributes are used when configuring users as Lync or Skype for Business-only and Avaya Aura®-only users on System Manager and Active Directory:

Communication address

Attribute	Description	Example
	System Manager User Management > User > Communication address	
Avaya Presence IM	The user's Presence IM address, which will define the Avaya Aura® only users address of record for both Presence and IM on Session Manager.	alice@example.com

Presence profile

Attribute	Description	Example
	System Manager User Management > User > Presence profile	
System	The user's Avaya Aura® Presence Services server. If this attribute and the Presence Services IM handle are set, then the user is enabled for Avaya Aura® Presence Services. The value is a reference to the Presence server.	uc-pres
IM Gateway SIP Entity	The user's Avaya Aura® IM server. If this server is set to the same server as System, Presence Services handles the user's IM. If it is set to the Avaya Multimedia Messaging SIP entity, Avaya Multimedia Messaging handles the user's IM. **Important:** This attribute must be set to the Avaya Multimedia Messaging front-end SIP entity.	uc-amm

Active Directory attributes

Attribute	Description	Example
msRTCSIP-PrimaryUserAddress	The SIP address of a Lync or Skype for Business user. For Lync or Skype for Business users, this defines the Lync or Skype for Business address of record for both IM and Presence. For Avaya Aura® users, this can be configured to allow Lync or Skype for Business users in the same active directory forest to use search to find the Avaya Aura® users IM and Presence address. In order for this attribute to be of any use, it must be equal to the Aura users Presence or IM handle from above. The SIP schema is usually prefixed to the use the handle.	sip:address123@exmpl.com
msRTCSIP-UserEnabled	The boolean that indicates whether Lync or Skype for Business has enabled the user. For Lync or Skype for Business users, this will be set by the Lync or Skype for Business client configuration. For Avaya Aura® users, this must be FALSE or not set to force Lync or Skype for Business to use an alternate static route to the user.	FALSE

Note:

For Avaya Aura® users, the `msRTCSIP-PrimaryUserAddress` must be equal to Avaya Aura® Presence Services or IM handle defined in the communication addresses of the Avaya Aura® users. You can do one of the following:

- Add a new Avaya Aura®-only user for which you create a new `msRTCSIP-PrimaryUserAddress` with the current SIP handle.

- Migrate an existing Lync or Skype for Business user to become an Avaya Aura®-only user. You can change the `msRTCSIP-Enable` value to FALSE and add an additional SIP handle to match `msRTCSIP-PrimaryUserAddress`.

Chapter 10: Avaya Multimedia Messaging remote access configuration

You can configure the Avaya Multimedia Messaging server to be accessible to remote workers using Avaya Equinox® clients from outside the enterprise network. The following configuration methods are available:

- Virtual private Network (VPN)
- Avaya Session Border Controller for Enterprise (Avaya SBCE)
- Application Delivery Controllers (formerly named Reverse Proxies)

The following section contains an example for configuring the remote access feature using Avaya Session Border Controller for Enterprise and instructions for configuring the A10 Thunder ADC.

Configuring remote access

About this task

You can use the Avaya SBCE for relaying HTTP and HTTPS traffic between Avaya Multimedia Messaging enabled application clients (such as the Avaya Equinox® clients) and the Avaya Multimedia Messaging server. For more information about relay services configuration in Avaya SBCE, see *Administering Avaya Session Border Controller for Enterprise.*

Before you begin

- If a reverse proxy or relay is configured to listen on a port other than the default port 443, the **Override port for reverse proxy** setting from the **Front-end host, System Manager and Certificate Configuration** menu must be set to `y` (yes). You must also set a value for the **Front-end port for reverse proxy** parameter.
- HTTPS traffic relay for Avaya Multimedia Messaging requires that you configure an external IP address for Avaya SBCE.

Note:

To use the remote worker functionality, you must configure one of the following:

- Implement Split-Horizon DNS: Avaya recommends the use of this configuration. This configuration optimizes traffic so that clients connect to Session Manager directly on the internal network and only use Avaya SBCE when external.

- Use Public cloud model: All FQDNs or URLs must point to the reverse proxy or Avaya SBCE. This configuration is used for cloud deployments and also for on premise deployments. By using this configuration, calls are preserved during any network transition from Wi-Fi to cellular data when the client IP address can change during an active call.
- Implement for internal access only and all remote devices must use VPN: This configuration is used when a security policy is in place such that all traffic must be either internal or via VPN. The VPN solution that is deployed must have sufficient bandwidth and latency to support the expected volume of VoIP calls.

Procedure

1. In the Avaya SBCE, navigate to **Device Specific Settings** > **Relay Services**.
2. In the **Remote Configuration** field, configure the parameters with the following values:
   - **Remote Domain**: the Avaya Multimedia Messaging server domain.
   - **Remote IP**: the IP address of the Avaya Multimedia Messaging server.
   - **Remote Port**: the **Front-end port for reverse proxy** configured during the Avaya Multimedia Messaging server installation. The default value is 443.
   - **Remote Transport**: TCP.
3. In the **Device Configuration** field, configure the parameters with the following values:
   - **Published Domain**: the Avaya Multimedia Messaging server domain.
   - **Listen IP**: the External Avaya SBCE IP address created for Avaya Multimedia Messaging relay.
   - **Listen Port**: 8443 or 443.
   - **Connect IP**: the internal Avaya SBCE IP address.
   - **Listen Transport**: TCP.

Reverse proxy configuration

Checklist for reverse proxy configuration

In networks where connections to an Avaya Multimedia Messaging instance go through Avaya SBCE placed in a DMZ, some additional configurations are required for the reverse proxy.

Important:

- Ensure that you use TLS 1.2 for appropriate negotiation.
- In the Avaya SBCE client or server profile for proxies, only use a single trusted CA.

No.	Task	Notes	✔
1	Configure Avaya Multimedia Messaging with the appropriate front end certificate.	The Front-end IP or address configured during installation is used as the common name for the nginx certificate and published during resource discovery. The front-end certificate is used on port 443 and is located at `/opt/Avaya/MultiMediaMessaging/<version>/CAS/<version>/nginx/certs/nginx.crt`.	
2	Generate certificate request on Avaya SBCE by using the Avaya Multimedia Messaging front-end FQDN.	See Creating a Certificate Signing Request on page 186.	
3	Issue certificate from Certificate Authority.	See Creating an end entity on page 189 and Creating the certificate using a CSR on page 189.	
4	Ensure port 443 is open on both sides of Avaya SBCE.		
5	Install server certificates on Avaya SBCE.	See Uploading certificate file on page 190 and Synchronizing and installing certificate in a multi-server deployment on page 191.	
6	Install client certificates on Avaya SBCE.	See Downloading the System Manager PEM certificate on page 192 and Installing CA certificate on page 193.	
7	Create client and server TLS profiles.	See Creating a new TLS server profile on page 193 and Creating a client profile on page 195.	
8	Add reverse proxy.	See Adding a reverse proxy on page 197.	

Creating a Certificate Signing Request

Procedure

1. Log in to the Avaya SBCE EMS web interface with administrator credentials.
2. In the left navigation pane, click **TLS Management** > **Certificates**.

   The system displays the Certificates screen.
3. Click **Generate CSR**.

   The system displays the TLS Management Generate CSR window.

4. Enter the appropriate information in the TLS Management Generate CSR screen, and click **Generate CSR**.

   Ensure that the **Key Encipherment** and **Digital Signature** check boxes are selected. Do not clear these check boxes.

TLS Certificates screen field descriptions

Certificates tab

Name	Description
Installed Certificates	Some Certificate Authority (CA) signed certificate or self-signed certificate. This certificate is incorporated into a server certificate profile and sent to clients to set up a TLS connection. **Note:** All certificates, certificate authorities, and certificate revocation lists uploaded to the EMS must be valid X.509 certificates in the PEM format. Certificates not in this format might be converted using a proper SSL tool, such as the publicly available OpenSSL tool. You can access this tool from https://www.openssl.org/.
Installed CA Certificates	The unsigned public key certificates from a Certificate Authority (CA), which vouch for the correctness of the data contained in a certificate and verify the signature of the certificate.
Installed Certificate Revocation Lists	The Certificate Revocation Lists (CRLs) that contain the serial numbers of CSRs that have been revoked, or are no longer valid, and should not be relied upon by any system subscriber.

Install Certificate

Name	Description
Type	The type of certificate that you want to install. Options are: **Certificate**, **CA Certificate**, or **Certificate Revocation List**.
Name	The name of the certificate that you want to install. This field is optional, and if not specified, the filename of the uploaded certificate is used as the certificate name. Additionally, specifying a name same as another certificate will overwrite the existing certificate with the one being uploaded.
Overwrite Existing	An option to control whether uploading a certificate with the same name is permitted. If this field is cleared, uploading a certificate with the same name as another certificate causes failure. If this field is selected, when you upload a certificate with the same name overwrites an existing certificate.

Table continues…

Name	Description
Allow Weak/Certificate Key	An option to permit usage of a weak private keys. This option bypasses the check that requires strong private keys. EMS rejects private keys lesser than 2048 bits or signed with an MD5 based hash by default.
Certificate File	The location of the certificate on your system. Depending on your browser, click **Browse** or **Choose file** to browse for the file. If the third party CA provides separate Root CA and Intermediate certificates, you must combine both files into a single certificate file for Avaya SBCE. To combine the files, add the contents of each certificate file one after the other, with the root certificate at the end.
Trust Chain File	The trust chain file used to verify the authenticity of the certificate. Depending on the browser, click **Browse** or **Choose File** to locate the file.
Key	The private key that you want to use. You can opt to use the existing key from the filesystem or select a file containing another key.
Key File	The button that is displayed when you select **Upload Key File** in the **Key** field. Depending on the browser, click **Browse** or **Choose File** to locate the file.

Generate CSR

Name	Description
Country Name	The name of the country within which the certificate is being created.
State/Province Name	The state/province where the certificate is being created.
Locality Name	The locality (city) where the certificate is being created.
Organization Name	The name of the company or organization creating the certificate.
Organizational Unit	The group within the company or organization creating the certificate.
Common Name	The name used to refer to or identify the company or group creating the certificate. You cannot provide wildcard (*) characters in this field.
Algorithm	The hash algorithms (SHA256) to be used with the RSA signature algorithm.
Key Size (Modulus Length)	The certificate key length (2048, or 4096) in bits.
Key Usage Extension(s)	The purpose for which the public key might be used: Key Encipherment, Non-Repudiation, Digital Signature. The Digital Signature and Key Encipherment options are selected by default.
Subject Alt Name	An optional text field that can be used to further identify this certificate. You can provide multiple comma-separated entries in this field. You cannot provide wildcard (*) characters in this field. Avaya SBCE does not support SIP URI as a valid value for the **Subject Alt Name** field.
Passphrase	The password used when encrypting the private key.
Confirm Passphrase	A verification field for the Passphrase.

Table continues…

Name	Description
Contact Name	The name of the individual within the issuing organization acting as the point-of-contact for issues relating to this certificate.
Contact E-mail	The e-mail address of the contact.

Creating an end entity

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. Click **RA Functions** > **Add End Entity**.
4. On the Add End Entity page, in **End Entity Profile**, select **INBOUND_OUTBOUND_TLS**.
5. Type the username and password.

   The password is mandatory for each end entity. Without the password, you cannot generate the certificate from System Manager because you require the password to authenticate the certificate generation request.
6. Enter the relevant information in the fields.

   The system automatically selects the following:

   - **ID_CLIENT_SERVER** in **Certificate Profile**
   - **tmdefaultca** in **CA**
   - **User Generated** in **Token**

     With **User Generated**, the system generates the certificate by using CSR. You can also select **P 12 file**.
7. Click **Add**.

   The system displays the message `End Entity <username> added successfully`.

Creating the certificate using a CSR

Before you begin

Create an end entity as described in Creating an end entity on page 189.

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. In the left navigation pane, click **Public Web**.

4. On the public EJBCA page, click **Enroll** > **Create Certificate from CSR**.
5. To get your certificate, on the Certificate Enrollment from a CSR page, do the following:
    a. Enter the same username and the password that you provided while creating the end entity.
    b. In the text box, paste the PEM-formated PKCS10 certification request.
    c. Click **OK**.

    A certificate in PEM format is generated. The certificate contains the values provided in the end entity.

Uploading certificate file

Before you begin

Obtain the signed certificate from the Certificate Authority (CA). You might also receive a certificate trust chain if the CA did not directly sign the certificate. The certificate trust chain might be provided as a separate file or it might be concatenated directly onto the signed certificate.

If the signed certificate is not in a PEM-encoded format, reencode the certificate in the PEM format before uploading it to the EMS.

An open-source SSL library with utilities for conversions is available at: http://www.openssl.org

You can use this utility to convert a file with a DER-encoded format to a PEM format, as shown in the example below:

```
openssl x509 –in input.der –inform DER –out output.pem –outform PEM
```

You can convert a certificate with a .PEM extension to the .CRT extension by renaming the file and changing the PEM extension to .CRT.

Procedure

1. In the left navigation pane, click **TLS Management** > **Certificates**.
2. Click **Install**.
3. In the **Type** field, select **Certificate**.
4. In the **Name** field, type the name of the Certificate file.

    Note:

    You can type only letters, numbers, and underscores in the **Name** field. Enter the name of the Certificate file that is uploaded to the EMS. If the name of the Certificate file that you browse for uploading has a different name, that name will be changed with the Certificate name that is uploaded to the EMS.
5. In the **Certificate File** field, click **Browse** and browse to the location of the Certificate file.

6. In the **Key** field, select one of the following options:

    - **Use Existing Key from Filesystem**: Select this option if you generated a CSR from the Generate CSR screen. In this option, the key file is already in the correct location on the EMS.

        ✳ **Note:**

        If you are using this option, ensure that the Common Name in the Generate CSR screen matches with the name of the install certificate.

    - **Upload Key File**: Select this option if you generated a CSR by using an alternate method than the built-in Generate CSR screen.

        In this option, you must upload the private key as described in Step 7.

7. **(Optional)** In the **Key File** field, click **Browse** and browse to the location of the key file
8. In the **Trust Chain File** field, click **Browse** and browse to the location of the trust chain file.

    This step is required if the CA provided a separate certificate trust chain.

    If the third party CA provides separate Root CA and Intermediate certificates, you must combine both files into a single certificate file for Avaya SBCE. To combine the files, add the contents of each certificate file one after the other, with the root certificate at the end.

9. Click **Upload**.

    The system uploads the signed X.509 certificate, and the key file, if necessary, to the EMS.

Next steps

Synchronize the certificate to Avaya SBCE through a secure shell (SSH) session.

Synchronizing and installing certificate in a multi-server deployment

About this task

A multi-server deployment can consist of one or more Avaya SBCE HA pairs or multiple individual Avaya SBCE servers. Use this procedure to synchronize and install certificates for each Avaya SBCE server in the multi-server deployment.

Procedure

1. Using a terminal emulation program such as PuTTY, start a secure shell (SSH) connection to each Avaya SBCE individually in a multiple server deployment.
2. In the **Host Name (or IP address)** field, type the IP address of an individual SBCE box.
3. In the **Port** field, type `222` and click **Open**.

    A short delay might occur before connecting.

4. To log in to Avaya SBCE, use ipcs login and password.

5. At the $ prompt, type `sudo su` and press `Enter`.

   The system displays a prompt to enter the password.

6. At the password prompt, type the ipcs password.
7. At the # prompt, type `clipcs` and press `Enter`.

   The system displays the CLIPCS console commands level, which is one level below root-level. For a list and descriptions of available CLIPCS commands, see “CLIPCS Console Commands”.

8. At the # prompt, type `certsync` and press `Enter`.

   Avaya SBCE synchronizes with EMS and displays the list of available certificates.

9. Type `certinstall` *`certificate_file_name`*, where *certificate_file_name* is the name of the certificate file that you want to install.

   If the **`certinstall`** command does not accept the certificate file name that you enter, rename the file with extension .crt and enter the filename again.

10. When the system requests the key passphrase, enter the passphrase.

    If you used the CSR generation utility that is built into Avaya SBCE, the passphrase is the password you entered in the Generate CSR screen.

11. At the # prompt, type `exit` and press `Enter`.

    The system exits the program level and displays the $ prompt.

12. At the $ prompt, type `exit` and press `Enter`.

    The system exits the secure shell session. You can also exit the session by clicking the Cancel (X) button in the upper-right portion of the window.

13. Use the EMS web interface to restart the Avaya SBCE application.

Downloading the System Manager PEM certificate

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **CA Structure & CRLs**.
4. Click **Download PEM file**.

   The system downloads the `.pem` file on your system.

Installing CA certificate

Procedure

1. In the left navigation pane, click **TLS Management** > **Certificates**.
2. Click **Install**.
3. In the **Type** field, select **CA Certificate**.
4. In the **Name** field, type a name for the certificate.
5. Click **Browse** to locate the certificate file.
6. Click **Upload**.

Creating a new TLS server profile

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **TLS Management** > **Server Profiles**.

   The system displays the Server Profiles screen.
3. Click **Add**.

   The system displays the New Profile window.
4. Enter the requested information into the appropriate fields.
5. Click **Finish**.

   The TLS Server profile is created, installed, and listed in the application pane.

TLS server profile screen field descriptions

Both TLS Server Profiles and TLS Client Profiles share the same configuration parameters. Therefore, the parameter descriptions in the following table match those in the table in TLS Client Profile Pop-up Screen Field Descriptions on page 196

Note:

The only exception is regarding the Peer Verification parameter setting (see description below). This setting determines if a peer verification operation should be performed. In a TLS client profile, the Peer Verification parameter setting cannot be changed and is locked to: **Required**, while in a TLS server profile, the Peer Verification parameter may be set to one of three possible values: **Required**, **Optional**, or **None**.

Field	Description
TLS Profile	

Table continues…

Field	Description
Profile Name	The descriptive name used to identify this profile.
Certificate	The certificate presented when requested by a peer.
Certificate Info	
Peer Verification	One of three check boxes indicating whether peer verification is required: • Required: The incoming connection must provide a certificate, the certificate must be signed by one of the Peer Certificate Authorities, and not be contained in a Peer Certificate Revocation List. In a client profile configuration screen, the **Required** check box is a locked setting and cannot be deselected. • Optional: The incoming connection may optionally provide a certificate. If a certificate is provided, but is not contained in the Peer Certificate Authority list, or is contained in a Peer Certificate Revocation List, the connection will be rejected. • None: No peer verification will be performed. **Note:** Peer Verification is always required for TLS Client Profiles, therefore the **Peer Certificate Authorities**, **Peer Certificate Revocation Lists**, and **Verification Depth** fields will be active.
Peer Certificate Authorities	The CA certificates to be used to verify the remote entity identity certificate, if one has been provided. **Note:** Using **Ctrl** or **Ctrl+Shift**, any combination of selections can be made from this list. Using **Ctrl+Shift** , the user can drag to select multiple lines, and using **Ctrl**, the user can click to toggle individual lines.
Peer Certificate Revocation Lists	Revocation lists that are to be used to verify whether or not a peer certificate is valid. **Note:** Using **Ctrl** or **Ctrl+Shift**, any combination of selections can be made from this list. Using **Ctrl+Shift** , the user can drag to select multiple lines, and using **Ctrl**, the user can click to toggle individual lines.
Verification Depth	The maximum depth used for the certificate trust chain verification. Each CA certificate might also have its own depth setting, referred to as the path length constraint. If both are set, the lower of these two values is used.
Renegotiation Parameters	
Renegotiation Time	The amount of time after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable.

Table continues…

Field	Description
Renegotiation Byte Count	The amount of bytes after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable.
Handshake Options	
Version	The TLS versions that the client or servers accepts or offers. The options are: • TLS 1.2 • TLS 1.1 • TLS 1.0 The default value for this field is TLS 1.2. Ensure that you select an appropriate TLS version according to the TLS version that the server supports.
Ciphers	The level of security to be used for encrypting data. Available selections are: • Default: The cipher suite recommended by Avaya. • FIPS: The cipher suite recommended by Avaya for FIPS 140–2 compatibility. • Custom: Selecting the Custom radio button enables a user-defined level of encryption that can be configured by using the Value field described below.
Value	A field provided to contain a textual representation of the ciphers settings used by OpenSSL. For a full list of possible values, see the OpenSSL ciphers documentation at http://www.openssl.org/docs/apps/ciphers.html. **Note:** The Value field is an advanced setting that must not be changed without an understanding of how OpenSSL handles ciphers. Invalid or incorrect settings in this field can cause insecure communications or even catastrophic failure.

Creating a client profile

Procedure

1. Log in to Avaya SBCE EMS web interface with administrator credentials.
2. In the left navigation pane, click **TLS Management** > **Client Profiles**.
3. Click **Add**.

   The system displays the **New Profile** window.
4. Enter the requested information in the appropriate fields.
5. Click **Finish**.

   The system installs and displays the new TLS client profile.

TLS client profile screen field descriptions

Both TLS Server Profiles and TLS Client Profiles share the same configuration parameters. Therefore, the parameter descriptions in the following table match those in the table in TLS server profile pop-up window field descriptions on page 193.

Note:

The only exception is regarding the Peer Verification parameter setting. This setting determines whether a peer verification operation must be performed. In a TLS client profile, the Peer Verification parameter setting cannot be changed and is locked to: **Required**. In a TLS server profile, the Peer Verification parameter can be set to one of three possible values: **Required**, **Optional**,or **None**.

Name	Description
TLS Profile	
Profile Name	A descriptive name used to identify this profile.
Certificate	The certificate presented when requested by a peer.
Certificate Info	
Peer Verification	The incoming connection must provide a certificate, the certificate must be signed by one of the Peer Certificate Authorities, and not be contained in a Peer Certificate Revocation List. In a client profile configuration screen, the **Required** is selected for this field. **Note:** Peer Verification is always required for TLS Client Profiles, therefore the **Peer Certificate Authorities**, **Peer Certificate Revocation Lists**, and **Verification Depth** fields will be active.
Peer Certificate Authorities	The CA certificates to be used to verify the remote entity identity certificate, if one has been provided. **Note:** Using **Ctrl** or **Ctrl+Shift**, any combination of selections can be made from this list. Using **Ctrl+Shift** , the user can drag to select multiple lines, and using **Ctrl**, the user can click to toggle individual lines.
Peer Certificate Revocation Lists	Revocation lists that are to be used to verify whether a peer certificate is valid. **Note:** Using **Ctrl** or **Ctrl+Shift**, any combination of selections can be made from this list. Using **Ctrl+Shift** , the user can drag to select multiple lines, and using **Ctrl**, the user can click to toggle individual lines.
Verification Depth	The maximum depth used for the certificate trust chain verification. Each CA certificate might also have its own depth setting, referred to as the path length constraint. If both are set, the lower of these two values is used.
Renegotiation Parameters	

Table continues…

Name	Description
Renegotiation Time	The amount of time after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable.
Renegotiation Byte Count	The number of bytes after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable.
Handshake Options	
Version	The TLS versions that the client or servers accepts or offers. The options are: • TLS 1.2 • TLS 1.1 • TLS 1.0 The default value for this field is TLS 1.2. Ensure that you select an appropriate TLS version according to the TLS version that the client supports.
Ciphers	The level of security to be used for encrypting data. Available selections are: • Default: The cipher suite recommended by Avaya. • FIPS: The cipher suite recommended by Avaya for FIPS 140–2 compatibility. • Custom: Selecting the Custom radio button enables a user-defined level of encryption that can be configured by using the Value field described below.
Value	A field provided to contain a textual representation of the ciphers settings used by OpenSSL. For a full list of possible values, see the OpenSSL ciphers documentation at http://www.openssl.org/docs/apps/ciphers.html. **Note:** The Value field is an advanced setting that must not be changed without an understanding of how OpenSSL handles ciphers. Invalid or incorrect settings in this field can cause insecure communications or even catastrophic failure.

Adding a reverse proxy

About this task

Use this procedure to configure the reverse proxy with the listed IP towards the enterprise and connect the IP to the network outside the enterprise.

In a remote worker environment, ensure split DNS configuration for Avaya Aura$^{®}$ Device Services to function properly.

Procedure

1. Log on to EMS.
2. In the left navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.

The system displays the Relay Services page.

3. In the **Reverse Proxy** tab, click **Add**.
4. On the Add Reverse Proxy page, do the following:
    a. In the **Service Name** field, type the reverse proxy profile name.
    b. Select the **Enabled** check box.
    c. In the **Listen IP** field, click the external SBC IP address.
    d. In the **Listen Protocol** field, select the protocol published towards remote workers.

       If you select the HTTPS protocol, the system enables the **Listen TLS Profile** field.
    e. In the **Listen TLS Profile** field, click the TLS profile you created.

       The default TLS profiles, such as AvayaSBCServer have demonstration certificates. For optimum security, Avaya recommends that you do not use demonstration certificates.
    f. In the **Listen Port** field, type 443 or the override port defined on Avaya Multimedia Messaging
    g. In the **Server Protocol** field, click the protocol used for the Avaya SBCE server.

       For security reasons, Avaya recommends the use of HTTPS.
    h. In the **Server TLS Profile** field, click the TLS profile that you created.
    i. In the **Connect IP** field, click the IP address that Avaya SBCE must use for communicating with the file servers.
    j. In the **Server Addresses** field, type the Avaya Multimedia Messaging server address and port.

       This field accepts an IP address or FQDN, and port. Specify the FQDN and port in the **Server Addresses** field. This field must match the **Subject Alt Name** defined in the Avaya Multimedia Messaging server certificate.
    k. In the **Load Balancing Algorithm** field, select a load balancing algorithm.
    l. Select the **Allow Web Sockets** check box.
    m. In the **Whitelisted IPs** field, type the whitelisted IPs.
5. Click **Finish**.

Chapter 11: Administration

After you finish installation and configuration required for Avaya Multimedia Messaging is completed, additional administration and management tasks can be performed on an ongoing basis. For information about these administration and management tasks, see *Administering Avaya Multimedia Messaging*.

Chapter 12: 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 25: Avaya Equinox® and Avaya Multimedia Messaging documentation

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

Table continues…

Title	Use this document to	Audience
Using		
Using Avaya Equinox® for Android, iOS, Mac, and Windows	Install and use your Avaya Equinox® client.	Enterprise users

Table 26: Other related documents

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

Important:

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

Using the Avaya Documentation Portal, you can:

- Search for specific content.

  To perform a search:

  - Type a keyword in the **Search** field.
  - Type a keyword in **Search**, and select the filters to search for content by product, release, and document type.
  - Select the appropriate product or solution and then select the appropriate item from the list.
- Search for a document from the **Publications** menu.
- Publish a PDF of the content. You can publish a PDF of the current section only, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** (☆).

  From the **My Content** > **My Docs** menu, you can:

  - 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 to the content using the **Watch** icon (👁).

From the **My Content** > **Watch list** menu, you can:

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

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

- Share a section on social media platforms, such as Facebook, LinkedIn, Twitter, and GooglePlus.
- 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.

Appendix A: Examples of Microsoft Active Directory LDAP property files

Examples of Microsoft Active Directory LDAP configuration that uses the user ID as the account name

```
# Binding parameters
ldapUrl=ldaps://gdc.global.example.com:3269
bindDN=global\AMMAssistant
bindCredential=admin123

# Authentication parameters
uidAttrID=sAMAccoutName
baseCtxDN=dc=global,dc=example,dc=com
allowEmptyPasswords=false

# Authorization parameters based on method #2 by searching for the groups
roleFilter=(&(objectClass=group)(member={1}))
rolesCtxDN=ou=Groups,dc=global,dc=example,dc=com
roleAttrID=cn
roleAttrIsDN=false
roleNameAttrID=
roleRecursion=1
searchScope=2
adminRole=AMMAdmin
usersRole=AMMUsers
auditorRole=AMMAuditor

# Internationalization parameters
language=en

# User management parameters
activeUsersFilter=(&(objectClass=user)(objectCategory=Person)(!(userAccountControl:
1.2.840.113556.1.4.803:=2)))
lastUpdatedTimeAttr=whenChanged
```

Examples of Microsoft Active Directory LDAP configuration that uses the email address as the account name

```
# Binding parameters
ldapUrl=ldaps://gdc.global.example.com:3269
bindDN=global\AMMAssistant
bindCredential=admin123

# Authentication parameters
uidAttrID=mail
baseCtxDN=dc=global,dc=example,dc=com
allowEmptyPasswords=false

# Authorization parameters based on method #2 by searching for the groups
roleFilter=(&(objectClass=group)(member={1}))
```

```
rolesCtxDN=ou=Groups,dc=global,dc=example,dc=com
roleAttrID=cn
roleAttrIsDN=false
roleNameAttrID=
roleRecursion=1
searchScope=2
adminRole=AMMAdmin
usersRole=AMMUsers
auditorRole=AMMAuditor

# Internationalization parameters
language=en

# User management parameters
activeUsersFilter=(&(objectClass=user)(objectCategory=Person)(!(userAccountControl:
1.2.840.113556.1.4.803:=2)))
lastUpdatedTimeAttr=whenChanged
```

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/.

HA
High availability. You can deploy Avaya Multimedia Messaging in a three-node or four-node cluster to obtain increased availability.

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 Management System
A system that lets you monitor the health and status of devices on your data network.

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.

SSL (Secure Sockets Layer) Protocol

The SSL protocol is the leading security protocol on the Internet. It runs above the TCP/IP protocol and below higher-level protocols such as HTTP or IMAP. SSL uses TCP/IP on behalf of the higher-level protocols and, in the process, allows an SSL-enabled server to authenticate itself to an SSL-enabled client.

TCP

Transmission Control Protocol.

TLS

Transport Layer Security

UDP

User Datagram Protocol. This is a communication method, similar to TCP.

Index