Deploying Avaya Multimedia Messaging

Release 3.0.0.1
Issue 2
March 2017

© 2014-2017, Avaya Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

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

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number

indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

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

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

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction ... 11
Purpose ... 11
Change history ... 11
Chapter 2: Avaya Multimedia Messaging overview ... 13
Topology ... 13
Components ... 15
Virtual machine and physical server deployment specifications ... 16
Chapter 3: Deployment process ... 17
Chapter 4: Planning and pre-configuration ... 18
Planning and pre-configuration checklist ... 18
PLDS overview ... 20
Downloading software from PLDS ... 21
Licensing requirements ... 21
Server node license tracking ... 22
Security requirements ... 23
Prerequisites ... 24
VMware knowledge ... 24
Configuration prerequisites ... 25
Avaya Multimedia Messaging domains configuration ... 25
System Manager configuration ... 31
LDAP server configuration ... 34
Chapter 5: Initial setup ... 36
Installation on a physical server ... 38
Prerequisites checklist ... 38
Installing the Avaya Multimedia Messaging server ... 48
Installation on a VMware virtual machine ... 49
Deployment options ... 50
Installing the Avaya Multimedia Messaging server on a VMware virtual machine ... 52
Avaya Multimedia Messaging initial installation configuration ... 53
Performing a silent installation ... 59
Extending disk volumes ... 60
Enhanced Access Security Gateway support for Avaya Multimedia Messaging ... 61
Avaya Multimedia Messaging cluster installation ... 64
Installing an Avaya Multimedia Messaging cluster ... 65
Installing the initial cluster node ... 67
Installing an additional cluster node ... 69
Virtual IP configuration fields ... 71
Creating and expanding a Gluster file system ... 72
Rebalancing the Gluster file system after adding a new node ... 73

Adding a new node while performing an Avaya Multimedia Messaging upgrade..... 73
Changing the Cassandra user name and password..... 74
Changing the LDAP parameters after installing an Avaya Multimedia Messaging cluster..... 75
Changing the seed node of a cluster..... 75
Removing a node from the Avaya Multimedia Messaging cluster..... 76
Uninstalling the Avaya Multimedia Messaging server..... 79
Patch setup..... 79
Adding a patch to the inventory..... 80
Querying patch status..... 80
Installing a patch..... 81
Uninstalling and removing a patch from the inventory..... 81
Chapter 6: Configuration..... 82
Configuring the Avaya Multimedia Messaging server using the configuration utility..... 83
Front-end host, System Manager, and certificate configuration..... 84
LDAP configuration..... 87
Messaging domains configuration..... 97
Cassandra DB user and password..... 97
Clustering configuration..... 98
Advanced configuration..... 100
Avaya Multimedia Messaging certificate management..... 102
Command for viewing certificate details..... 103
Importing the Avaya Aura® System Manager trusted certificate..... 105
Importing local certificates..... 105
Importing intermediate CA certificates..... 107
Default Lync server certificate to put in the trust store for each Avaya Multimedia Messaging node..... 108
Messaging domains configuration..... 112
Configuring the messaging domains using the configuration utility..... 112
Configuring the messaging domains using the administration portal..... 113
LDAP settings configuration..... 113
Importing the Secure LDAP certificate using the configuration utility..... 114
Importing the Secure LDAP certificate using the web-based administration portal..... 115
LDAP configuration for Microsoft Active Directory..... 115
LDAP attribute mapping..... 124
Avaya Multimedia Messaging federation configuration with Presence Services..... 129
Presence Services side configuration..... 129
Configuring the XMPP interface in Avaya Multimedia Messaging for federation with Presence Services..... 132
Configuring the HTTPS REST interface in Avaya Multimedia Messaging for federation with Presence Services..... 133
Avaya Multimedia Messaging federation configuration with Microsoft Lync..... 134
Lync federation checklist..... 135
System Manager configuration..... 135

Avaya Multimedia Messaging server configuration..... 142
Lync server configuration for an internal domain..... 145
Lync server configuration for an external domain..... 155
Configuring Lync federation for Presence Services..... 155
DNS configuration..... 156
Avaya Multimedia Messaging cluster configuration with Lync interoperability..... 157
User configuration..... 158
Customizing the login screen message for the Message Playback component..... 161
External configuration requirements..... 162
Avaya Multimedia Messaging remote access configuration..... 163
Configuring remote access..... 163
Reverse proxy configuration..... 164
Enhanced Access Security Gateway support for Avaya Multimedia Messaging..... 178
Enabling and disabling the Enhanced Access Security Gateway..... 178
Installing and enabling the Enhanced Access Security Gateway on a physical server..... 179
Removing EASG..... 181
Chapter 7: Administration..... 182
Working with the Avaya Multimedia Messaging administration portal..... 182
Starting and stopping the Avaya Multimedia Messaging service..... 183
Managing server storage..... 183
Managing messaging domains..... 183
Updating media size limits..... 184
Updating feature entitlements..... 185
Updating enterprise directory settings..... 186
Configuring the LDAP attribute mappings..... 187
Managing trusted hosts..... 187
Managing federation gateway connections..... 187
Verifying cluster nodes..... 188
Generating performance data and statistics..... 188
Adding and editing local and remote sites for multisite configuration..... 190
Updating logging levels..... 190
Adjusting the virtual hardware of virtual machines..... 190
Adjusting the memory resource of a virtual machine..... 191
Adjusting the CPU resource of a virtual machine..... 191
Adjusting the virtual network interface..... 192
Adjusting the size of virtual disks..... 192
Adjustment of disk volume sizes..... 193
Scheduling periodic repairs of database inconsistencies..... 197
Logs and alarms..... 197
Preventing the creation of audit audispd logs on a physical server..... 202
Integrated Windows Authentication support..... 203
Authentication prerequisites..... 203
Setting up the Windows Domain Controller..... 203

Setting up IWA on the Avaya Multimedia Messaging administration portal..... 205
Avaya Multimedia Messaging multisite adapter setup..... 207
Connector types for the Avaya Multimedia Messaging adapter..... 207
Home site ID..... 207
Multisite adapter field descriptions..... 208
Backup and restore..... 209
Making a backup for an Avaya Multimedia Messaging node..... 210
Restoring an Avaya Multimedia Messaging node in a standalone deployment..... 211
Restoring a node from a cluster..... 212
Restoring a cluster..... 213
Lync recovery..... 216
Administration tools..... 217
gluster volume status..... 219
nodetool..... 220
cleanAMM..... 221
clitool..... 222
collectLogs..... 223
collectNodes..... 223
Configuring the Avaya Multimedia Messaging server to connect to a secondary System Manager node..... 224
Archiving..... 224
Enabling and disabling TLS versions..... 226
Avaya Multimedia Messaging upgrades and migrations..... 226
Avaya Multimedia Messaging migration..... 227
Restoring Avaya Multimedia Messaging to the previous version if you abort migration..... 239
Migration of the Avaya Aura® environment..... 240
Upgrading the Avaya Multimedia Messaging server..... 242
Checking for DRS synchronization after a migration or upgrade..... 245
Applying patches..... 245
Chapter 8: Troubleshooting..... 247
Troubleshooting best practices for IWA..... 247
An Avaya Multimedia Messaging node has malfunctioned and been inactive for an extended period of time..... 247
Avaya Multimedia Messaging server returns alarm code 00064: Remote domain connection lost..... 248
Cannot log in to the web-based administration portal using Internet Explorer 10..... 248
Client cannot connect to the Avaya Multimedia Messaging server..... 249
Failure to retrieve System Manager user settings..... 250
Gluster configuration failure..... 250
Gluster rebalancing fails when you add a new node..... 250
HTTP services disabled due to storage capacity reaching critical threshold..... 251
Troubleshooting License error..... 252
Troubleshooting LDAP server authentication problems..... 252

Long poll timeout for Avaya Equinox™ client connections to the Avaya Multimedia Messaging server.... 253
Troubleshooting Lync federation issues.... 253
System Manager certificate on Lync edge server is missing or invalid.... 253
Lync certificate on System Manager or Session Manager is missing or invalid.... 254
Lync certificate on Avaya Multimedia Messaging is missing or invalid.... 254
System Manager certificate on Lync Front end server is missing or invalid.... 255
SIP Adapter for Session Manager is not enabled or with a misconfigured IP address.... 255
SIP Adapter for Session Manager is not enabled or enabled with a misconfigured IP address.... 256
Avaya Multimedia Messaging node is not a trusted host on Lync.... 256
LyncAdaptation is missing from Avaya Multimedia Messaging SIP entity.... 257
Lync Adaptation is missing from Lync Edge remote server.... 257
The routing pattern to Avaya Multimedia Messaging is missing or incorrect.... 257
The routing pattern to Lync Edge is missing or incorrect.... 258
Route to the destination domain is missing.... 259
Avaya Multimedia Messaging front-end FQDN is not administered as a SIP federated provider.... 259
Avaya Multimedia Messaging user does not have presence or IM handle.... 260
System Manager data is inaccessible.... 260
LDAP data is inaccessible.... 261
Problem in System Manager administration of Avaya Multimedia Messaging SIP entities.... 262
Avaya Multimedia Messaging lost Lync session information.... 262
User did not acknowledge message receipt.... 263
Lync front-end server cannot start.... 263
Networking issues after upgrading.... 263
OpenFire log displays Requested node not found in cluster error.... 264
Participant has invalid messaging address.... 265
The resource discovery operation returns error code 404.... 265
Special characters displayed incorrectly when playing multimedia attachment.... 266
Unable to view alarms using Avaya Aura® System Manager Admin Viewer.... 267
Unable to view Avaya Multimedia Messaging logs using Log Viewer.... 268
Upgrade fails when trace logging is turned on.... 268
User is unable to log in to the Avaya Multimedia Messaging server.... 269
User is unable to send message from an Avaya Multimedia Messaging enabled client.... 269
User cannot send a message to a non-Avaya Multimedia Messaging Presence Services enabled client.... 269
Virtual IP node is inaccessible.... 270
Chapter 9: Resources.... 271
Documentation.... 271
Finding documents on the Avaya Support website.... 273
Training.... 273
Viewing Avaya Mentor videos.... 273

Support..... 274
Using the Avaya InSite Knowledge Base..... 274
Appendix A: Examples of Microsoft Active Directory LDAP property files..... 276
Appendix B: Example images of the Avaya Multimedia Messaging migration process 278
Glossary..... 302

Chapter 1: Introduction

Purpose

This document contains Avaya Multimedia Messaging planning, installation, configuration, and administration checklists and procedures.

Change history

The following table summarizes major changes in this document.

Issue	Release date	Summary of changes
Release 3.0, Issue 1	December 2016	• Added a warning about copying and pasting commands from this document. • Added additional information about configuring Presence Services in deployments with Presence federation. • Added information about configuring Lync federation. • Updated administration portal content to reflect changes made in this release. • Added Integrated Windows Authentication (IWA) setup information. • Added information about migration from one major release to another. • Updated alarm list and descriptions. • Added information about Enhanced Access Security Gateway (EASG). • Added information about patch installation. • Added a warning about patching the build before restoring data.
Release 3.0.0.1, Issue 2	March 2017	• Updated Home site ID on page 207 to indicate that user synchronization will also update the home site of users if they were changed in System Manager.

Table continues…

Issue	Release date	Summary of changes
		• Added information about deploying Avaya Multimedia Messaging on a vCenter-managed or a standalone ESXi host. • Added additional information about silent installation. • Added Extending disk volumes on page 60 to describe how to increase the size of the application and media virtual disks. • Added information about adjusting virtual hardware. • Updated migration information and described migration phases. • Indicated that you need to migrate to Release 3.0 and then upgrade to a Service Pack (SP), such as Release 3.0.0.1. • Updated the LDAP configuration information with a description of the testUser parameter.

Chapter 2: Avaya Multimedia Messaging overview

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

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

- Exchange text-based instant messages with users of Avaya Multimedia Messaging, Avaya Aura® Presence Services, Microsoft Lync, and Skype.
- 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. VMware options for the Avaya Multimedia Messaging server are also available. You can deploy Avaya Multimedia Messaging as a single server or within a cluster of servers.

Topology

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

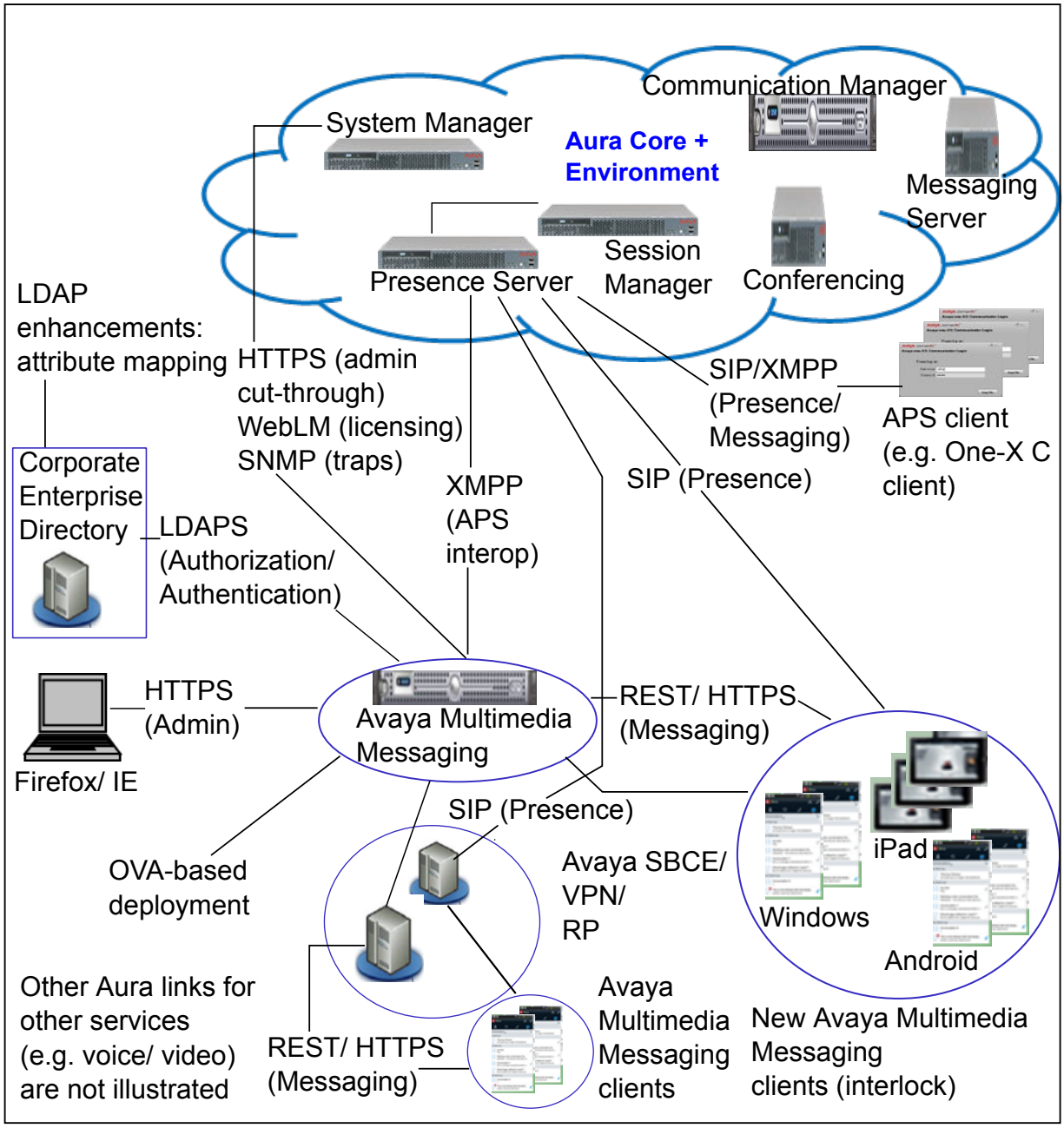


Figure 1: Avaya Multimedia Messaging deployment architecture

Components

Table 1: Avaya Multimedia Messaging Components

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

Component	Description
Avaya Aura® Core	The Avaya Aura® network, that encompasses the Avaya products needed by Avaya Multimedia Messaging: • Avaya Aura® Presence Services: For Presence and IM federation with other applications. • Avaya Aura® System Manager: For centralized Avaya Aura® management. Avaya Aura® System Manager enables: - Licensing with Avaya WebLM - Viewing capabilities for logs and alarms - Certificate management For applications to perform registration and telephony functions such as call escalation, Avaya Aura® Session Manager can also be present in the system configuration. Avaya Aura® Session Manager is an optional component. • Avaya Aura® Communication Manager: for organizing and routing voice, data, image, and video transmissions. **Note:** XMPP federations between Avaya Aura® Presence Services and other products are not supported when Avaya Multimedia Messaging is federated with Avaya Aura® Presence Services.
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

Table continues…

Component	Description
	Multimedia Messaging through the Message Playback functionality: • Avaya one-X® Communicator for Windows

Virtual machine and physical server deployment specifications

The following tables describe VMWare and physical server deployment specifications.

VMWare deployments

Specification	500 users	1000 users	5000 users
vCPUs	2	4	24
CPU resources	Minimum: 4786 GHz	Minimum: 9572 GHz	70000 MHz (unlimited)
Memory	12 GB	12 GB	32 GB
Storage reservation	0.5 TB	1 TB	5 TB
Hard drive	N/A	N/A	N/A

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

Chapter 3: Deployment process

The following table describes the deployment process for the Avaya Multimedia Messaging server.

Planning and preconfiguration	Complete Avaya Multimedia Messaging questionnaires
	Obtain components and licenses
	Connect and plug in hardware components
	Configure network
Initial setup and connectivity	Set up VMware environment or servers used for deploying Avaya Multimedia Messaging
	Install operating system and other required libraries (only for deployments on physical servers)
	Install the Avaya Multimedia Messaging software
Configuration	Configure the Avaya Multimedia Messaging server
	Configure external systems to interwork with the Avaya Multimedia Messaging server
Administration	User management
	Component management
	Monitoring and analysis
	Routine maintenance

Chapter 4: 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.

Related links

Planning and pre-configuration checklist on page 18
PLDS overview on page 20
Licensing requirements on page 21
Security requirements on page 23
Prerequisites on page 24
Configuration prerequisites on page 25

Planning and pre-configuration checklist

Table 2: 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 that you can 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 15.	
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/.	

Table continues…

Task	Notes	✔
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 for your deployment in the following Avaya Multimedia Messaging questionnaires: • Avaya Multimedia Messaging General Questionnaire: Preliminary information about the Avaya Multimedia Messaging installation requirements. • Avaya Multimedia Messaging Server Information: Specifications that apply to the Avaya Multimedia Messaging server. • Avaya Aura® Detailed Section: Information about the other Avaya Aura® components that interwork with the Avaya Multimedia Messaging server. • System Manager Detailed Section: Connecting to Avaya Aura® System Manager. • Certificate Settings: Certificate requirements. • Directory (LDAP) Settings: Configuring the Avaya Multimedia Messaging and LDAP servers to interwork. • Database (Cassandra) Settings: Settings for database credentials. • Federation Settings: Avaya Multimedia Messaging federation configuration. • Cluster Settings: Information about a cluster installation. This questionnaire only applies to cluster deployments.	
Complete site preparation.	Prepare your network so that you can install and connect equipment without costly delays. 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.	

Table continues…

Task	Notes	✔
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.	

Related links

Planning and pre-configuration on page 18

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

Related links

Planning and pre-configuration on page 18
Downloading software from PLDS on page 21

Downloading software from PLDS

About this task

Note:

You can download product software from http://support.avaya.com also.

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS website.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Search for the available downloads by using one of the following:
   - An application type and the version number
   - Download name
6. Click the download icon from the appropriate download.
7. When the system displays the confirmation box, select **Click to download your file now**.
8. If you receive an error message, click the message, install Active X, and continue with the download.
9. 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 software and enhanced user privileges are sold as licensed capabilities.

The following licenses exist for Avaya Multimedia Messaging:

- Avaya Multimedia Messaging server software: Sold per instance and by major release number. You require this license to access Avaya Multimedia Messaging services.
- Enhanced Avaya Multimedia Messaging services: Sold on a per user basis. You must enforce the Rich Content license restrictions by disabling the Rich Content feature when there is no license for a user. You must identify which users have access to Enhanced privileges in the web-based administration portal. You can change user privileges in the web-based administration portal any time.

  For more information about changing user privileges using the administration portal, see Updating feature entitlements on page 185.

By default, users are given Standard Basic privileges. No additional license, besides the server software license, is required for the Standard Basic user privilege. The following table summarizes the instant messaging features available for Basic users and Enhanced users.

Note:

When an administrator revokes your enhanced Avaya Multimedia Messaging 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 privilege entitlements will take effect when you log out and log back in to the client.

Table 3: 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

Related links

Planning and pre-configuration on page 18
Server node license tracking on page 22

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.

Related links

Planning and pre-configuration on page 18
Additional security information on page 23

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/.

Related links

Security requirements on page 23

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 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.
- 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 Linux on a physical server, ensure you modify the `ifcfg-eth0` file and set the ONBOOT parameter to `Yes`. Otherwise, the installation fails during network configuration.

VMware knowledge

You can deploy Avaya Multimedia Messaging servers directly on physical servers or on VMware virtual machines.

Note:

The supported ESXi versions for Avaya Multimedia Messaging using VMware are 5.1, 5.5, and 6.0.

Systems that need virtual disks with more than 2TB of disk space require ESXi 5.5 or 6.0.

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.

Related links

Planning and pre-configuration on page 18
Avaya Multimedia Messaging domains configuration on page 25
LDAP server configuration on page 34

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 112.

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, such as XMPP, 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.

Related links

Configuration prerequisites on page 25
Avaya Multimedia Messaging reachable domains on page 26
Supported address types on page 26
Selection of the correct routing domain for configuring XMPP federation with the Presence Services 6.2.x server on page 27
Configuring the DNS for the Presence Services — Avaya Multimedia Messaging federation on page 28
Changing the local FQDN on page 30

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

Related links

Avaya Multimedia Messaging domains configuration on page 25

Selection of the correct routing domain for configuring XMPP federation with the Presence Services 6.2.x server

An Avaya Multimedia Messaging Routing Domain (or Avaya Multimedia Messaging domain) is an XMPP domain. Choosing the proper Avaya Multimedia Messaging Routing Domain is crucial for enabling the federation with Presence Services.

From a conceptual perspective, the Avaya Multimedia Messaging is an external component of the Openfire server, as outlined by XMPP extension 0114. Therefore, the Avaya Multimedia Messaging Routing Domain is a sub-domain of the Openfire domain.

For example, if the AMM Routing Domain is "component.amm.yourcompany.com", then the Openfire domain must be "amm.yourcompany.com".

The main reason for enabling XMPP federation is to allow XMPP servers with different XMPP domains to communicate. To federate two XMPP servers, the XMPP domains must not be a sub-domain of each other.

In the current Avaya Multimedia Messaging deployment, Presence Services is federated with the Openfire server. Since changing the Presence Services domain is not trivial, Avaya recommends selecting the Avaya Multimedia Messaging Routing Domain such that the Openfire and the Presence Services domains are not a sub-domain of each other.

For example:

- Choose the Presence Services domain, for example: `pres.yourcompany.com`
- Replace the first sub-domain, for example: replace `pres` with `amm`, which results in `amm.yourcompany.com`
- Add a sub-domain, for example: `component`, to create a correct Avaya Multimedia Messaging Routing Domain, which can be `component.amm.yourcompany.com`.

SRV record configuration

A Service record (SRV record) is a specification of data in the Domain Name System (DNS) defining the location (hostname and port number) of servers for specified services. SRV records are defined in RFC 2782.

Inter-domain federation between Presence Services and Avaya Multimedia Messaging requires XMPP server SRV records such that both Presence Services and Avaya Multimedia Messaging servers can find the location of the XMPP server service for the PS and AMM domains.

An XMPP Server SRV record has the following form:

```
_service._proto.name class SRV priority weight port target
```

- **service**: the symbolic name of the desired service, which is "xmpp-server"
- **proto**: the transport protocol of the desired service, which is "tcp"
- **name**: the domain name for which this record is valid, e.g. "pres.yourcompany.com"
- **class**: standard DNS class field (this is always IN).

- **priority**: the priority of the target host, lower value means more preferred.
- **weight**: A relative weight for records with the same priority.
- **port**: the TCP or UDP port on which the service is to be found. The default port for XMPP server is "5269"
- **target**: the canonical hostname of the machine providing the service.

Note:

Priority and weight are not relevant in the context of Presence Services - Avaya Multimedia Messaging federation. The default value is sufficient.

For example:

Given the following information:

- PS domain: pres.yourcompany.com
- hostname: host.avaya.com
- port: 5269

The XMPP Server record would be `_xmpp-server._tcp.pres.yourcompany.com IN SRV 0 0 5269 host.avaya.com`.

Related links

Avaya Multimedia Messaging domains configuration on page 25

Configuring the DNS for the Presence Services — Avaya Multimedia Messaging federation

About this task

This procedure describes how to perform the DNS configuration for the Avaya Multimedia Messaging and Presence servers.

The DNS configuration consists of creating SRV records containing the following entries:

- The host name FQDN and XMPP port number
- The domain name (routing domain)

Before you begin

Before you begin the Domain Name Server (DNS) configuration, the Avaya Multimedia Messaging and Presence servers must be installed.

In a cluster setup, all the nodes must be configured to use the eth0 interface.

Procedure

1. For Avaya Aura® Presence Services, configure one SRV record for each Presence domain.

   In the following examples, the routing domain is `pres.yourdomain.com`.

   This SRV record for Presence Services 6.2.x is as follows:

   ```
   _xmpp-server._tcp.component.pres.yourdomain.com
   ```

   - Priority: 100

- Weight: 100
- Port: 5269
- SRV host name: FQDN or virtual IP of the Presence server.

This SRV record for Presence Services 7.0.x is as follows:

```
_amiogw-https._tcp.component.pres.yourdomain.com
```

- Priority: 100
- Weight: 100
- Port: 443
- SRV hostname: FQDN or virtual IP of the Presence server.

The FQDN of the target host provides the type of TCP/IP-based service that is described in the Service parameter. This name must match a valid host (A) resource record in the DNS domain namespace. If a target FQDN consisting of a single period (".") is used, it indicates to any DNS resolvers (clients) requesting this type of service that this service is not available for this domain

Note:

The priority/weight must be based on corporate policy and depends on whether there is more than one server acting as an XMPP node. In the case where there is more than one server offering the service (for example: a Presence Services cluster) the recommendation is that the priority and weight values for each record be the same.

2. (Optional) To check that the SRV records are configured properly for the Avaya Aura® Presence server, open a terminal window on the Avaya Multimedia Messaging server and run commands similar to the following:

```
nslookup -querytype=SRV _xmpp-server._tcp.pres.yourcompany.com
```

3. For the Avaya Multimedia Messaging server, configure one SRV record for every Avaya Multimedia Messaging domain.

   In the following examples, the routing domain is `component.amm.yourdomain.com`.

   The SRV record for Presence Services 6.2.x is as follows:

```
_xmpp-server._tcp.component.amm.yourdomain.com
```

   - Priority: 100
   - Weight: 100
   - Port: 5269
   - SRV host name:
     - FQDN of the Avaya Multimedia Messaging server, if the Avaya Multimedia Messaging server is deployed as a standalone server.
     - FQDN the Avaya Multimedia Messaging server virtual IP backup node, if the Avaya Multimedia Messaging is deployed in a cluster.

The SRV record for Presence Services 7.0.x is as follows:

```
_amiogw-https._tcp.component.amm.yourdomain.com
```

- Priority: 100
- Weight: 100
- Port: 8453
- SRV host name:
  - FQDN of the Avaya Multimedia Messaging server, if the Avaya Multimedia Messaging server is deployed as a standalone server.
  - FQDN the Avaya Multimedia Messaging server virtual IP backup node, if the Avaya Multimedia Messaging is deployed in a cluster.

4. (Optional) To check that the SRV records are configured properly for the Avaya Multimedia Messaging server, open a terminal window on the Presence server and run the following command:

```
nslookup -querytype=SRV _xmpp-server._tcp.component.amm.yourdomain.com
```

Related links

Avaya Multimedia Messaging domains configuration on page 25

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 Force Update of the LDAP configuration 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 32.

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.

Related links

Configuration prerequisites on page 25

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.

Related links

Configuration prerequisites on page 25

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

About this task

The following procedure describes how to add the document 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.

Related links

Configuration prerequisites on page 25

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 87. 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 115.

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.

Related links

Configuration prerequisites on page 25

Chapter 5: Initial setup

The following table summarizes the initial setup and installation tasks that you must perform for each of the following deployment models:

Tasks performed in a cluster must be repeated on each node in the cluster.

Table 4: Summary of installation tasks

Task	Physical server deployment		OVA deployment on a virtual machine	
	Single server	Cluster	Single server	Cluster
Complete Prerequisites checklist for deployments on physical servers	Y	Y Tasks performed in a cluster must be repeated on each node in the cluster.	N	N
Deploy the Avaya Multimedia Messaging OVA image using vSphere or vCenter	N	N	Y	Y Tasks performed in a cluster must be repeated on each node in the cluster.
Expand virtual machine capabilities: virtual disk sizes, RAM memory, number of CPUs	N	N	Y	Y Tasks performed in a cluster must be repeated on each node in the cluster.
Run the Avaya Multimedia Messaging installation binary	Y	Y Tasks performed in a cluster must be repeated on each node in the cluster.	Y	Y Tasks performed in a cluster must be repeated on each node in the cluster.

Table continues…

Task	Physical server deployment		OVA deployment on a virtual machine	
	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.	Y	Y Tasks performed in a cluster must be repeated on each node in the cluster.	Y	Y Tasks performed in a cluster must be repeated on each node in the cluster.
Cluster Configuration, and settings Cassandra Encryption	N	Y Tasks performed in a cluster must be repeated on each node in the cluster.	N	Y Tasks performed in a cluster must be repeated on each node in the cluster.
Configure Gluster (under Advanced Configuration)	N	As indicated in the Cluster installation section.	N	As indicated in the Cluster installation section.
Configure the Avaya Multimedia Messaging using the configuration utility. **Note:** The configuration utility starts automatically during installation, after you read and accept the End-User License Agreement. 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 the Configuration chapter.	Y	Y Tasks performed in a cluster must be repeated on each node in the cluster.	Y	Y Tasks performed in a cluster must be repeated on each node in the cluster.

Installation on a physical server

To install the Avaya Multimedia Messaging server on a physical server, you must perform the following actions:

- Complete the prerequisites checklist by performing the tasks described in the checklist.
- Run the installation binary located in the `/opt/Avaya` directory.
- Perform the additional configurations that are required.

Note:

The configurations and the administration tasks described in this document apply to the Avaya Multimedia Messaging deployments made on physical servers, as well as deployments made using OVA images.

Prerequisites checklist

The following checklist outlines the required installation steps for the prerequisites of the Avaya Multimedia Messaging server, when deployed on a physical server.

No.	Task	Notes	✔
1	Install Red Hat Enterprise Linux 6.6 (64 bit) and configure partition sizes as required by the Avaya Multimedia Messaging server.	Red Hat Enterprise Linux is the operating system to install on the Avaya Multimedia Messaging servers. You can install the Avaya Multimedia Messaging application on a physical machine or on a virtual machine, using VMWare.	
2	Create the directory structure for the Avaya Multimedia Messaging application and mount the separated hard disks used for Rich Content storage.	Avaya Multimedia Messaging is designed to function using a predefined directory structure for application files, database files, and plug-in files.	
3	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.	
4	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 the Open JDK 1.8 component.	
5	Update OpenSSL	To avoid potential vulnerabilities of the OpenSSL package installed with the	

Table continues…

No.	Task	Notes	✔
		operating system, update the OpenSSL package.	
6	Update the Linux kernel	The Linux kernel version required by the Avaya Multimedia Messaging server is 2.6.32-220.13.1 or higher.	
7	Configure the system according to the requirements of the Avaya Multimedia Messaging server.	Before you install Avaya Multimedia Messaging, you must perform the following configuration tasks on the Avaya Multimedia Messaging server: • SSH configuration • Add your host name to the /etc/hosts file • Disable SELinux • DNS configuration • Network Time Protocol (NTP) configuration	
8	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.	
9	Download the R3.0.0.1 version of the Avaya Multimedia Messaging installation file from PLDS.	None.	

Installation guidelines for the Red Hat Enterprise Linux operating system

Disk space requirements and partitioning information

For details about specifications, see *Avaya Multimedia Messaging Reference Configuration*.

Red Hat Enterprise Linux installation options

During the installation of the Red Hat Enterprise Linux operating system, you must select the following options:

- Software set: **Basic Server**
- Additional repositories: **Red Hat Enterprise Linux**

To improve the time required for the operating system installation, select the **Customize later** option for a later customization of the software selection.

Important:

Do not install the default Java package that is included in the Red Hat Enterprise Linux installation. The Java package is installed automatically at a later time, while running the Avaya Multimedia Messaging installer.

Creating the directory structure for the Avaya Multimedia Messaging server

About this task

The following procedure describes how to create the directories required for the Avaya Multimedia Messaging server and how to mount the corresponding logical volumes to the directories. You might not need to perform this procedure if it was completed through the server console when running the RedHat installer.

The directories are:

- `/opt/Avaya`: the default directory for storing Avaya Multimedia Messaging installation files and tools.

  The`/opt/Avaya` directory must be the mount point of the logical volume used for storing Avaya Multimedia Messaging installation files.

- `/media/data`: the directory for storing the Cassandra database and the Gluster file system.

  The `/media/data` directory must be the mount point of the hard disk used for storing the media files.

Procedure

1. To verify the mounted partitions and the available disk space for each partition, run the following command:

   ```
   df -h
   ```

2. **(Optional)** Do the following if it was not completed through the server console:

   a. Create the required directories:

   ```
   mkdir /opt/Avaya
   mkdir /media/data
   ```

   b. Display the available partitions and hardware devices:

   ```
   fdisk -l
   ```

   c. Note the devices to use for mounting to the Avaya Multimedia Messaging directories.

   For example:

   - `/dev/sda3` for the partition to mount to the `/opt/Avaya` directory
   - `/dev/sdb1` for the hard drive to mount to the `/media/data` directory

   d. To mount the devices to the corresponding directories, run the following commands:

   ```
   mount /dev/sda3 /opt/Avaya
   mount /dev/sdb1 /media/data
   ```

   Warning:

   If the volumes are not mounted after the reboot, use any text editor and add the volumes in the `/etc/fstab` file.

Next steps

After a non-root Linux user is created for performing the Avaya Multimedia Messaging installation, the user must become the owner of the `/opt/Avaya` directory.

Creating non-root users

About this task

The Avaya Multimedia Messaging deployment must be made by a non-root Linux user with sudo privileges.

For a clustered deployment of Avaya Multimedia Messaging, the steps described in this procedure must be performed on every node in the cluster.

In an Avaya Multimedia Messaging cluster, the Linux users that perform the installation must have the same user ID (UID), and the groups of users must have the same group ID (GID) on each server.

The following procedure describes how to add users and groups.

Procedure

1. Log in as the root user.
2. Verify the `/etc/passwd` file on each server of the cluster to find a UID that is not currently in use.

   For example, you can set the UID to 1005. To check if the UID is present on a Linux machine, run the following command:

   ```
   grep 1005 /etc/passwd
   ```

3. Verify the `/etc/group` file on each server of the cluster to find a GID that is not currently in use.

   For example: To check if the 1002 GID is present on a Linux machine, run the following command:

   ```
   grep 1002 /etc/group
   ```

4. Create a group.

   For example: To create a group called `ucgrp`, run the following command:

   ```
   /usr/sbin/groupadd -g 1002 ucgrp
   ```

5. Create the non-root user.

   For example: To create a user called `ammapp`, run the following command:

   ```
   /usr/sbin/useradd -u 1005 -g ucgrp ammapp
   ```

6. Create a password for the new user.

   For example: To create a password for the `ammapp` user, type the following command and enter the password:

   ```
   passwd ammapp
   ```

Next steps

- In a clustered deployment, you must grant the new user sudo permissions on every server in the cluster.
- Verify that the user was created successfully with the required permissions

Granting sudo permissions to non-root users

About this task

Non-root users need 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.

Before you begin

Create a group and a non-root user on every Linux server in the cluster.

Procedure

1. Log in as the root user.
2. Open the `/etc/sudoers` file using a text editor.

   For example:

   ```
   vim /etc/sudoers
   ```

   If you use vi or vim, you must press **I** or the **Insert** key to enable editing for the 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` with the name of the new user in the new line.

   For example:

   ```
   #Allow root to run any commands anywhere
   root        ALL=(ALL)        ALL
   ammapp        ALL=(ALL)        ALL
   ```
5. Save the `/etc/sudoers` file and exit the text editor.

   For example:

   If you use vi or vim, you can save and exit by pressing **Esc**, typing `wq`, and pressing **Enter**.
6. (Optional) To verify that the sudo rights have been assigned to the `ammapp` user, perform the following actions:

   a. 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 `ammapp` user.

      If the `ammapp` user has sudo access, the content of the `/etc/shadow` file is displayed in the text console.

Libraries required by the Avaya Multimedia Messaging server

Avaya Multimedia Messaging server requires that you install the following Linux libraries and packages for the Avaya Multimedia Messaging server components:

- `/lib/ld-linux.so.2`, for the Serviceability Agent
- `libgcc.i686`, for granting access to Avaya Services
- `libstdc++.i686`, for granting access to Avaya Services
- `dialog.x86_64`, for the Linux dialog component
- `python-argparse`, for the `cqlsh`, Cassandra command line interface.
- `xfsprogs`, for the XFS file system.

Avaya Multimedia Messaging also requires Open JDK, which is installed automatically when you run the installation process.

Warning:

Before you install the Avaya Multimedia Messaging server, you must also update OpenSSL to the latest version.

Updating OpenSSL is a mandatory security enhancement.

For information about applying package updates from the Red Hat network, follow the instructions at the Red Hat customer portal.

Installing the Linux libraries

About this task

Some components of the Avaya Multimedia Messaging server require the presence of the following Linux libraries and packages to be present on the system prior to the installation:

- `/lib/ld-linux.so.2`, for the Serviceability Agent
- `libgcc.i686`, for granting access to Avaya Services
- `libstdc++.i686`, for granting access to Avaya Services
- `dialog.x86_64`, for the Linux dialog component
- `python-argparse`, for the `cqlsh`, Cassandra command line interface.
- `xfsprogs`, for the XFS file system.

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

Procedure

1. To install the `/lib/ld-linux.so.2` library, run the following command and enter `y` when prompted to confirm the package installation:

```
sudo yum install /lib/ld-linux.so.2
```

2. To install the `libgcc.i686` library, run the following commands and enter `y` when prompted to confirm the package installation:

```
sudo yum install libgcc
sudo yum install libgcc.i686
```

3. To install the `libstdc++.i686` library, run the following commands and enter `y` when prompted to confirm the package installation:

```
sudo yum install libstdc++
sudo yum install libstdc++.i686
```

4. To install the `dialog.x86_64` library, run the following command and enter `y` when prompted to confirm the package installation:

```
sudo yum install dialog.x86_64
```

5. To install the `python-argparse` library, run the following command and enter `y` when prompted to confirm the package installation:

```
sudo yum install python-argparse
```

6. To install the `xfsprogs` library, run the following command and enter `y` when prompted to confirm the package installation:

```
sudo yum install xfsprogs
```

7. To update the `openjdk 1.8` library, run the following command and enter `y` when prompted to confirm the package update:

```
sudo yum update java-1.8.0-openjdk
```

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:

```
sudo 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.

   You must restart your machine for this change to take effect.

Updating the Red Hat Enterprise Linux kernel

About this task

The Red Hat Enterprise Linux kernel version required for the Avaya Multimedia Messaging server is Red Hat kernel version 2.6.32-220.13.1 or greater.

This procedures describes how to update the Linux kernel on your system before you perform the Avaya Multimedia Messaging server installation.

Procedure

1. Check the current version of the Linux kernel used by your system.

   For example:

   ```
   sudo uname —a
   Linux ott-253-18.sc.sc 2.6.32-220.el6.x86_64 #1 SMP Wed Nov 9 08:03:13 EST 2011
   x86_64 x86_64 x86_64 GNU/Linux
   ```

2. Download the required files from the Red hat website by performing the following steps.

   You must download the latest versions of two .rpm files: the kernel file and the firmware file. For example:

   ```
   kernel-2.6.32-220.13.1.el6.x86_64.rpm
   kernel-firmware-2.6.32-220.13.1.el6.noarch.rpm
   ```

   a. Log in to the Red hat website with your account.

   b. In the **Software & Download Center** section, select **Packages**.

   c. Enter the name of the package in the **Search For** field.

      For example: `kernel-2.6.32-220.13.1.el6.x86_64.rpm`

   d. In the **Where to search** field, select **In the following architectures** and **x86_64**.

   e. In the result list, click the Linux kernel package to view information about the package.

   f. In the Download section, click **Download Package**.

3. Run the following command to install the latest kernel and firmware versions:

   ```
   sudo yum install kernel-2.6.32-220.13.1.el6.x86_64.rpm kernel-
   firmware-2.6.32-220.13.1.el6.noarch.rpm
   ```

4. Reboot the server by using the following command:

   ```
   sudo shutdown -r now
   ```

5. Log in as the `ammapp` user and verify the new kernel version.

   ```
   sudo uname -r
   ```

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. Open the hosts file using a text editor.

   For example:

   ```
   sudo vim /etc/hosts
   ```

2. 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.

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

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

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

Procedure

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

   For example:

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

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

   For example:

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

   Note:

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

3. Save the `/etc/ntp.conf` file and start the NTP server.

   ```
   sudo service ntpd start
   ```

4. Configure the NTP daemon to start when the Avaya Multimedia Messaging server boots.

   ```
   sudo chkconfig ntpd on
   ```

5. (Optional) To verify if the NTP daemon is started, use the following command:

```
sudo service ntpd status
```

6. Check the accuracy of the local clock by using the **ntpdate** command.

   For example:

```
sudo ntpdate -qu ntpserver.example.com
```

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. Open the SSH configuration file using a text editor.

   For example:

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

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

```
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.

3. 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.

4. Save the configuration file and reload the sshd service using one of the following commands:
   - `sudo service sshd restart`
   - `sudo /etc/init.d/sshd restart`

Installing the Avaya Multimedia Messaging server

About this task

This task describes how to install the Avaya Multimedia Messaging server using the binary file provided for the installation.

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

The directory where the binary file is located on the server is referred to as `<ammbinary_dir>`. `<ammbinary_dir>` is the download directory of the Avaya Multimedia Messaging binary file.

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 Prerequisites checklist on page 38 are met.
- To run the commands in this procedure, you must log in as the ammapp 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 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. Make the Avaya Multimedia Messaging installer executable using the following command:

   For example:

```
sudo chmod 755 <ammbinary_dir>/amm-<version_number>.bin
```

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

   ```
   sudo <ammbinary_dir>/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.

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

   ```
   sudo <ammbinary_dir>/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.

5. 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 53.

6. Select **Continue** and press Enter.

Next steps

The next menu displayed after the initial installation phase is the configuration menu.

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

For information about using the configuration menu, see Configuring the Avaya Multimedia Messaging server using the configuration utility on page 83.

Installation on a VMware virtual machine

To install the Avaya Multimedia Messaging server on a VMware virtual machine using the Avaya Multimedia Messaging OVA file, you must perform the following actions:

- Download the Avaya Multimedia Messaging R3.0.0.0 OVA file from PLDS.
- Deploy the OVA file to a vCenter-managed, or standalone, ESXi host.
- Modify machine capabilities such as disk space, memory or CPU if necessary.
- Copy the R3.0.0.1 version of the Avaya Multimedia Messaging installation file to the `/opt/Avaya` directory, and run it with the “--initOVA” parameter.
- Perform the additional configurations that are required.

Note:

The configurations and the administration tasks described in this document apply to the Avaya Multimedia Messaging deployments from OVA images, as well as deployments made on physical servers.

The Avaya Multimedia Messaging OVA file includes openjdk. Operating system updates for virtual machines include updates for openjdk.

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 R3.0.0.0 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 configuration values for the virtual machine and then click **Next**.
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 16.
12. Update the virtual machine's virtual hardware as required.
    - For memory adjustments required from step 11 on page 51, see Adjusting the memory resource of a virtual machine on page 191.
    - For CPU adjustments required from step 11 on page 51, see Adjusting the CPU resource of a virtual machine on page 191.
    - Update the size of the application disk to 204 GB, and the size of the media disk to the storage reservation determined in step 11 on page 51, see Adjusting the size of virtual disks on page 192.
13. Start the virtual machine.

Next steps

Install the application software.

- To perform a standard, interactive installation, see Installing the Avaya Multimedia Messaging server on a VMware virtual machine on page 52.
- To perform a silent installation, see Performing a silent installation on page 59.

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 R3.0.0.0 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 50 to 5 on page 50.
3. On the Name and location page, enter a name for the virtual machine and then click **Next**.
4. Perform steps 7 on page 50 and 8 on page 50.
5. Review the summary and then click **Finish**.
6. Perform steps 11 on page 51 and 12 on page 51.
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 configuration values for this virtual machine.
12. Review the summary and then enter `y` to continue.

Next steps

Install the application software.

- To perform a standard, interactive installation, see Installing the Avaya Multimedia Messaging server on a VMware virtual machine on page 52.
- To perform a silent installation, see Performing a silent installation on page 59.

Installing the Avaya Multimedia Messaging server on a VMware virtual machine

About this task

This task describes how to install the Avaya Multimedia Messaging server using the binary file provided for the installation.

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

The directory where the binary file is located on the server is `/opt/Avaya`.

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

Important:

Log in as the ammapp non-root user to perform the installation and any other configuration or administration tasks.

Before you begin

If you are installing the Avaya Multimedia Messaging server on a VMware virtual machine, you must first deploy the OVA using one of the deployment options described in Deployment options on page 50.

NTP must be enabled and synchronized between Avaya Multimedia Messaging nodes.

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. Download the R3.0.0.1 version of the Avaya Multimedia Messaging installation file from PLDS to the home directory of the administrative user.
2. Verify the integrity of the file by performing the following actions:
   a. Run the `sha256sum` command on the `amm-<version_number>.bin` file:

      ```
      /usr/bin/sha256sum 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.

When the hashes match exactly, the downloaded file is almost certainly intact. If the hashes do not match, there was a problem with the download or with the server and you must download the file again.

3. Move the file to the `/opt/Avaya` directory and make it executable.

```
Sudo mv amm-<version_number>.bin /opt/Avaya
Sudo chmod 750 /opt/Avaya amm-<version_number>.bin
```

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

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

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.

5. Provide the configuration details listed in the Initial Installation Configuration menu.
6. Select **Continue** and press `Enter`.

Next steps

To perform an initial installation configuration, see Avaya Multimedia Messaging initial installation configuration on page 53.

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. For information about using the configuration menu, see Configuring the Avaya Multimedia Messaging server using the configuration utility on page 83.

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.	`REST_FRONTEND_HOST`

Table continues…

Item name	Description	Equivalent properties file parameter
	The front-end FQDN is the address that end-user clients use to access the services provided by Avaya Multimedia Messaging . The default value for this field 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 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 the default port 8443. 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**.	`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
	Note: If this parameter is changed after the installation, all of the nodes in a cluster must be restarted to apply the change. The command is AMMService restart.	
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. The Avaya Multimedia Messaging configuration utility uses this value to generate certificates for the node. **Important:** In a clustered configuration, the Local frontend host is different from one node to the other and is also different from the Front-end FQDN.	`LOCAL_FRONTEND_HOST`
Keystore password	The keystore password for the MSS and Tomcat Avaya Multimedia Messaging certificates.	`KEYSTORE_PW`

Table continues…

Item name	Description	Equivalent properties file parameter
	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 (.)	

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
Installation Directory	The installation directory for the Avaya Multimedia Messaging server. The Linux user who performs the installation must have access to the GlusterFS directory. The default value for this setting is `/opt/Avaya`.	`INSTALL_PARENT`
Directory for the database files	The path to the directory for storing the Cassandra Database files. This path is relative to the Avaya Multimedia Messaging installation directory. This directory can be a mount point, for remotely mounted storage systems.	`CASS_DATA_DIR`

Table continues…

Item name	Description	Equivalent properties file parameter
	The default value for this setting is `/opt/Avaya`.	
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 `/opt/Avaya`.	`GLUSTER_BRICK_DIR`
Configure Gluster (no for multi-node restores)	For Avaya Multimedia Messaging systems that contain one or two nodes, the GlusterFS configuration is automatic. Select `y` (yes) to enable the automatic configuration of GlusterFS or `n` (no) to disable automatic configuration. The default value for this setting is `y` (yes). This setting must be set to `y` (yes), unless you are performing a restore. See Backup and restore on page 209 for more information.	`GLUSTER_AUTO_CONFIG`
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	`RUN_FIREWALL_CONFIG`

Table continues…

Item name	Description	Equivalent properties file parameter
	configuration of the next nodes of the cluster might be incorrect. The default value for this setting is `y` (yes).	
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. The default value for this setting is `y` (yes).	`CLEAR_DB_AT_INSTALL`
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`

After you finish the initial installation configuration, you must extend the size of disk volumes as described in Extending disk volumes on page 60.

Performing a silent installation

About this task

The following 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 and contains the same settings that you can configure during the interactive installation, grouped after the 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 separately, 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 Configuration chapter of this document.

   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 application, run the following command:

```
service AMMService start
```

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

Next steps

Extend the size of disk volumes as described in Extending disk volumes on page 60.

Extending disk volumes

About this task

The deployment of the Avaya Multimedia Messaging OVA enables you to increase the size of the application and media virtual disks. This procedure extends the sizes of volumes on those disks to make use of the allocated space.

Procedure

Increase the size of the `/opt/Avaya` and `/media/data` volumes to utilize the remaining space on their respective host disks.

For more information, see Adjusting disk volumes using core Linux commands on page 195.

Enhanced Access Security Gateway support for Avaya Multimedia Messaging

Enabling and disabling the Enhanced Access Security Gateway

About this task

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

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

Procedure

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

   ```
   EASGStatus
   ```

   By default, the EASG status is disabled.
3. To enable EASG, do the following:
   a. In the SSH console, run the following command:

      ```
      sudo /usr/sbin/EASGManage --enableEASG
      ```

   b. Run the following command to verify the product certificate:

      ```
      sudo EASGProductCert --certInfo
      ```

      The system displays the product certificate details.

      For example:

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

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

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

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

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

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

4. To disable EASG, run the following command:

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

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

About this task

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

Procedure

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

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

The system installs the EASG `.rpm` file and creates the `susers` group if it is unavailable. It also adds the users to the `susers` and `ucgrp` groups.

3. Check the EASG status by running the following command:

```
EASGStatus
```

By default, the EASG status is disabled.

4. To enable EASG, run the following command:

```
sudo /usr/sbin/EASGManage --enableEASG
```

5. To verify the product certificate, run the following command:

```
sudo EASGProductCert --certInfo
```

The system displays the product certificate details.

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

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

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

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

Using keyboard-interactive authentication.


Challenge: 10005-37279073              Product ID: 3548b37a63d84ecf8ee4c6ae5cce8
df001

Response:
```

7. To complete the Pluggable Authentication Module (PAM) settings for user authentication, do the following:

   a. In the PAM file stack, add `auth [success=done auth_err=bad default=ignore] pam_asg.so` so that it appears before `pam_unix.so`.

   b. In the password stack, add `password sufficient pam_asg.so` so that it appears in the first line.

   The following is an example of the PAM settings:

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

account required pam_access.so

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

session required pam_limits.so
```

Removing EASG

About this task

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

Procedure

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

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

Related links

Installing and enabling the Enhanced Access Security Gateway on a physical server on page 62

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:

To achieve redundancy, you must install an Avaya Multimedia Messaging cluster of more than one nodes and configure 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. Also, 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

The prerequisites for installing an Avaya Multimedia Messaging cluster are the same as for installing an individual Avaya Multimedia Messaging server. For information about prerequisite configuration, see the section about Prerequisites checklist on page 38.

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.

For information about installing the initial node, see Installing the seed node on page 67.

2. Install one or more additional nodes.

   For information about installing an additional node, see Installing an additional node on page 69.

   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:

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

   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 Lync federation, use the configuration utility to add the Lync certificate to the trust store of each node.

   For more information, see Importing the Lync front-end server certificate into the trust store on page 109.

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:

   ```
   service AMMService 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:

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

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.

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.

For information about the Avaya Multimedia Messaging configuration settings, see Installing the Avaya Multimedia Messaging server on page 48 and the sections under Configuring the Avaya Multimedia Messaging server using the configuration utility on page 83.

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 page 48.

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.

   For more information about the LDAP configuration, see LDAP configuration on page 87.

   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.

   For information about the LDAP configuration settings, see Importing the LDAPS certificate using the configuration utility on page 114 and LDAP configuration on page 87.

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.

   For information about virtual IP configuration values, see Virtual IP configuration fields on page 71.

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

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.

For information about the Avaya Multimedia Messaging configuration settings, see Installing the Avaya Multimedia Messaging server on page 48 and the sections under Configuring the Avaya Multimedia Messaging server using the configuration utility on page 83.

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 73.

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 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 **Clustering Configuration** > **Cluster configuration** > **Cassandra Encryption Configuration** 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 fields on page 71.

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 73.

Virtual IP configuration fields

Enter the following virtual IP configuration values:

Option	Description
Virtual IP address	The virtual IP address shared by all the cluster nodes.
Virtual IP interface	The 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.
Virtual IP master node	The setting to determine if the current node is the virtual IP master node. For the current node, set this value to `n` (no).
Virtual IP router ID	This field is an integer with a value from 1 to 255 and it 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 and it is limited to cluster deployments.
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 seed node.

Creating and expanding a Gluster file system

About this task

This procedure describes how to:

- Build a new Gluster file system.
- 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`. This location is the same for building and expanding a Gluster file system.

Tip:

- When building a Gluster file system, all nodes should have the same disk size.
- When adding nodes, do not use machines with disk sizes that are smaller than the ones in the existing nodes.

Procedure

1. If you are building a new Gluster file system, delete the following existing empty non-clustered file systems on the seed node:
   - `sudo gluster volume stop cs_volume`
   - `sudo gluster volume delete cs_volume`
   - `sudo rm -rf /media/data/content_store/brick*`
2. Run one of the following commands:
   - To build a new Gluster file system: `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.
   - To add a new node to an existing Gluster file system: `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.
3. 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.

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
   ```

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, as described in Upgrading the Avaya Multimedia Messaging server on page 242.
2. To install the new node on VMware, 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 69.
3. To install a new node on a physical server, download the latest Avaya Multimedia Messaging binary and install as described in Installing an additional node on page 69.

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.

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

   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.

   ```
   service AMMService 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.

   For information about installing a cluster node, see Installing an additional node on page 69.
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.

   ```
   sudo service AMMService restart
   ```

5. Restart the Avaya Multimedia Messaging service on the other cluster nodes.

   ```
   sudo service AMMService restart
   ```

Next steps

- Disable the virtual IP on the old seed node.
- Configure the new node to be the virtual IP Master node. For details, see Installing the initial cluster node on page 67.
- If you must decommission the former seed node, see Removing a non-seed cluster node on page 76.

Removing a node from the Avaya Multimedia Messaging cluster

About this task

The following procedure describes how to remove a node from an Avaya Multimedia Messaging cluster by providing an example for a three-node cluster.

Important:

If the node that you are removing is the virtual IP master or backup node, you must first configure another node to take the virtual IP function of the node to be removed.

The remove-node operation is done in two phases:

- The first phase consists of scanning the files on the bricks to be removed and requires approximately one hour per TB.
- The second phase consists of moving the files from one of the bricks (not both) onto the remaining nodes and requires approximately 32 hours per TB.

The transition from two servers (two bricks) to one server (one brick) does not require the second phase, because file copying is not required. It just reduces the replication factor.

Note:

Replacing a nonfunctional server with another server requires approximately 7 hours per TB to copy data from the replica. For more information, see Restoring Gluster after a Gluster brick is properly removed on page 216.

Before you begin

If you want to uninstall the Avaya Multimedia Messaging cluster and not just one node, perform a backup of the media files and then delete the files.

Warning:

Removing the Gluster bricks for all the servers can require a large amount of time, up to a few days.

Important:

Do not go through the process of removing the Gluster bricks as described in this section, if you want to remove the Avaya Multimedia Messaging cluster completely. To decommission a node from the Avaya Multimedia Messaging cluster, ensure that you back up the files on the Gluster bricks associated with the node and assign the virtual IP function of the note to another node of the cluster.

Procedure

1. Perform the following actions to move the replicated data from the Gluster File System of the node to the remaining nodes in the cluster:

   a. In the CLI of the Avaya Multimedia Messaging node to be removed, type the following command:

   ```
   sudo gluster volume info cs_volume
   ```

   This command lists the details of the volume configuration.

   The system displays the bricks in the volume and their paths, in the order in which the bricks are paired for replication. On a three-node cluster, the system displays three brick pairs.

   For example:

   ```
   Brick1: 1.2.3.10:/media/data/content_store/brick0
   Brick2: 1.2.3.20:/media/data/content_store/brick0
   Brick3: 1.2.3.20:/media/data/content_store/brick1
   Brick4: 1.2.3.30:/media/data/content_store/brick0
   Brick5: 1.2.3.10:/media/data/content_store/brick1
   Brick6: 1.2.3.30:/media/data/content_store/brick1
   ```

   The bricks are paired for replication as follows: Brick1/Brick2, Brick3/Brick4, Brick5/Brick6.

   b. Identify the brick pairs that include the node to be removed.

   For example:

   The brick pairs to remove for the third node are Brick3/Brick4 and Brick5/Brick6.

   c. (Optional) Measure the amount of data that is present on a brick by running the following command:

   ```
   du -sh
   ```

   The command may require several minutes to complete.

   d. For each brick in the pair that you must remove, type the following command:

   ```
   sudo gluster volume remove-brick <Volume Name> ip1:/media/data/content_store/
   brick2 ip2:/media/data/content_store/brick0 start
   ```

Important:

The remove-node operation uses 5% of the CPU and is designed to function while the traffic continues. and so the re-balance of the content is paced very slowly. There is no option to increase the speed of this operation.

For example:

```
sudo gluster volume remove-brick cs_volume 1.2.3.4:/media/data/content_store/
brick2 1.2.3.5:/media/data/content_store/brick0 status
```

Important:

If you are removing a node from a two-node cluster, you must also disable replication.

To disable replication while removing the brick pair, run the command as follows:

```
sudo gluster volume remove-brick cs_volume replica 1 <BrickNumber ip1:/
path>  <BrickNumber ip2:/path>  start
```

e. Run the following command to verify the progress of the brick removal:

```
sudo gluster volume remove-brick <Volume Name> ip1:/media/data/content_store/
brick2 ip2:/media/data/content_store/brick0  status
```

When the status output does not display any *in progress* lines, the removal of the bricks is complete.

f. Commit the removal of the bricks by running the following command:

```
sudo gluster volume remove-brick <Volume Name> ip1:/media/data/content_store/
brick2 ip2:/media/data/content_store/brick0  commit
```

g. Repeat *Steps c, d, and e* for any remaining bricks that contain the node that you are removing.

In the example provided for a three-node cluster, you must also remove the pair Brick3/Brick4, because Brick4 is linked to the IP address of the third node.

h. In the CLI of a node that is currently in the cluster, type the following command:

```
sudo gluster peer detach <ip of node being removed> force
```

For example:

```
sudo gluster peer detach 1.2.3.30 force
```

i. Identify the brick directories that are not used and remove the directories.

On each node in the cluster, run the following command:

```
/opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/glusterfs/
configGluster.sh -v
```

Run the **`rm -r`** command to remove the directories listed by the **`configGluster`** command.

j. On the node being removed, unmount the Gluster content mount point.

For example:

```
sudo umount /opt/Avaya/MultimediaMessaging/<version>/content_mount
```

2. Run the Avaya Multimedia Messaging uninstall script.

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

   When the system prompts you to confirm that you want to uninstall the Avaya Multimedia Messaging server, type `uninstall` and press Enter.

   When the system prompts you to confirm if you want to preserve the database, type `no` and press Enter.

3. If the Avaya Multimedia Messaging server is deployed on a VMware virtual machine, remove the virtual machine from the VMware vSphere client.

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 restoring the previous version, see Restoring a previous version of the Avaya Multimedia Messaging server on page 244.

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 76.

Procedure

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

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

Patch setup

This section describes how to extract, install, and remove a patch from the inventory.

Avaya Multimedia Messaging patches are delivered as tarballs (`.tgz`) files. You can install a patch after it is added to the build inventory.

Patch limitations are described in “Caveats and limitations” in *Avaya Multimedia Messaging Reference Configuration*.

Adding a patch to the inventory

About this task

Use this procedure to extract a patch and add it to the inventory of the running build. This procedure does not install the patch, but just makes it available for installation.

If a patch is in the inventory but not installed, use this procedure to replace the existing patch in the inventory. If the patch is installed or partially installed, use this procedure to replace the implementation login of the existing patch, so the artifacts that were saved during the patch installation are retained so the patch can be uninstalled later.

Procedure

1. In the SSH console, run the following command:

   ```
   tar -zxf amm-<version>-patch-1.tgz
   cd amm-<version>-patch-1
   sudo ./patch.sh --add
   ```

   The system extracts and adds a patch.

2. **(Optional)** To delete the tarball file and the extracted directory after adding the patch, run the following command:

   ```
   cd ..
   rm -f amm-<version>-patch-1.tgz
   rm -rf amm-<version>-patch-1
   ```

   Tip:

   Keep the tarball file if you need to re-add it to the inventory later.

Querying patch status

About this task

Use this procedure to query the current patch level of the running build and the list of existing patches in the inventory.

Procedure

1. In the SSH console, run the following command:

   ```
   sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/patches2/patchmgt.sh --query
   ```

2. **(Optional)** To get additional information on managing existing patches, run the following command:

   ```
   sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/patches2/patchmgt.sh --hhelp
   ```

Installing a patch

Before you begin

Close Avaya Multimedia Messaging.

Procedure

In the SSH console, run the following command:

```
sudo service AMMService stop
sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/patches2/patchmgt.sh --install
sudo service AMMService start
```

Uninstalling and removing a patch from the inventory

About this task

You can remove a patch if it is already uninstalled from the inventory.

Procedure

1. **(Optional)** To uninstall a patch, run the following command:

   ```
   sudo service AMMService stop
   sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/patches2/patchmgt.sh --
   uninstall
   sudo service AMMService start
   ```

2. **(Optional)** To remove an uninstalled patch from the inventory, run the following command:

   ```
   sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/patches2/patchmgt.sh --
   remove 1
   ```

   The number in `remove 1` indicates the patch number that you are removing.

   The system compresses the removed patch logs and stores them in the following file format: `sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/patches2/patchmgt.sh --logs`.

Chapter 6: Configuration

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

You can perform some configuration procedures using the configuration utility, others by using the administration portal. For example, Configuring the messaging domains using the administration portal on page 113.

Table 6: Summary of installation tasks

Task	Physical server deployment		OVA deployment on a virtual machine	
	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.

Table continues…

Task	Physical server deployment		OVA deployment on a virtual machine	
	Single server	Cluster	Single server	Cluster
Federation configuration	If federation is required			
Multisite configuration	If multisite federation is required.			
Configure LDAP synchronization with System Manager Customize login screen for the message playback component Install the AFS authentication file	Y	Y Repeat for every node in the cluster.	Y	Y Repeat for every node in the cluster.
Remote access configuration	Y	Y	Y	Y
Enhanced Access Security Gateway configuration	Y	Y	Y	Y

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.

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

   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 the **CORS Configuration** and **Serviceability Agent Configuration** field 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:

```
service AMMService 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.

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 for this field 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 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 the default port 8443. Select `y` (yes) to configure the port for the reverse proxy server or `n` (no) to keep the default configuration that remains disabled.	`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
	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 to apply the change. The command is AMMService restart.	
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. The Avaya Multimedia Messaging configuration utility uses this value to generate certificates for the node. **Important:** In a clustered configuration, the Local frontend host is different from one node to the other and is also different from the Front-end FQDN.	`LOCAL_FRONTEND_HOST`

Table continues…

Item name	Description	Equivalent properties file parameter
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`

LDAP configuration

Warning:

Changing the LDAP configuration parameters, other than *Bind DN* and *Bind Credential*, once 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. Also, changing the server URL must only be done 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.	pathToLdapPropertiesFile

Table continues…

Item name	Description	Equivalent properties file parameter
	The default value for this setting is `<install_dir>/config/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 and 2012 • IBM Domino Server 7.0 • Novell e-directory 8.8 • OpenLDAP 2.4	ldapType

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.
		ldapUrl

Table continues…

Item name	Description	Equivalent properties file parameter
	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.	
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

Table continues…

Item name	Description	Equivalent properties file parameter
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: If the Administrator role is configured as `AMMAdmin,AMMxyz`, any user whose list of roles contains `AMMAdmin` or `AMMxyz` is mapped to the Avaya Multimedia Messaging ADMIN 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. **Important:** To avoid situations when potential loss of credentials could impact the administration tasks, Avaya recommends creating more than one	adminRole

Table continues…

Item name	Description	Equivalent properties file parameter
	user account with administrator privileges.	
Auditor Role	The list of LDAP roles that match the Avaya Multimedia Messaging Auditor role. 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 for the mapping of the LDAP roles to the Avaya Multimedia Messaging application roles to succeed.	auditorRole
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	serviceAdminRole

Table continues…

Item name	Description	Equivalent properties file parameter
	of roles contains the `AAMMUser` or `AMMxyz` role is mapped to the Avaya Multimedia Messaging Services 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 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, admin, or auditor • Validates the values for Role Attribute ID and Role Name Attribute	testUser

Table continues…

Item name	Description	Equivalent properties file parameter
	• Verifies the Last Updated Time attribute, role filter syntax, and active users search filter syntax The configuration is not saved if any of these validations fail. The testUser parameter is optional. If you do not specify a value in the testUser field, 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.	`rolesCtxDN`

Table continues…

Item name	Description	Equivalent properties file parameter
	For example: `ou=ammsusers,dc=example,dc=com`	
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	`roleRecursion`

Table continues…

Item name	Description	Equivalent properties file parameter
	For example: the user jsmith can be in the Sales group, which can be in the AMM users group. In this case, *Role Recursion* must be set to 2true to permit role recursion.	
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 string	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 that contains the last time when 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 traffic between the Avaya Multimedia Messaging server	`lastUpdatedTimeAttr`

Table continues…

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

Messaging domains configuration

Table 10: 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`

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 11: 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`

Table continues…

Item name	Description	Equivalent properties file parameter
New Cassandra Database Password	The new password for gaining access to the Cassandra database server.	`NEW_CASSANDRA_PW`

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

Cluster Configuration

Table 12: 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`
Gluster Trusted Node Peer Configuration	The setting to add a new node to the existing cluster. This setting is only required starting with the second node, if the cluster contains more than two nodes.	This setting does not have an equivalent parameter in the installation.properties file. You must configure the GlusterFS server using the configuration tool after the silent installation is complete.

Cluster utilities

Table 13: Cluster Utilities

Item name	Description	Equivalent properties file parameter
Utility to configure Gluster bricks on 2 or more nodes	The *Utility to configure Gluster bricks on 2 or more nodes* configures the Gluster File System for replicated media storage. For the seed node, Gluster configuration is performed automatically during the installation. For all the additional nodes, you must run this script during the installation of the Avaya Multimedia Messaging server on the nodes.	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.
Utility to configure Openfire for cluster operation	The *Utility to configure Openfire for cluster operation* utility configures a cluster of Openfire servers. You must run this utility on every Avaya Multimedia Messaging server 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.
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.

Virtual IP Configuration

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 14: Virtual IP 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	`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
	• 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 authentication password: the password to use for virtual IP authentication.	

Advanced configuration

Table 15: 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 GUI or using an SSH console.	`SECURITY_BANNER_PATH`

Configuring the Avaya Multimedia Messaging server firewall

About this task

The following task describes the procedure to configure the firewall after the Avaya Multimedia Messaging installation.

Warning:

The firewall configuration utility replaces the current firewall configuration with the configuration required by the Avaya Multimedia Messaging server. The utility erases the previous firewall configuration, so you must enable any additional ports that your server might require manually after every run of the configuration utility.

Procedure

1. Run the configuration utility.

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

2. Select **OS Security Tools** > **Run the firewall configuration script**.

   The firewall is configured automatically, without requiring any input.

3. **(Optional)** Add new ports to the firewall configuration.

   For example:

```
sudo iptables -I INPUT 6 -p tcp -m tcp --dport 7010 -j ACCEPT
```

   For more information about firewall configuration, see section *7.3. Firewall configuration* in the Red hat customer portal.

4. Check the iptables status to verify that the ports were added successfully.

   For example:

```
sudo iptables --list
sudo service iptables status
```

Configuring the Avaya Multimedia Messaging server From Forking

Procedure

1. Run the configuration utility.

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

2. Click **Form 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.

Avaya Multimedia Messaging certificate management

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

- Using Avaya Multimedia Messaging for certificate management.
- Importing local or public certificates.
- Importing local certificates that are signed by an intermediate Certificate Authority.

You can also view the details for a certificate.

Certificate management is performed during the installation of the Avaya Multimedia Messaging server and there are no additional steps required after the installation is complete. The following

sections illustrate the steps to perform for every certificate management option. After you import a certificate, you must restart Avaya Multimedia Messaging for the changes to take effect.

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 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.
- 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.
- The Lync certficate is used for communication with a Lync front-end server. This is only needed if the Avaya Multimedia Messaging is interoperating with Lync.

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.

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

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** option.

   The System Manager enrollment password is 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.

Importing local 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.

Procedure

1. Run the Avaya Multimedia Messaging configuration utility.

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

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

   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 certificate file under **Advanced Configuration** > **Import Microsoft Lync trusted certificate**.
8. Configure the **MSS/Tomcat keystore password** option.

   The MSS/Tomcat keystore 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.

Importing intermediate CA certificates

About this task

In some deployments where certificates are imported rather than generated by Avaya Aura® System Manager, server certificates are signed by an intermediate Certificate Authority (CA) rather than a root CA. To use the certificates, a chain of trust is required: the root CA signs the intermediate CA certificate and the intermediate CA signs the server certificate.

To create a certificate chain, you must concatenate the PEM-format certificate files for the server and the intermediate CA, so that the server certificate is first.

Important:

Only the REST and OAM front-end certificates support intermediate Certificate Authorities. The node and back-end certificates do not support intermediate CAs and importing certificate chains for those certificates fails.

The following procedure describes how to concatenate the PEM-format certificate files and import the files using the configuration utility.

Procedure

1. Copy the server certificate file to a new file for concatenation.

   For example:

   ```
   cp server.crt certificate-chain.crt
   ```

2. Concatenate the intermediate certificate file to the file created in the previous step.

   For example:

   ```
   cat intermediateca.crt >> certificate-chain.crt
   ```

3. Run the Avaya Multimedia Messaging configuration utility.

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

4. Select **Front-end host, System Manager and Certificate Configuration**.
5. 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).
6. 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.
7. Set **Use System Manager** to `n` (no).

   The menu displays options for importing individual certificate files.

8. Select one of the following options to provide the path to the concatenated certificate file:
   - **REST interface certificate file**
   - **OAM interface certificate file**
9. Import the key file of the certificate by using the corresponding menu option:
   - **REST interface key file**
   - **OAM interface key file**

   The key file does not require alteration. Import the key file as if you are importing individual certificates.
10. Import the Lync certificate file using **Advanced Configuration** > **Import Microsoft Lync trusted certificate**.
11. Configure the **MSS/Tomcat keystore password** option.

    The MSS/Tomcat keystore 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.
12. Restart Avaya Multimedia Messaging and check the configuration utility log files to ensure that the certificates were imported successfully.

Default Lync 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 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 server to each node.

Getting the certificate from the Certificate Authority

About this task

You can obtain the certificate for communicating with the Lync 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 server to the node

About this task

You can obtain the certificate for communicating with the Lync servers using one of two methods.This procedure describes the second method, which involves copying the certificate from the Lync 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 front-end server, and the certificate for Session Manager from the Lync Edge server.

Procedure

1. Use Remote Desktop to connect to the Lync 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.

    (Optional) To check the location for the saved certificate, click **Browse**.
12. Click **Next** and then click **Finish**.

Importing the Lync front-end server certificate into the trust store

Before you begin

Obtain the certificate. For more information, see Methods for obtaining the certificate on page 108.

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 certificate and select **OK**.

The file must be in `per` or `der` format.

5. Select **Apply**.

Adding the Lync certificate to the MSS trust store on each node

Procedure

1. In System Manager, create a keystore that contains the subject-alternative-name (SAN) of the cluster FQDN and each of the local FQDNs.

   Use this as the Mobicents Sip Servlets (MSS) keystore.

2. Back up the Lync certificate in your browser.
3. Install the certificate.

Creating a keystore with subject-alternative-name format

Procedure

1. In System Manager, navigate to **Services** > **Security** > **Certificates** > **Authority**.
2. If this is your first time creating a certificate for any cluster, perform the following:
   a. Click **Edit End Entity Profiles**.
   b. Select the **INBOUND_OUTBOUND_TLS** profile.
   c. Scroll down to the Subject Alternative Name Fields section and select **DNS Name**.

      DNS Name is the FQDN of the DNS server.

   d. Add a field for the cluster FQDN.
   e. Add a field for each of the local FQDNs.
   f. Click **Save**.
3. Do one of the following to create or edit an entity:
   - If this is your first time creating a certificate for this Avaya Multimedia Messaging cluster, click **Add End Entity**.
   - To edit information for this Avaya Multimedia Messaging cluster, click **List/Edit End Entities**, find the appropriate entity, and edit it.
4. Complete the following fields for the entity:
   - Click **List/Edit End Entities**.
   - To edit information for your Avaya Multimedia Messaging cluster, click **Edit End Entity**, find the appropriate entity, and edit it.

   a. Enter the cluster FQDN as the **Common Name** and the first **DNS Name**.

      Note:

      For consistency and ease of sharing, use the short cluster name as the username and 123456 as the password.

   b. Enter the local FQDNs in the other **DNS Name** fields.

   c. Set the status to **New**.
   d. Click **Save**.
5. Select **Security** > **Public Web** and click **Create Keystore**.
6. Enter the username and password you set earlier in this procedure.
7. Set **Key Length** to `2048` and click **OK**.

   A new keystore in p12 format is created.
8. Save the keystore locally.

Next steps

Install the certificate.

Note:

You might receive an alert saying `If you see this alert message, you must back up the certificate from a browser to save it to a file on your disk before installing.`

Backing up a certificate from your browser

About this task

This procedure provides general guidelines for viewing and backing up a certificate. The exact process for accessing certificates varies depending on the browser you are using.

Procedure

1. View the certificates in your browser.

   The exact process varies depending on the browser you are using.
2. In the Certificate Manager window, select your saved certificate and click **Backup**.
3. In the Choose a Certificate Backup Password window, enter your password and then click **OK**.
4. Save the file locally.

Next steps

Install the certificate.

Installing the Lync certificate to the Avaya Multimedia Messaging cluster

Procedure

1. Start the Java keytool application.
2. To convert the keystore file from p12 to jks, enter the following commands:

```
-importkeystore
-deststorepass <password>
-destkeystore choose_new_file_name.jks
-srckeystore file_created_by_SMGR.p12
-srcstoretype PKCS12
-srcstorepass 123456
```

`password` is the keystore password used in the installation of Avaya Multimedia Messaging.

123456 is the password used when creating the file on System Manager.

The `keystore_file.p12` file with password `123456` is converted to `keystore_file.jks` with password `password`.

3. To verify the contents of the keystore, enter the following command:

```
keytool -list -v -keystore keystore_file.jks -storepass <password>
```

4. Open the keystore_file.jks and note the Alias name.

   Note:

   The name can be the cluster FQDN.

5. To set the key password to be the same as the storepass, enter the following command:

```
keytool -keypasswd -alias keystore_file.example.com -keystore keystore_file.jks -
keypass 123456 -new password
```

6. Enter the new password when prompted.
7. Copy the `mss-ssl-ks.jks` file to all the servers in the Avaya Multimedia Messaging cluster.

   Important:

   Make sure that the file is readable by the non-root user used to install Avaya Multimedia Messaging.

8. Restart the MSS.

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, such as XMPP, 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 25.

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. In the Avaya Multimedia Messaging GUI, run the configuration utility.

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

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**.

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.

Importing the Secure LDAP certificate using the configuration utility

About this task

Using a Secured LDAP server requires adding a CA trust certificate file to the Tomcat trust store.

The following procedure describes how to import the certificate using the configuration utility.

Before you begin

The Avaya Multimedia Messaging configuration utility can import certificate files in the .PEM format only.

If the certificate file has 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
```

Procedure

1. Run the configuration utility.

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

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 filename 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-based administration portal

About this task

The following procedure describes how to import a Secure LDAP certificate, in the case when Secure LDAP is used.

Before you begin

The Avaya Multimedia Messaging server must be installed and configured before you can gain access to the web-based 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 **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.
3. Select the **Secure LDAP** check box.
4. Click **Import Certificate** to import the certificate file from the location where it is stored on the hard disk.
5. Click **Save**.

LDAP configuration for Microsoft Active Directory

The following sections contain tasks for configuring the LDAP server for Microsoft Active Directory (AD).

The tasks follow the LDAP configuration example provided in this section, to provide a comprehensive view of how the LDAP configuration must be made.

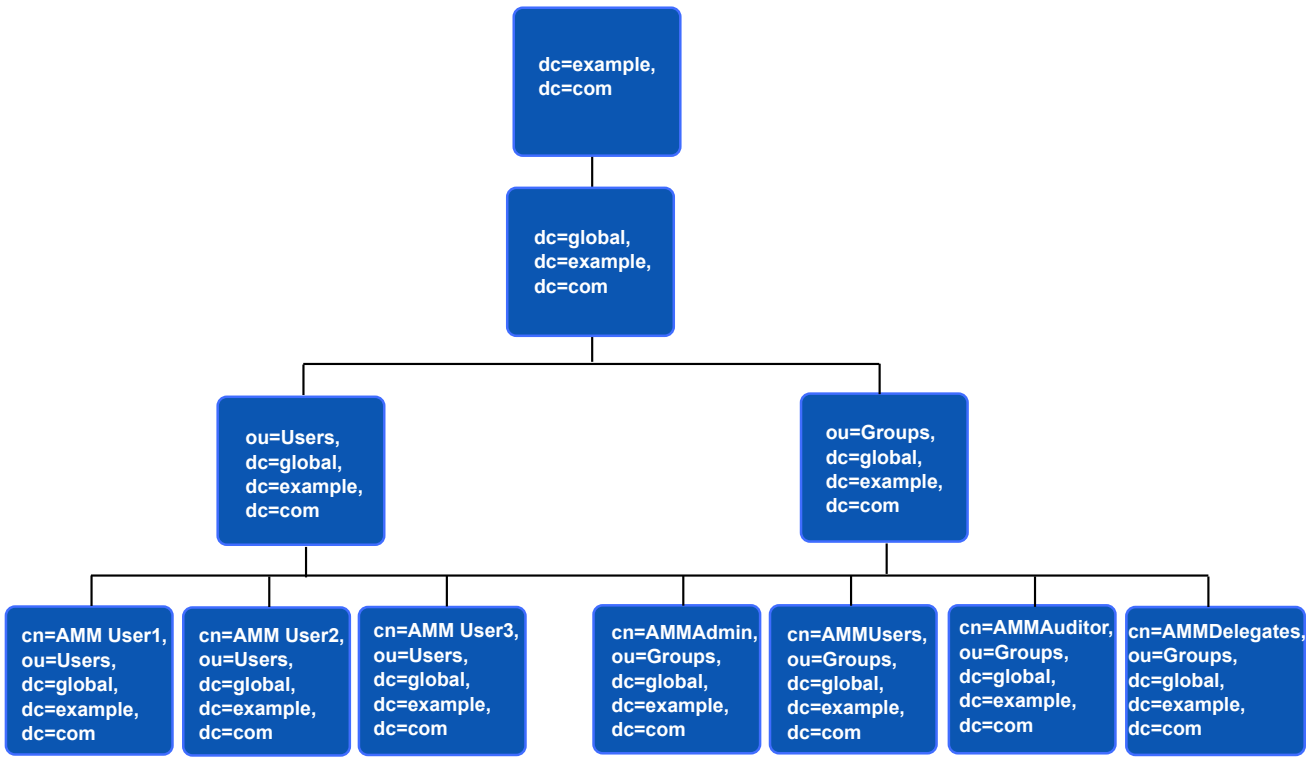


Figure 2: LDAP configuration example

- 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 User2” as the value of its “member” attributes.

Configuring the binding parameters

About this task

The following procedure describes how to configure the LDAP binding parameters when Microsoft Active Directory (AD) is used.

Procedure

1. In the Avaya Multimedia Messaging CLI, run the following command to start the configuration utility:

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

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/search access to Active Directory.	global\AMMAssistant
Bind Credential	The password for the Bind User.	admin123

Configuring the authentication parameters

About this task

The following procedure describes how to configure the LDAP authentication parameters when Microsoft Active Directory (AD) is used.

Procedure

1. In the Avaya Multimedia Messaging CLI, run the following command to start the configuration utility:

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

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 Microsoft Active Directory, there are usually two types of userID: Domain user ID or User Principal Names. Avaya Multimedia 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”.	sAMAccoutName userPrincipalName

Table continues…

Parameter	Description	Example
	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=example,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

The following 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. Typically, 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” attributes that stores the DNs of all of the users and sub-groups that are members of this group.

Procedure

1. In the Avaya Multimedia Messaging CLI, run the following command to start the configuration utility:

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

2. Select **LDAP Configuration** > **Advanced LDAP parameters**.
3. Configure the following 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” attribute of the user.	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 that this 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		Must be left empty, since “Role Attribute is DN” is false.
Role Recursion	0	This configuration does not allow	1 or higher	You must set this value to 0 if there

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
		recursive search. So **Note:** Using this configuration, the users under the “AMMDelegates” group will not be able to use AMM so this is not the recommended configuration for this example.		are no subgroups or a value from 1 to 10 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.

4. Configure the following attributes as described in the following table.

   The configuration of the following parameters is the same, regardless of the configured search mechanism.

Parameter	Description	Example
Search Scope	Set to 2 or SUBTREE_SCOPE to search the role base context and under it.	2 or SUBTREE_SCOPE
Administrator Role	This parameter 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 parameter 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 parameter 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	This parameter specifies the list of the “role” string extracted from LDAP that would be mapped to the Avaya Multimedia Messaging server Service Administrator application role.	AMMServiceAdmin

Table continues…

Parameter	Description	Example
Services Maintenance and Support Role	This parameter specifies the list of the “role” string extracted from LDAP that would be mapped to the Avaya Multimedia Messaging server Services Maintenance and Support application role.	AMMMaintenance

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. 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. 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

4. Click **Save**.
5. Click **Modify Attribute Mappings**.
6. 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

Table continues…

Parameter	Description	Default value
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" parameters are 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.

7. Click **Save**.

   The Avaya Multimedia Messaging services restart for the changes to take effect.

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.

The following procedure describes how to configure the user management parameters for Microsoft Active Directory.

Procedure

1. In the Avaya Multimedia Messaging CLI, run the following command to start the configuration utility:

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

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 bit-wise AND filter to check the second lowest bit in the value of “userAccountControl”, which is “1” if the 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	(&(objectClass=user)(objectCategory=Person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
Last updated time attribute	The value for AD is “whenChanged”.	whenChanged

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 124.

```
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 update**.

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 update**.

Avaya Multimedia Messaging federation configuration with Presence Services

The Avaya Multimedia Messaging federation supports four different deployment models, that can contain:

- A standalone Avaya Multimedia Messaging server and an Avaya Aura® Presence server
- A standalone Avaya Multimedia Messaging server and a cluster of Avaya Aura® Presence servers
- An Avaya Multimedia Messaging cluster and an Avaya Aura® Presence server
- An Avaya Multimedia Messaging cluster and a cluster of Avaya Aura® Presence servers

The federation configuration for each deployment model consists of an XMPP server that contains all the Avaya Multimedia Messaging servers and all the Avaya Aura® Presence servers.

The federation configuration must be performed on the Avaya Multimedia Messaging server side, as well as the Presence Services side.

Presence Services side configuration

The following procedures describes how to configure Avaya Multimedia Messaging federation on the Presence side. The configuration process varies depending on whether you are using Presence Services Release 6.2.x or Release 7.x. Presence Services Release 6.2.x is XMPP-based, and Release 7.x is HTTP-based. You cannot use XMPP and REST concurrently. or information about migrating to the 7.x REST environment, see Migration of the Avaya Aura environment on page 240.

In a clustered Presence Services configuration, the following procedures must be performed for every node in the Presence Services cluster.

Configuring Presence Services Release 6.2.x for Avaya Multimedia Messaging federation

About this task

This procedure describes how to configure the Avaya Multimedia Messaging federation on the Presence Release 6.2.x. side using the Presence server GUI. You must repeat this procedure on every node in the cluster.

For more details about configuring an XMPP federation, see *Administering Avaya Aura® Presence Services*.

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. Log in to the Presence server GUI.

   The browser displays the XCP Controller configuration page.

2. In the XCP Controller configuration page, perform the following actions to enable the Federation and Avaya Multimedia Messaging domains:

   a. In the top right corner, in the **Configuration view** field, select **Advanced**.

   b. In the **Router** field, locate to the **Core Router** in the **Plugin** column and click **Edit**.

   c. Select the **Federation Domains** check box and add the Avaya Multimedia Messaging domain in the corresponding text box.

   d. Select the **Avaya Multimedia Messaging Configuration** check box and add the Avaya Multimedia Messaging domain.

   e. Click **Submit** to save the changes.

3. In the XCP Controller configuration page, perform the following actions to add a new Connection Manager:

   a. In the **Components** field, select **Add a new Connection Manager** and click **Go**.

   b. In the **Description** field, type `AMM Connection Manager`.

   c. In the **Add a New Command Processor** field, select **S2S Command Processor** and click **Go**.

   Important:

   Remember the **S2S Command Processor ID**, as you must use the S2S Command Processor ID to create an Open Port.

   d. In the **Authorized Outgoing 'From' Addresses** field, select **deny** as the default behavior and enter each Presence domain in the **Host Filters** text box.

   e. In the **Actions** column, click **Detail** to view the details of the active rules.

   f. In the **Outgoing Connection Attempt Rules** field, ensure that the only active rule is the rule that has the value of **DNS SRV lookup to use** equal to `_xmpp-server._tcp`.

   g. Click **Submit** to save the changes until you return to the XCP Controller configuration page.

4. In the XCP Controller configuration page, perform the following actions to add a new Open Port:

   a. In the **Components** field, select **Open Port** and click **Go**.

   b. In the **enter ID of open port component** alert window, enter the S2S Command Processor ID.

Important:

Ensure that you use the same S2SCP component name, created during the configuration of the OCS Gateway, for the Open Port component name. Also, you must not include `.presence` in the Open port component name.

For example: if the name of the Connection Manager was `cm-2` and the S2SCP is `cm-2_s2scp-1`, then enter `cm-2_s2scp-1` as the component ID for the Open Port component.

c. In the **Description** field, type `AMM Open Port`.

d. In the **Hostnames for this Component** field, add the Avaya Multimedia Messaging domain name.

e. Click **Submit** to save the changes.

5. Restart the Presence server.

Note:

In a clustered Presence Services configuration, you must perform all the configuration steps on every Presence Services node and perform a system restart on every node.

Configuring Presence Services Release 7.x for Avaya Multimedia Messaging federation

About this task

The following procedure describes how to configure Presence Services Release 7.x federation. 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** checkbox for each item and set the following values:
   a. Set **AMM Integration enabled** to **True**.
   b. Enter the URL of the Avaya Multimedia Messaging server.
   c. Enter the web service path for the Avaya Multimedia Messaging server. For example, `aem/xmpp/stanza`.
   d. Enter all trusted Avaya Multimedia Messaging host names using a comma-separated list.

Configuring the XMPP interface in Avaya Multimedia Messaging for federation with Presence Services

About this task

Use this procedure to configure XMPP for Avaya Multimedia Messaging federation with Presence Services. This procedure describes the configuration you perform on the Avaya Multimedia Messaging server side, by using the administration portal.

For the configuration needed on the Avaya Aura® Presence Services side, see *Administering Avaya Aura® Presence Services*.

Before you begin

Before you configure the Avaya Multimedia Messaging–Presence Server federation, you must ensure that:

- The Presence server is reachable.
- The DNS server contains an SRV record of each Presence domain.

Important:

In an Avaya Multimedia Messaging cluster, make sure there is network connectivity between every node and the Presence Server.

Procedure

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

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

   Important:

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

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

2. In the left panel, select **Server Connections** > **Federation Configuration**.

3. In **XMPP Adapters**, do one of the following:
   - Click **Add**.
   - Select an existing option and click **Edit**.
4. In **XMPP-0114 Connection Adapter**, perform the following actions:
   a. Select the **Adaptor Enabled** check box.
   b. In the **Name** field, type a name, such as Pe`XMPP1`.
   c. In the **Routing Domain** field, enter the Avaya Multimedia Messaging domain name.
   d. Select the **Send Presence Ping** check box.
   e. In **Add Domain**, add the Presence domains and select the corresponding check boxes to enable the domains.
5. Click **Save**.
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`.

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.

For the configuration needed on the Avaya Aura® Presence Services side, see *Administering Avaya Aura® Presence Services*.

Procedure

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

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

   Important:

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

   To gain access to the web-based administration portal, you must use an account that has the Administrator role defined in the LDAP server configuration.
2. In the left panel, select **Server Connections** > **Federation Configuration**.

3. In **HTTPS REST to Avaya Presence Services Connection Adaptors**, do one of the following:
   - Click **Add**.
   - Select an existing option and click **Edit**.
   a. Select the **XEP-0033** protocol.

      Note:

      Only the XEP-0033 protocol is supported.

   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. In the **Routing Domain** field, enter the Avaya Multimedia Messaging domain name.
   g. Select the **Send Presence Ping** check box.
   h. In **Add Domain**, add the Presence domains and select the corresponding check boxes to enable the domains.
4. Click **Save**.
5. 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`.

Avaya Multimedia Messaging federation configuration with Microsoft Lync

The following sections describe how to configure Avaya Multimedia Messaging to interoperate with Lync.

Avaya Multimedia Messaging server can be federated with a Lync installation using SIP. The Avaya Multimedia Messaging server can be federated directly to the Lync front end in the case of an intRA enterprise deployment, or via the Avaya Aura® Session Manager to the Lync edge server in the case of an intER enterprise deployment."

For information about Lync federation limitations, see “Caveats and limitations” in *Avaya Multimedia Messaging Reference Configuration*.

Lync federation checklist

The following checklist outlines the tasks you must perform to configure Avaya Multimedia Messaging federation with Microsoft Lync.

No.	Task	✔
1	Obtain the default Lync server certificate to put in the trust store for each Avaya Multimedia Messaging node. Review the sections under Default Lync server certificate to put in the trust store for each Avaya Multimedia Messaging node on page 108.	
2	Configure the Lync attributes for Presence Services to allow presence updates.	
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 31.	
5	Configure the Avaya Multimedia Messaging server for Lync federation.	
6	Configure the Lync server for an internal or external domain as required.	
7	Perform DNS configuration for Lync and for the Avaya Multimedia Messaging server.	
8	Configure Avaya Multimedia Messaging clusters to interoperate with Lync	
9	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 and Lync interoperability within the same domain:

No.	Task	✔
1	Add the default server certificate to the System Manager trust store.	
2	Configure the Adaptation module for Lync.	
3	Complete the Local Host Resolution Table.	
4	Configure SIP entities and set the IM Gateway SIP entity for each user for an Avaya Multimedia Messaging cluster entity.	
5	Use the Application Editor to set application media attributes, so media types used for IM are sequenced through Communication Manager.	
6	Configure application media attributes.	

Table continues…

No.	Task	✔
7	Configure domains.	
8	Configure users.	
9	Configure routing policies and expressions.	
10	Configure the Lync Edge server.	

Adding the Lync certificate to System Manager

About this task

Use this procedure only if System Manager and Lync are using different certificate authorities.

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 **Configure 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.

Lync adaptation configuration

The `LyncAdapter.jar` is bundled with the Avaya Multimedia Messaging binary installer. You can find the `.jar` file in the `asm-adaptation` directory under the Avaya Multimedia Messaging install root. For example, the location might be `/opt/Avaya/MultimediaMessaging/3.0.0.0.2266/CAS/3.0.0.0.2266/asm-adaptation/LyncAdapter.jar`.

Installation command line

You can use the following command line for installation:

```
--tar xf -- ./LyncAdapter.jar
```

This command extracts the file into the same directory where the command was run.

Adding the Lync adapter file in System Manager

About this task

You must transfer the `LyncAdapter.jar` file to the computer running System Manager. You can place the file anywhere, as long as it is accessible from the System Manager interface.

Procedure

1. In the System Manager web interface, navigate to **Elements** > **Routing** > **Adaptations**.
2. From **More Actions**, click **Manage Modules**.
3. Upload the `LyncAdapter.jar` file.
4. Select the file and click **Deploy** to finish deploying the `.jar` file.
5. To create a new Lync adaptation, click **New**.
6. In **Adaptation Name**, enter a name, such as `LyncAdaptation`.
7. Select **LyncAdapter** from the **Module Name** drop-down menu.
8. Click **Commit** to save your changes.

   The Lync Adapter appears in the list of adaptations with the name you entered and can be associated with an entity.

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.

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. For the relay entity, do the following:
   a. Type a unique name that identifies the relay entity in **Host Name (FQDN)**.

      This entry will resolve this name locally in Session Manager. It does not need to be resolved in the enterprise.
   b. In an Avaya Multimedia Messaging cluster configuration, enter the virtual IP in the **IP Addresses** field. Otherwise, enter the node IP.

c. In the **Port** field, type `5063` .

d. Ensure that **Transport** is set to **TLS**.

4. Click **Commit** to save your changes.

SIP entities

You can add SIP entities in System Manager by navigating to **Elements** > **Routing** > **SIP Entities**.

Two types of SIP entities exist for Avaya Multimedia Messaging. One handles IM requests from Lync, and the other is for the relay function that Avaya Multimedia Messaging performs between Lync and Avaya Aura® Session Manager. Both entities' FQDN need to be resolvable by Session Manager and can be identified in the Local Host Resolution Table. The entities must be distinct, with their own routing policy, and different FQDNs.

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.

Relay SIP entity

The relay entity bridges the connection between Lync and Avaya Aura® Session Manager. The entity FQDN does not need to be the same as the front-end FQDN. This entity requires the Lync adaption.

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	Value for relay 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.	Enter any value.
Type	Select **Other**.	Select **SIP Trunk**.
Adaptation	Leave this blank.	Select **LyncAdaptation**.

Table 20: Entity links

You must configure Entity links between Avaya Aura® Session Manager and both the front-end and relay SIP entities of Avaya Multimedia Messaging. You must configure at least two Session Manager instances to have entity links to both for redundancy.

Entity link field	Value for front-end SIP entity	Value for relay SIP entity
Name	Enter any value.	
SIP Entity 1 and **SIP Entity 2**	Select from the drop-down list. SIP entity 1 is for the Session Manager side, and SIP entity 2 is for the Lync Edge server.	
Protocol	Select **TLS**	
Port for the Avaya Multimedia Messaging side	Always set to 5061.	Always set to 5063.
Port for the Session Manager side	Same as the administered port for the Session Manager SIP adaptor. This port is usually set to 5061.	Must be different from the administered port of the Session Manager SIP adapter. For example, if the Session Manager SIP adaptor port is 5061, then use another port, such as 5062 or 5063.

Setting the IM Gateway SIP entity for a user in an Avaya Multimedia Messaging cluster

About this task

Repeat this procedure for each user in an Avaya Multimedia Messaging cluster.

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 Avaya Multimedia Messaging cluster.
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 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 edge 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 only
- Avaya Multimedia Messaging only

Note:

Avaya Multimedia Messaging does not support dual users.

Routing policies and regular expressions

You must set routing policies corresponding to each SIP entity, IM, and Relay. You must do this in System Manager by navigating to **Elements** > **Routing** > **Routing policies**. The regular expressions patterns corresponding to each routing policy are the following:

- For IM: The front-end FQDN, which is set during the front-end configuration. This FQDN is part of the URI (Uniform Resource Identified) in all the requests from Lync to the Avaya Multimedia Messaging front-end SIP entity.
- For relay: The string `lync_front_end`. This is set as a parameter in the URI request by Presence Services to indicate that the `SUBSCRIBE` request must go to the Avaya Multimedia Messaging relay SIP entity.

Example

The following policy shows the presence request routing for mycompany.com:

```
amm\.frontend\.fqdn@.+ AMMfront-end
.+@mycompany\.com.+lync_front_end.* AMMRelay
```

Lync edge server configuration

You must configure SIP entities, routing policies, and regular expressions for routing to the Lync 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 edge server:

SIP entity values

Table 21: SIP entity general fields

Field name	Value for Lync edge server SIP entity
Name	Enter any value.
FQDN	Enter same value as Lync edge.
Type	Select **SIP Trunk**.
Adaptation	Select **LyncAdaptation**.

Table 22: Entity link fields

Field name	Value for Lync edge server SIP entity
Name	Enter any value.
SIP Entity 1 and **SIP Entity 2**	Select from the drop-down list. SIP entity 1 is for the Session Manager side, and SIP entity 2 is for the Lync 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 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 edge server
Name	Enter any value.
SIP Entity	SIP Entity of Lync 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 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 Lync 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 front-end server certificate. For more information, see Importing the Lync front-end server certificate into the trust store on page 109.	
3	Verify LDAP and System Manager setup in the Avaya Multimedia Messaging administration portal. You can also force updates.	
4	Configure SIP adapters.	

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 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 34.

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 Update** button on this page. Data synchronization can take a few minutes.

Configuring SIP adapters

About this task

You must create two SIP adapters for Lync federation: one for Session Manager and the other for Microsoft Lync.

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 143 and 4 on page 143 for each SIP adapter.

3. Click **Add** to add each SIP adaptor.

4. On the new adapter page:

   a. Set **Select Type** to **Avaya Session Manager** for the first SIP adapter, and to **Microsoft Lync** for the second SIP adapter.

   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 adapter.

      Note:

      If you are using multiple Session Manager servers, instead of entering an address, select the **Use SRV Record** check box.

   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. Add a Remote domain if needed.

   The Remote domain is the Avaya Multimedia Messaging server domain.

h. Add a From domain, if needed, to pick the correct SIP adaptor.

   The From domain can be used for simultaneous Lync and Presence interoperability. This can occur if an existing company uses Presence Services as the IM server and is federated with Lync through the Lync Edge server. The Lync domain is “company.com” and the domain used for federation is “ps.company.com”. In this case, you want addresses from “company.com” to go to the Lync front end server and addresses from “ps.company.com” to go to the Lync Edge server.

   When the From domain does not find a match, it uses the Lync adaptor by default.

   Important:

   The Remote domain always takes precedence over the From domain. If you require a From domain, you can leave the Remote domain empty.

i. **(Optional)** To add a domain without directory access from the network of a different enterprise and to enable message exchange between users, in the **Domains without Directory Access** table, type the domain name in **Add Domain** and then click **Add**.

   All users from the domain are considered valid.

j. Click **Save** when you complete the configuration for each adapter.

5. After both SIP adapters are added, restart the system.

   A restart is required to use the newly enabled adapters.

Related links

Multiple Session Manager servers on page 144

Multiple Session Manager servers

You can configure multiple Session Manager servers by selecting the **Use SRV Record** checkbox for the Session Manager SIP adapter. Avaya recommends configuring DNS with one of the Avaya Multimedia Messaging messaging domains.

You must configure SRV records for each Session Manager with the following values:

Field	Value
Service name	**_amm-sm**
Transport	**_tcp**
Domain	One of the domains configured for Avaya Multimedia Messaging to use.

Table continues…

Field	Value
	For example, if Avaya Multimedia Messaging is configured to use avaya.com as a domain, the SRV record name is `amm-sm._tcp.avaya.com`.

Related links

Configuring SIP adapters on page 143
Selection of the correct routing domain for configuring XMPP federation with the Presence Services 6.2.x server on page 27

Lync server configuration for an internal domain

The following sections describe the Lync server internal domain configuration required for Lync federation.

Lync server internal domain configuration checklist

Use this checklist to complete the Lync 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 140.	
2	Check that the Avaya Aura® System Manager and Avaya Aura® Session Manager use the same domain recognized by Lync. For more information, see Domain configuration on page 140.	
3	Configure Avaya Multimedia Messaging as a Lync trusted server. For details, see Configuration of Avaya Multimedia Messaging as a Lync trusted server on page 145.	
4	Get a Lync certificate with both client and server authentication. For details, see Getting a certificate with client and server authentication on page 152.	
5	Place the System Manager CA certificate into the Lync Trust Store. For details, see Placing the System Manager CA certificate into the Lync Trust Store on page 155.	

Configuration of Avaya Multimedia Messaging as a Lync trusted server

The following configuration allows an Avaya Multimedia Messaging SIP application to register to the server and function as a Lync user device in multiple instances, without requiring user credentials.

Ensuring that port 5061 is enabled on the Lync server

Before you begin

If you have users in the domain used by Lync, 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 front end and Lync 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 as a trusted application

Adding each Avaya Multimedia Messaging server node and front-end FQDN as a trusted application to Lync Standard Edition

About this task

Use the following procedure to add each Avaya Multimedia Messaging server node and the front-end FQDN to Lync 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 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 logs.

If the Trusted Application Pool is created, Lync 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 Enterprise Edition

About this task

Use the following procedure to add each Avaya Multimedia Messaging server node and the front-end FQDN to Lync 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 Avaya Multimedia Messaging as the destination of a static route

About this task

All requests from the Lync server that create a dialog with Avaya Multimedia Messaging are routed through Session Manager, which is used as a load balancer. You must set up a static route to the Avaya Multimedia Messaging virtual IP node by associating its FQDN with the Avaya Multimedia Messaging messaging domain. This Avaya Multimedia Messaging node relays the request to Session Manager. Because this node is a SIP relay node, the port used is 5063.

Important:

Because dual users are not supported, the Avaya Multimedia Messaging user must not have the `msrtcsip-userenable` attribute set to **true** in the Enterprise Directory.

If the `msrtcsip-userenable` attribute is set to **true**, the user has logged into Avaya Multimedia Messaging and has valid Lync contact in the messaging domain, then Avaya Multimedia Messaging will not send message for that Lync contact.

Note:

Routing to external users, on both static and dynamic route, requires that the destination domain exists as an allowed federated domain on Lync side.

Procedure

1. Log in to the Lync front-end server.
2. Go to **Start** > **Lync Server Management Shell**.
3. To create a static route to Avaya Multimedia Messaging for the Lync domain, run the following commands:

   a. `$route = New-CsStaticRoute -TLSRoute -destination "<AMM_node_FQDN>" -port 5063 -matchuri "<lync_server_domain>" -usedefaultcertificate $true`

   b. `Set-CsStaticRoutingConfiguration -identity global -route @{Add=$route}`

4. Enable the newly created topology by entering the following command:

```
Enable-CsTopology
```

5. To enable all communications for the static route, open the Lync server control panel and do the following:
   a. In **Federation and External Access**, click **SIP Federated Domains**.
   b. Click **New** and create an Allowed Domain.
   c. In **Domain Name (FQDN)** enter the messaging domain of the Avaya Multimedia Messaging server and leave **Access Edge FQDN** blank.
   d. Verify that the Lync users `External Access policy` has **Federated User Access** enabled.
6. **(Optional)** To display a route, run the following command:

```
Get-CsStaticRoutingConfiguration | Select-Object -ExpandProperty Route
```

7. **(Optional)** To delete a route, run the following command:

```
Set-csstaticroutingconfiguration -identity global -route $null
```

Adding the Avaya Multimedia Messaging root signing certificate to the Lync server

About this task

Use this procedure to allow the Lync 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 Trust Store on page 155.

Procedure

1. Log in to the Lync 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 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 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** checkbox.
   e. Click **Add Host**.

Adding the Avaya Multimedia Messaging domain as a SIP federated provider

Procedure

1. Log in to the Lync 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 front-end servers

About this task

Use this procedure when you first add certificates into Lync. 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 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 153.
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:
   a. Select **Local Computer**.
   b. Click **Finish**.
   c. Click **OK**.
10. Expand **Certification Authority (Local)**.
11. Right-click **Certificate Templates**.
12. If the template you identified in step 5 on page 152 is not available, do the following:

Note:

If the template is available in the list, then skip this step.

a. Click **New** > **Certificate Template to Issue**.
b. From the list, select the certificate template to enable.
c. Click **OK**.

Next steps

On the Lync 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:
   a. Select **Local Computer**.
   b. Click **Finish**.
   c. 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 template and then click **Duplicate Template**.
10. Enter the general information in the General tab.
11. Click the **Extensions** tab and do the following:
    a. Right-click **Application Policies**.
    b. In the Edit Application Policies Extension screen, click **Add**.
    c. Click **Client Authentication** or **Server Authentication** as the application policy.
    d. Click **OK**.

    The template must support both client and server authentication. You can repeat this process if required.

Next steps

On the Lync front-end server, assign the certificate.

Assigning the certificate to the Lync front-end server

Procedure

1. Log in to the Lync 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 154 and click **Open**.
4. Choose a name for the certificate file and click **Save**.
5. Copy the certificate file to the Lync 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 users. Lync recognizes one domain as local and any other domain must be federated. If the Avaya Multimedia Messaging and the Lync 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. For details, see Adding Avaya Multimedia Messaging as the destination of a static route on page 149. You must also add this domain to the SIP federated domains list, without entering the Edge server details, in the Lync front-end server control panel, in **Federation and External Access** > **SIP Federated Domains**.

Placing the System Manager CA certificate into the Lync 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.

Lync server configuration for an external domain

Lync server configuration for an external domain is the same as a standard Lync setup. You must deploy external user access in the Lync server. For more information, see https://technet.microsoft.com/en-us/library/gg398918(v=ocs.15).aspx.

Ensure you complete System Manager configuration. The most important tasks are:

- Create a SIP entity for the LyncEdge server and route the Lync domain through Session Manager to the Lync Edge, either by DNS or regular expression.
- Add the System Manager CA certificate as a trusted root certificate in the Lync trust store.
- Add the CA signed certificate used by Lync edge server and update the TLS certificate through Session Manager. For details, see *Avaya Aura® Presence Services Snap-in Reference*.

Related links

Domain configuration on page 140
Placing the System Manager CA certificate into the Lync Trust Store on page 155

Configuring Lync federation for Presence Services

About this task

Use this procedure to allow for Presence updates to Lync federation.

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 the arrow to expand the Lync federation items.

5. Select the **Override Default** checkbox for each item and set the following values:
   a. Set the **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**.

DNS configuration

DNS configuration for Lync

Servers that Lync communicates with using SIP must have an FQDN that is accessible through the DNS lookup service. Lync cannot communicate with an external server that is identified by only an IP address. The Lync edge server is designed for external communication. The Lync front-end server can only handle SIP messages that:

- Have the Lync 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 edge server:

```
_sipfederationtls._tcp.<remote.domain>
```

SRV records for Lync client DNS processing

Lync clients use DNS to discover services. For information about determining the DNS requirements for your Lync 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 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.

Table continues…

SRV record	Description
`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 adapter 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 adapter 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 interoperability

The following sections describe how to set up an Avaya Multimedia Messaging cluster with Lync federation. Start with a normal Avaya Multimedia Messaging cluster and then add Lync interoperability.

Avaya Multimedia Messaging cluster with Lync checklist

The following checklist outlines the tasks you must perform to configure an Avaya Multimedia Messaging cluster with Lync.

No.	Task	Reference	✔
1	Configure a normal Avaya Multimedia Messaging cluster.	Clustering configuration on page 98	

Table continues…

No.	Task	Reference	✔
2	Make each nodal IP a trusted node on Lync, and ensure that the Lync server can resolve the node's FQDN. You must do the following: • Add each Avaya Multimedia Messaging server node to Lync as a trusted application. **Important:** Do not set up static routes for each cluster node. • Ensure that each Avaya Multimedia Messaging server node is in DNS.	Configuration of Avaya Multimedia Messaging as a Lync trusted server on page 145	
3	Make the virtual IP a trusted node on Lync, and ensure that the Lync server can resolve the cluster's FQDN.	Adding each Avaya Multimedia Messaging server node and front-end FQDN as a trusted application to Lync Standard Edition on page 146 Adding each Avaya Multimedia Messaging server node and front-end FQDN as a trusted application for Lync Enterprise Edition on page 147	
4	Add a static route to the cluster IP. **Important:** Do not add static routes to the nodal IPs.	Adding Avaya Multimedia Messaging as the destination of a static route on page 149	
5	Configure SIP entities in System Manager.	SIP entities on page 138	
6	Complete the Local Host Resolution Table in System Manager.	Adding Avaya Multimedia Messaging nodes to the Local Host Resolution Table on page 137	
7	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 cluster on page 139	
8	Add the Lync certificate to the MSS trust store on each node.	Adding the Lync certificate to the MSS trust store on each node on page 110	

User configuration

The following types of Lync and Avaya Multimedia Messaging users exist:

- Lync only

- Avaya Multimedia Messaging only

  Note:

  Avaya Multimedia Messaging does not support dual users.

Related links

User profile configuration in System Manager on page 140

User configuration checklist

The following checklist outlines the tasks that you must perform to configure Lync and Avaya Multimedia Messaging users.

No.	Task	✔
1	Add Lync users to the Lync 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. For information about configuring Avaya Equinox™ settings, see *Using Avaya Equinox™ for Android, iOS, Mac, and Windows*.	
3	Configure Lync-only and Avaya Multimedia Messaging-only users.	

Related links

Adding Lync users to the Lync server on page 159
Configuration of Lync-only and Avaya Aura-only users on page 160

Adding Lync users to the Lync server

Procedure

1. Open the Lync 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-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-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 user. For Lync users, this defines the Lync address of record for both IM and Presence. For Avaya Aura® users, this can be configured to allow Lync 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	sip:address123@exmpl.com

Table continues…

Attribute	Description	Example
	Aura users Presence or IM handle from above. The SIP schema is usually prefixed to the use the handle.	
msRTCSIP-UserEnabled	The boolean that indicates whether Lync has enabled the user. For Lync users, this will be set by the Lync client configuration. For Avaya Aura® users, this must be FALSE or not set to force Lync 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 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`.

Customizing the login screen message for the Message Playback component

About this task

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

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

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

Procedure

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

   The `value` attribute contains the instructions text.

For example:

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

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

External configuration requirements

Install Adobe Flash Player for Message Playback

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

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

Note:

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

Do Not Disturb functionality for Avaya Aura® Presence Services

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

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

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

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

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

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

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

Disable instant messaging for 96x1 SIP desk phones

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

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

Configure Avaya Equinox™ for iPad to use the IM capabilities

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

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

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

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 8443, 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.

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 8443.
   - **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.

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 8443 and is	

Table continues…

No.	Task	Notes	✔
		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 165.	
3	Issue certificate from Certificate Authority.	See Creating an end entity on page 167 and Creating the certificate by using certificate signing request on page 168.	
4	Ensure port 8443 is open on both sides of Avaya SBCE.		
5	Install server certificates on Avaya SBCE.	See Uploading certificate file on page 169 and Synchronizing and installing certificate in a multi-server deployment on page 170.	
6	Install client certificates on Avaya SBCE.	See Downloading the System Manager certificate on page 171 and Installing CA certificate on page 172.	
7	Create client and server TLS profiles.	See Creating a new TLS server profile on page 172 and Creating a client profile on page 175.	
8	Add reverse proxy.	See Adding reverse proxy on page 177.	

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.
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.

Table continues…

Name	Description
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.
Passphrase	The password used when encrypting the private key.
Confirm Passphrase	A verification field for the Passphrase.
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

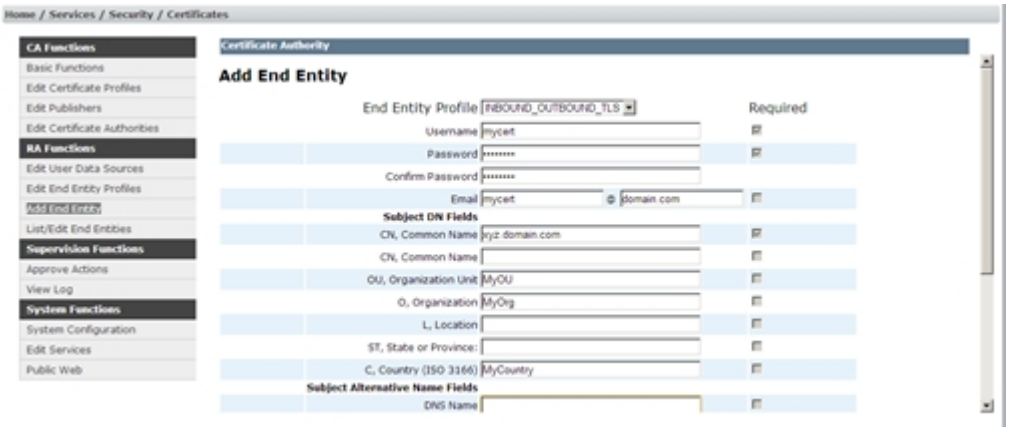
Procedure

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**, click **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.

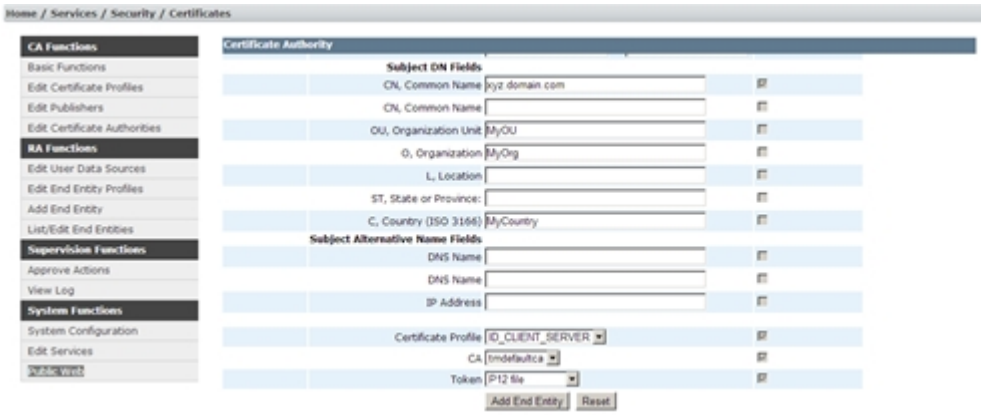
6. Complete the fields that you want in your certificate.



   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 End Entity**.

   The system displays the message `End Entity <username> added successfully.`

Creating the certificate by using certificate signing request

Before you begin

Create an end entity.

For more information, see 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. 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**.

      The system signs the certificate signing request (CSR) and generates a PEM-formatted certificate that 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.

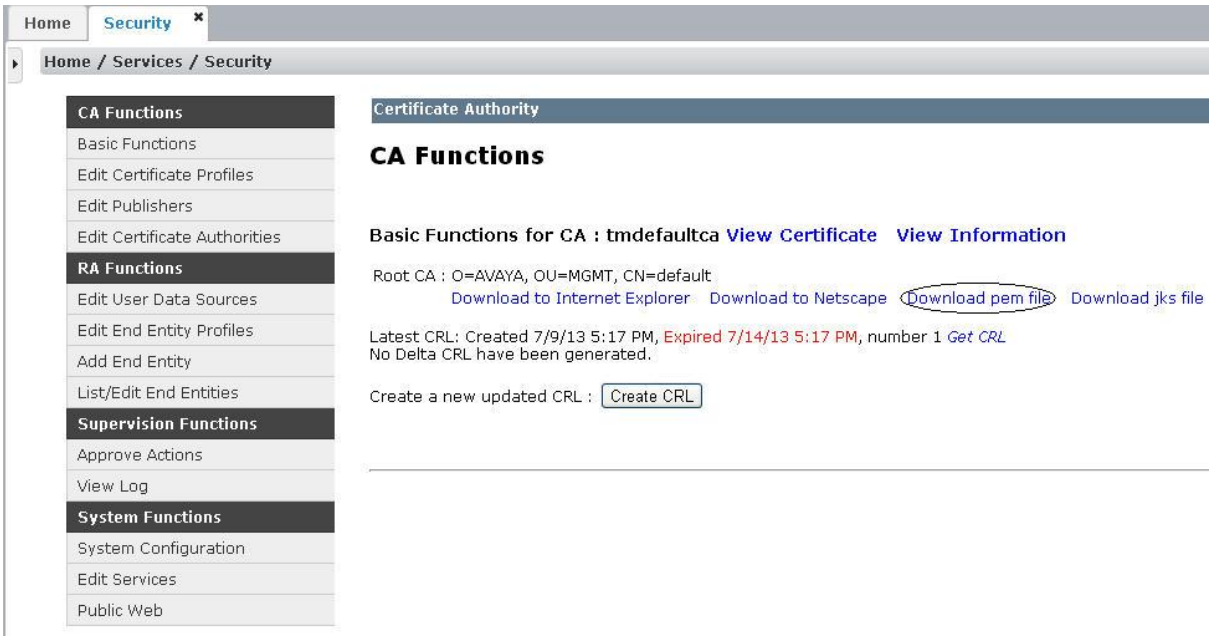
13. Use the EMS web interface to restart the Avaya SBCE application.

Downloading the System Manager certificate

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.

3. On the CA Functions page, click **Download pem file**.



4. After you download the .pem file, save the file to 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 175

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	
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.

Table continues…

Field	Description
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.
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 173.

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.

Table continues…

Name	Description
	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	
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 reverse proxy

About this task

You must 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 8443 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. Preferably, 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**.

Enhanced Access Security Gateway support for Avaya Multimedia Messaging

Enabling and disabling the Enhanced Access Security Gateway

About this task

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

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

Procedure

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

   ```
   EASGStatus
   ```

   By default, the EASG status is disabled.
3. To enable EASG, do the following:
   a. In the SSH console, run the following command:

      ```
      sudo /usr/sbin/EASGManage --enableEASG
      ```

   b. Run the following command to verify the product certificate:

      ```
      sudo EASGProductCert --certInfo
      ```

      The system displays the product certificate details.

      For example:

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

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

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

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

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

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

4. To disable EASG, run the following command:

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

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

About this task

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

Procedure

1. Open the SSH console as an administrator.

2. To install EASG, run the following command:

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

   The system installs the EASG `.rpm` file and creates the `susers` group if it is unavailable. It also adds the users to the `susers` and `ucgrp` groups.

3. Check the EASG status by running the following command:

```
EASGStatus
```

   By default, the EASG status is disabled.

4. To enable EASG, run the following command:

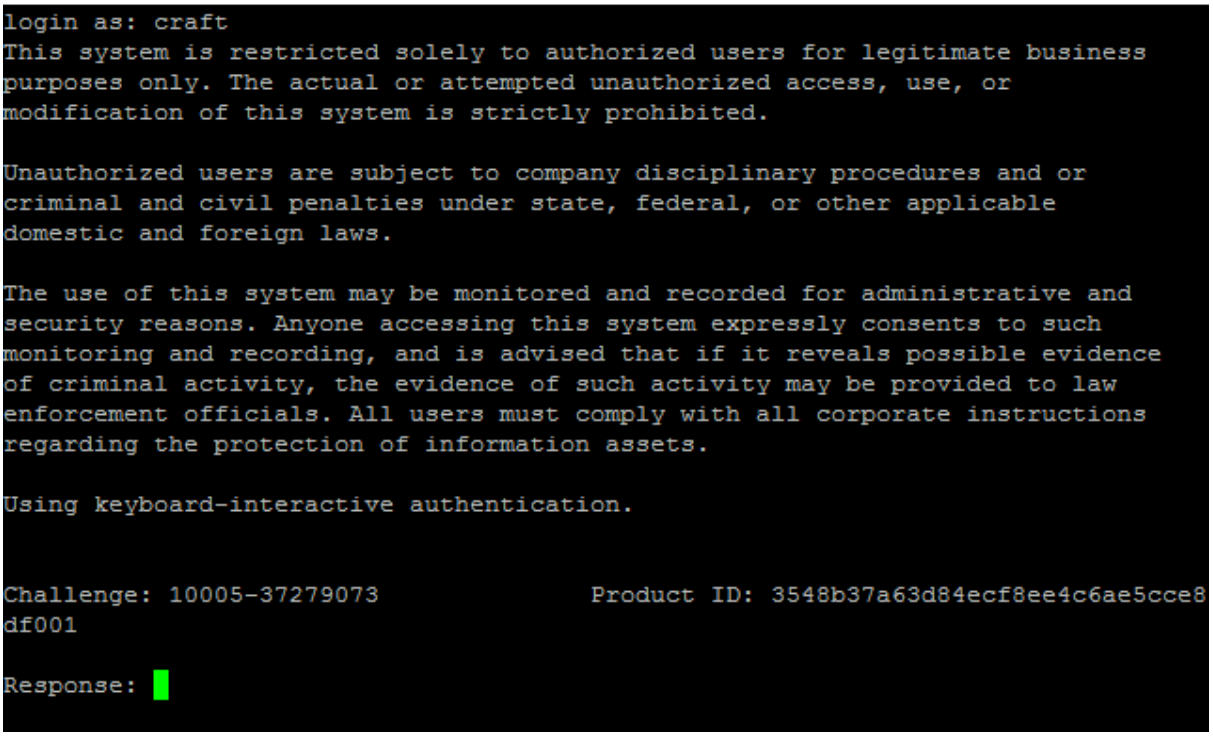
```
sudo /usr/sbin/EASGManage --enableEASG
```

5. To verify the product certificate, run the following command:

```
sudo EASGProductCert --certInfo
```

   The system displays the product certificate details.

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



7. To complete the Pluggable Authentication Module (PAM) settings for user authentication, do the following:

   a. In the PAM file stack, add `auth [success=done auth_err=bad default=ignore] pam_asg.so` so that it appears before `pam_unix.so`.

b. In the password stack, add `password sufficient pam_asg.so` so that it appears in the first line.

   The following is an example of the PAM settings:

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

account required pam_access.so

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

session required pam_limits.so
```

Removing EASG

About this task

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

Procedure

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

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

Related links

Installing and enabling the Enhanced Access Security Gateway on a physical server on page 62

Chapter 7: Administration

Working with the Avaya Multimedia Messaging administration portal

About this task

The following sections describe the tasks you can perform on the web-based administration portal. You can make changes to server settings in the administration portal at any time. To access the administration portal, you must use one of the following web browsers:

- Internet Explorer 9, 10, or 11.
- The latest version of Mozilla Firefox or the version before it.

Before you begin

- Complete server installation and configuration. You cannot access the Avaya Multimedia Messaging web-based administration portal until the server is configured.
- To log in to the web-based administration portal, you must configure the Administrator role as part of LDAP configuration.

Note:

The format for the user name might be `user@yourdomain.com` or `domain\user`, depending on the configuration of the LDAP server.

Procedure

Log in to the Avaya Multimedia Messaging administration portal.

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

Important:

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

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

Result

A menu with administration options displays on the left side of the screen.

Starting and stopping the Avaya Multimedia Messaging service

Procedure

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

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

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

Managing server storage

About this task

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

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

Procedure

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

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

Managing messaging domains

About this task

Use this procedure to update the list of messaging domains.

Procedure

1. In the Navigation pane, click **Client Administration** > **Client Settings**.

2. In the Messaging Domains area, to add a new domain:
   a. In **Add new Messaging Domain**, enter the new messaging domain name.
   b. Click **Add To List**.
3. In the Messaging Domains area, to remove a domain:
   a. In the **Messaging Domain List** box, select the messaging domain.
   b. Click **Delete Selected**.
4. On the Client - Device Certificate Policy page, configure the policy for the administration portal or the REST service by clicking the OAMP drop-down list and then choosing one of the following:
   - **NONE**: The server does not check for a certificate. The connection is established with or without a valid certificate.
   - **OPTIONAL**: The server requests a certificate. The connection is established with or without a certificate, but the process stops if a client provides an invalid or untrusted certificate, and the system returns the error code `HTTP 400`.
   - **OPTIONAL_NO_CA**: The server requests a certificate. The connection is established with any valid certificate even if the CA is untrusted, but the process stops if a client provides an invalid certificate, and the system returns the error code `HTTP 400`.
   - **REQUIRED**: The server requests a certificate. The server rejects a connection if a client fails to provide a valid certificate, and the system returns the error code `HTTP 400`.

   The default value is: **OPTIONAL**.
5. To set the policy from the configuration utility, enter the following command:

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

   where _value_ can be `off` (NONE) or `optional` (OPTIONAL or OPTIONAL_NO_CA) or `on` (REQUIRED).
6. Click **Save**.

Updating media size limits

Procedure

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

   You can update the size limit for the following types of attachments:
   - Video files
   - Audio files
   - Images
   - Text-based messages

- Other generic attachments

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

Updating feature entitlements

About this task

Feature entitlements determine privileges for Avaya Multimedia Messaging users.

Procedure

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

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

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

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

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

   ```
   Doe, John, john@doe.com
   jane@doe.com
   ```
5. Click **Apply**.

Related links

Licensing requirements on page 21

Feature entitlements field descriptions

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

Name	Description
WebLM Server	The WebLM Server is the license server hosting the Avaya Multimedia Messaging license. If the License Server Status is *Normal*, the license is correctly installed and the Avaya Multimedia Messaging server can communicate properly with the WebLM server.
Entitlement Status	Displays the current status and details of the license.
Entitlement Type	Displays the type of license with assigned value.

Table continues…

Name	Description
Validity	Displays the validity and can have one of the following values: • *VALID* if the license file is valid and the server can communicate with the WebLM Server. • *NO_LICENSE* if the license file cannot be found on the WebLM Server. • *EXPIRED* if install license file is expired. • *INVALID* if the license file on WebLM Server is invalid.
Expiry	Displays the date when the installed license file will expire.
Licensed	Displays the total number of available licenses.
Available	Displays the number of licenses still available for use.
Acquired	Displays the number of licenses currently acquired.

Updating enterprise directory settings

Procedure

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

   You populate the LDAP settings as part of the server configuration, but you can change the values of these settings with the administration portal. For a description of LDAP settings, see LDAP configuration on page 87.
3. Click **Test Connection** to verify your LDAP connection.
4. Under **User Synchronization Update Instructions**, set the rate at which the Avaya Multimedia Messaging server synchronizes with the users in your enterprise directory.
5. Click **Force LDAP Sync** to force an immediate user synchronization.

   Warning:

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

Configuring the LDAP attribute mappings

About this task

Use this procedure to configure LDAP attribute mappings.

Procedure

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

Managing trusted hosts

About this task

Use this procedure to add, edit, or delete the trusted host.

Procedure

1. In the Navigation pane, click **Server Connections** > **Trusted Hosts** and do one of the following:
   - To add a new host, click **Add** and type the details in the field.
   - To edit a host, select the host from the list and click **Edit**.
   - To delete a host, select the host name from the list and click **Delete**.
2. Click **Save**.

Managing federation gateway connections

About this task

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

Procedure

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

Adaptors are required for Presence Services and Lync federation configuration. For more information, see the links at the end of this procedure.

- Edit an existing adaptor.
- Delete an existing adaptor.

Related links

Configuring the XMPP interface in Avaya Multimedia Messaging for federation with Presence Services on page 132
Configuring the HTTPS REST interface in Avaya Multimedia Messaging for federation with Presence Services on page 133
Configuring SIP adapters on page 143

Verifying cluster nodes

About this task

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

Procedure

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

Cluster field descriptions

The following fields supply additional information about the cluster:

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

Generating performance data and statistics

About this task

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

Procedure

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

   You can generate the following types of data:

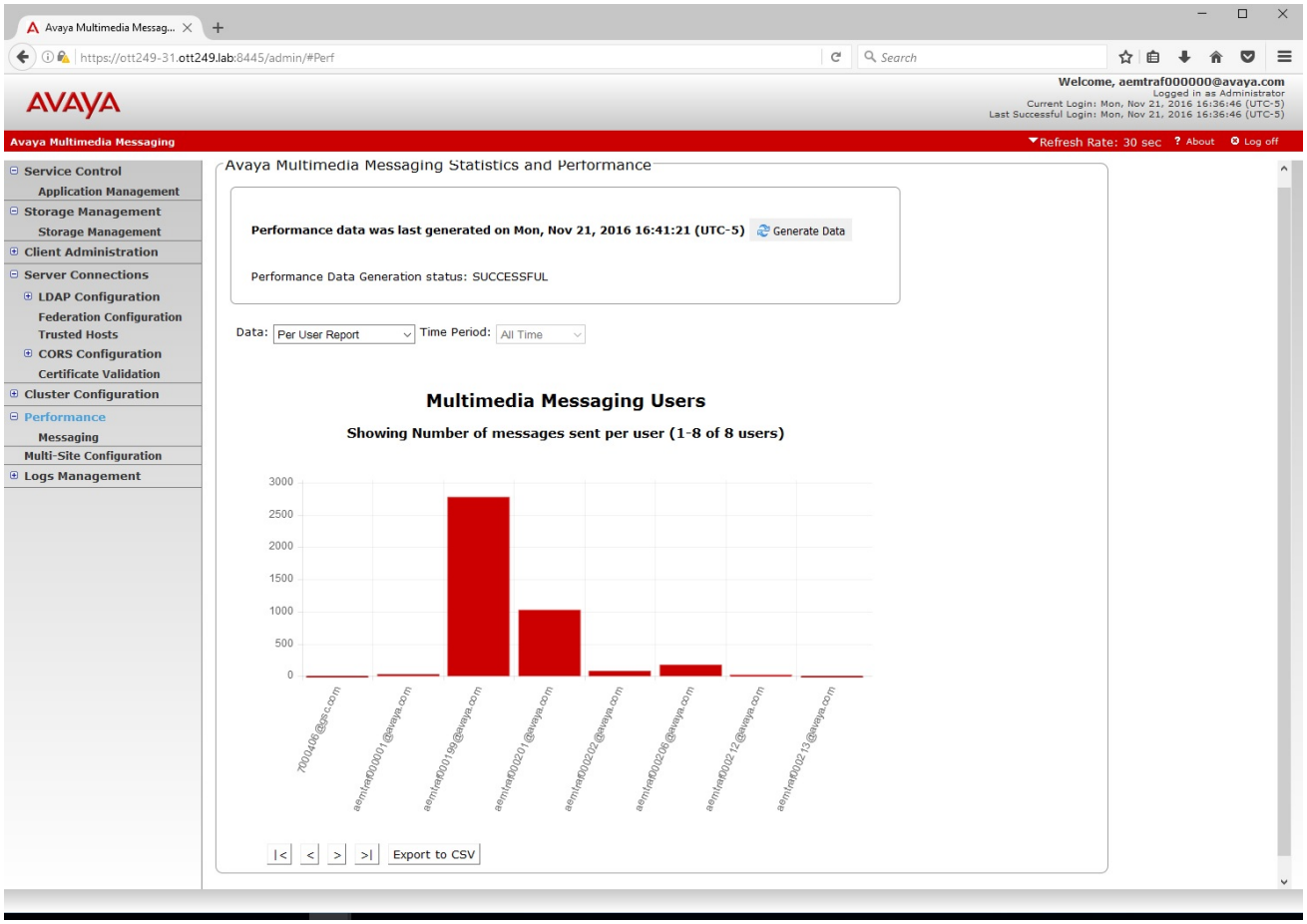
   - The number of Avaya Multimedia Messaging users.
   - Message traffic.
   - The number of messages sent per user.
   - Attachment breakdown with media types and size.
4. Select a time period.

Result

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

Example

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



Adding and editing local and remote sites for multisite configuration

About this task

Use this procedure to update the configuration of a local or remote site. For more information about multisite configuration, see Avaya Multimedia Messaging multisite adapter setup on page 207.

Procedure

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

Updating logging levels

About this task

Use the following procedure to select the level of detail that you want captured in log files. The “Finest” option provides the most detailed logs. The “Error” option produces the least detailed logs that only contain information about server errors.

Procedure

1. In the Navigation pane, click **Logs Management** > **Log Level**.
2. From the **Logger** drop-down menu, select the log type.
3. From the **Current logging level** drop-down menu, select the level of detail that you want captured in log files.

Adjusting the virtual hardware of virtual machines

When the Avaya Multimedia Messaging OVA is deployed, the resulting virtual machine has the following virtual hardware:

- 8 virtual CPUs with no CPU reservation.
- 8 GB of memory with no memory reservation.
- Three virtual disks:
  - The first disk is the system disk. It is 50 GB and hosts the boot partition, swap space, and the Linux partition.

- The second disk is the application disk. It is 25 GB and hosts the home directories, which are mounted at `/home`, and the application partition, which is mounted at `/opt/Avaya`.
- The third disk is the media disk. It is 10 GB and hosts the Cassandra database and media content, which are mounted at `/media/data`.

• One virtual network interface.

For the required adjustments to virtual hardware, see the guidelines in Installation on a VMware virtual machine on page 49. This section describes how to perform these adjustments.

Adjusting the memory resource of a virtual machine

About this task

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

Procedure

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

   ```
   sudo shutdown -h now
   ```

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

Adjusting the CPU resource of a virtual machine

About this task

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

Procedure

1. Perform steps 1 on page 191 to 3 on page 191.
2. From the Hardware tab, click **CPUs**.

3. In **Number of virtual sockets**, select the desired number of virtual CPUs for the virtual machine.
4. In **Number of cores per socket**, select **1**.
5. Click the **Resources** tab.
6. From **Settings**, click **CPU**.
7. In **Resource Allocation**, use the **Reservation** slider to set the desired CPU reservation.
8. Click **OK**.

Adjusting the virtual network interface

About this task

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

Procedure

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

Adjusting the size of virtual disks

About this task

This procedure describes how to adjust the size of the application-related virtual disks on an Avaya Multimedia Messaging virtual machine.

Before you begin

Delete all snapshots from the virtual machine. Disk sizes cannot be adjusted while snapshots exist.

Procedure

1. Perform steps 1 on page 191 to 3 on page 191.
2. From the Hardware tab, select the hard disk to be enlarged:
   - To increase the size of the application disk that hosts the disk volumes for the home directories and application software, click **Hard Disk 2**.
   - To increase the size of the media disk that hosts the disk volume for the database and media content, click **Hard Disk 3**.
3. In **Disk Provisioning**, enter a higher value for the disk size and select the appropriate unit of measure.

4. Click **OK**.
5. If a second disk needs to be increased in size, repeat steps 2 on page 192 to 4 on page 193 for that disk.

Next steps

Disk volumes located on virtual disks that have been enlarged need to be increased to make the space available to the running system. For more information, see Adjusting disk volumes using core Linux commands on page 195.

Adjustment of disk volume sizes

Use the procedures in this section to adjust the size of the disk volumes that are located on the virtual disks that have been increased in size. Perform this procedure during low traffic periods to minimize the chance of adverse impacts on system performance.

The R3.0.0.1 version of the Avaya Multimedia Messaging server provides a command that facilitates the management of disk volumes. To determine if the script is present on the system, type the following command:

```
app volmgt --help
```

If the command is recognized, then use the procedure in Adjusting disk volumes using app volmgt command on page 193. If the command is not recognized, then use the procedure in Adjusting disk volumes using core Linux commands on page 195.

Tip:

The above command is created during the process of logging into the Linux shell. Perform the above verification in a new login shell (new SSH session) after the Avaya Multimedia Messaging server has been installed.

Note:

Since migrations from R2.1 to R3.0 use the R3.0.0.0 version of the Avaya Multimedia Messaging, the above command will not be available, and the core Linux commands will therefore need to be used.

Adjusting disk volumes using “app volmgt” command

About this task

Use this procedure to adjust the size of the disk volumes using the disk volume management command that is provided by the R3.0.0.1 Avaya Multimedia Messaging server.

Before you begin

The virtual disks that host the volumes to be increased must first be increased in size. For more information, see Adjusting the size of virtual disks on page 192.

Procedure

1. If the virtual machine is not running, then power it up using the vSphere client graphical interface.

Note:

If this procedure is being done as part of the deployment of the OVA to a standalone ESXi host, the power up procedure will enter into the first boot sequence where the user is prompted for server-level configuration. Proceed through that configuration step before continuing with the next step of this procedure.

2. To scan the application and media disks for new storage made available for the increase if virtual disk size, run the following command: `app volmgt --scan`.

   Note:

   The above form of the command is an aliased version of the actual underlying command from the installed software load. The equivalent command from the software load is invoked as follows:

   ```
   sudo
   /opt/Avaya/MultimediaMessage/<version>/CAS/<version>/misc/volMgt.pl
   ```

   It is recommended to use the alias form of the command.

   Tip:

   For more information on this script and to get a list of invocation modes, run the command: `app volmgt --help`.

3. To generate a summary of the storage available for allocation on the second (application) and third (media) disks, as well as the current size of application related volumes, run the following command: `app volmgt --summary`.

   Note:

   - The application disk is reported as “sdb” and the media disk is reported as “sdc”.
   - Due to rounding differences from the underlying core Linux commands used by this script, the size of volumes reported under the `Allocated (LVM)` and `Allocated (Linux/df)` commands are often not exactly the same. The larger the volume is, the more these numbers deviate. Use them as a guide only. If in doubt, use the `--resize` argument to restart the volume resizing operation. After the `--status` argument indicates that the resize has completed, reinspect the numbers. If the numbers in these columns remain unaffected, then they are considered to be equal.

4. To allocate a specific amount of storage to a volume, run the following command:

   ```
   app volmgt -extend <volume> <number><unit>
   ```

   In these commands:

   - `<volume>` is one of either /opt/Avaya, /home, or /media/data.
   - `<number>` is an integer or decimal number that provides a storage increment.
   - `<unit>` is the unit of storage increment; specify m for megabytes, g for gigabytes, or t for terabytes.

Note:

- The amount of storage specified cannot exceed the available storage on the disk hosting the volume.
- The storage is taken from the available storage of the disk that hosts the volume.

5. To allocate all remaining available storage from a disk to one of its volumes, run the following command:

```
app volmgt -extend <volume> --remaining
```

Where `<volume>` is one of either /opt/Avaya, /home, or /media/data.

Note:

- For large increases in disk volume, the `resize2fs` operation can take a long time. To minimize issues with dropped SSH connections, the script always runs the `--extend` operation as a background process. The progress of the operation can be queried at any time using the `--status` argument. Alternatively, its progress can be monitored continuously using the `--monitor` argument. Use `Ctrl-C` to exit from the monitor command.
- If the `--resize` operation is unable to complete due to a server reboot, then the resizing operation can be restarted by running the following command: `app volmgt -extend`

Adjusting disk volumes using core Linux commands

About this task

Use this procedure to adjust the size of the disk volumes using core Linux commands.

Before you begin

The virtual disks that host the volumes to be increased must first be increased in size. For more information, see Adjusting the size of virtual disks on page 192.

Procedure

1. If the virtual machine is not running, then power it up using the vSphere client graphical interface.

   Note:

   If this procedure is being done as part of the deployment of the OVA to a standalone ESXi host, the power up procedure will enter into the first boot sequence where the user is prompted for server-level configuration. Proceed through that configuration step before continuing with the next step of this procedure.

2. Log in to the virtual machine as an administrator, then switch to the root user using the `su -` command.
3. If the application disk was increased in size, then continue with step 4 on page 196; otherwise, proceed to step 7 on page 196.

4. To make the newly allocated disk space available to the operating system, run the following command:

```
pvresize /dev/sdb
```

5. To extend the size of the application volume, mounted at `/opt/Avaya`, do one of the following:

   - Run the following command:

```
lvextend -L +<number><unit> /dev/mapper/application_vg-Avaya
resize2fs /dev/mapper/application_vg-Avaya
```

   - Alternatively, to extend the size using the remaining unallocated space on the second disk, run the following command:

```
lvextend -l +100%FREE /dev/mapper/application_vg-Avaya
resize2fs /dev/mapper/application_vg-Avaya
```

   Note:

   In these commands:

   - `<number>` is an integer or decimal number that provides a storage increment.
   - `<unit>` is the storage increment unit. Specify `m` for megabytes, `g` for gigabytes, or `t` for terabytes.
   - For large increases in disk volume, the `resize2fs` operation can take a long time. If the SSH session drops while this executes, establish a new session and repeat the command.

6. **(Optional)** Repeat one of the commands in the previous step to increase the size of the volume hosting directories, which are mounted at `/home`.

   Tip:

   Storage increases for `/home` directories are normally not required. Consider carefully the need to increase storage for this directory.

7. If the third disk, which is the media disk, was increased in size, do the following to make the newly allocated disk space available to the operating system:

   a. Run the following command:

```
pvresize /dev/sdc
```

   b. To extend the size of the media volume, mounted at `/media/data`, run the following command:

```
lvextend -l +100%FREE /dev/mapper/application_vg-Avaya
resize2fs /dev/mapper/application_vg-Avaya
```

   Note:

   For large increases in the disk volume, the `resize2fs` operation can take a long time. If the SSH session drops while this executes, establish a new session and repeat the command.

Scheduling periodic repairs of database inconsistencies

About this task

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

Procedure

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

   For example:

   ```
   crontab -e
   ```

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

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

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

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

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

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

   Note:

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

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

Logs and alarms

Logs

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

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

Alarms

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

Important:

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

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

Table 25: Avaya Multimedia Messaging alarms

Name	Description	Severity	Event code	SNMP OID
avESMComponentNotRunning	The system raises this alarm when a component has stopped functioning, does not start, or does not restart: • Cassandra • Nginx • Tomcat • Mobicents • snmpd • spiritAgent • glusterd/glusterfsd • keepalived • openfire	Major	OP_AMM-00010	enterprises.6889.2.65.0.10
avAMMLDAPServerConnectionLost	The system raises this alarm if the Avaya Multimedia Messaging application cannot connect to the corporate LDAP server. This alarm can be triggered manually by testing the LDAP connectivity through the Avaya Multimedia Messaging administration portal or as the result of an audit that is being performed every 60 seconds. The Avaya Multimedia Messaging application relies on the LDAP server for	Major	OP_AMM-00020	enterprises.6889.2.65.0.20

Table continues…

Name	Description	Severity	Event code	SNMP OID
	authentication, authorization and identity management.			
avAMMDataStoreAccessFailed	The system raises this alarm if the Avaya Multimedia Messaging application cannot connect to the database or the database cluster. This alarm is triggered by an audit process performed every 60 seconds.	Major	OP_AMM-00024	enterprises.6889.2.65.0.24
avAMMMediaStoreAccessFailed	The system raises this alarm if the Avaya Multimedia Messaging application cannot connect to the distributed file system, GlusterFS. This alarm is triggered by an audit process performed every 60 seconds. Under this alarm condition, the end users are only able to send text messages. Multimedia and generic attachments are rejected by the Avaya Multimedia Messaging server.	Major	OP_AMM-00026	enterprises.6889.2.65.0.26
avAMMDBStorageReachedCriticalThreshold	The system raises this alarm when the disk partition size where the Cassandra database is hosted exceeds 95% of the total size. The disk audit is performed every 60 minutes.	Critical	OP_AMM-00046	enterprises.6889.2.65.0.46
avAMMRESTCertificateFault	The system raises this alarm if the REST certificate is about to expire, has expired or if the application is unable to read the certificate file. The certificate audit is performed every 60 seconds.	Major	OP_AMM-00052	enterprises.6889.2.65.0.52
avAMMOAMCertificateFault	The system raises this alarm if the OAM certificate is about to expire, has expired or if the application is unable to read the certificate file. The certificate audit is performed every 60 seconds.	Major	OP_AMM-00054	enterprises.6889.2.65.0.54

Table continues…

Name	Description	Severity	Event code	SNMP OID
avAMMSIPCertificateFault	The system raises this alarm if the SIP certificate is about to expire, has expired or if the application is unable to read the certificate file. The certificate audit is performed every 60 seconds.	Major	OP_AMM-00058	enterprises. 6889.2.65.0.58
avAMMLicenseErrorModeActive	The system raises this alarm if one or more license errors are present.	Major	OP_AMM-00060	enterprises. 6889.2.65.0.60
avAMMLicenseRestrictedModeActive	The system raises this alarm if one or more license errors are present and the 30 day grace period has expired.	Critical	OP_AMM-00062	enterprises. 6889.2.65.0.62
avAMMRemoteDomainConnectionLost	The system raises this alarm if the Avaya Multimedia Messaging application is unable to ping one or more remote domains. The audit is performed every 30 seconds.	Major	OP_AMM-00064	enterprises. 6889.2.65.0.64
avAMMVirtualIPAcquiredFromPrimary	The system raises this alarm when the primary node hosting the virtual IP address of the application has stopped.	Major	OP_AMM-00066	enterprises. 6889.2.65.0.66
avAMMSMGRLDAPServerConnectionLost	The system raises this alarm if the application cannot establish connectivity with the Avaya Aura® System Manager LDAP server. This alarm can be triggered manually by testing the LDAP connectivity through the Avaya Aura® System Manager administration portal or as the result of an audit that is being performed every 60 seconds.	Major	OP_AMM-00068	enterprises. 6889.2.65.0.68
avAMMMediaStorageReachedWarningThreshold	The system raises this alarm when the disk partition size where the media files are stored exceeds 90% of the total size. The disk audit is performed every 60 minutes.	Minor	OP_AMM-00070	enterprises. 6889.2.65.0.70

Table continues…

Name	Description	Severity	Event code	SNMP OID
avAMMMediaStorageReachedCriticalThreshold	The system raises this alarm when the disk partition size where the media files are stored exceeds 95% of the total size. The disk audit is performed every 60 minutes.	Critical	OP_AMM-00072	enterprises.6889.2.65.0.72
avAMMTimeServerSynchronizationLost	The system raises this alarm if the Avaya Multimedia Messaging application does not have time synchronization with one or multiple NTP servers. An audit is performed every 60 seconds.	Major	OP_AMM-00074	enterprises.6889.2.65.0.74
avAMMNodeCertificateFault	The system raises this alarm if the node certificate is about to expire, has expired or if the Avaya Multimedia Messaging application is unable to read the certificate file. The certificate audit is performed every 60 seconds.	Major	OP_AMM-00076	enterprises.6889.2.65.0.76
avAMMPPMConnectionLost	The system raises this alarm if the Avaya Multimedia Messaging application cannot connect to the PPM service on the Session Manager. This alarm is cleared if the connection is re-established.	Major	OP_AMM-00078	enterprises.6889.2.65.0.78
avAMMMSExchgConnectionLost	The system raises this alarm if the Avaya Multimedia Messaging application cannot connect to the Microsoft Exchange, either because the connection cannot be made or because the delegate account credentials are rejected. This alarm is cleared if the connection is re-established.	Major	OP_AMM-00080	enterprises.6889.2.65.0.80
avAMMMultiSiteConnectionLost	The system raises this alarm if the Avaya Multimedia Messaging application cannot connect to one or more remote sites in a multisite configuration.	Major	OP_AMM-00084	enterprises.6889.2.65.0.84

Table continues…

Name	Description	Severity	Event code	SNMP OID
	This alarm is cleared if the connection is re-established.			
avAMMUserLicensesUnavailable	The system raises this alarm when it automatically assigned all available rich media feature entitlements. The system no longer assigns automatically feature entitlements.	Major	OP_AMM-00086	enterprises.6889.2.65.0.86
avAMMUserLicensesThresholdReached	The system raises this alarm when it assigned 90% of available rich media feature entitlements.	Minor	OP_AMM-00088	enterprises.6889.2.65.0.88
avAMMCertificateAuthorityCertificateAlarmRaised	The system raises this alarm if the certificate authority certificate is about to expire, has expired or if the application is unable to read the certificate file. The certificate audit is performed every 60 seconds.	Major	OP_AMM-00090	enterprises.6889.2.65.0.90
avSIPAdapterContactLostAlarmRaised	The system raises this alarm if the Avaya Multimedia Messaging application cannot connect to either the Lync server or the Session Manager for interoperability with Lync. This alarm is cleared if the connection is re-established.	Major	OP_AMM-00092	enterprises.6889.2.65.0.92

Preventing the creation of audit audispd logs on a physical server

About this task

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

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

Procedure

1. Open the `/etc/audisp/plugins.d/syslog.conf` file using a text editor and then replace the `LOG_INFO` text with `LOG_LOCAL0`.

2. Open the `/etc/syslog.conf` file, and in line number 42, add `local0.none` to the first part of the line as follows:

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

Integrated Windows Authentication support

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

Use the following sections to complete IWA configuration on the Avaya Multimedia Messaging and Active Directory servers. Errors in the setup might cause the authentication to fail. You can enable debug logs to assist with troubleshooting.

Authentication prerequisites

You must have the following to set up IWA:

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

Important:

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

Setting up the Windows Domain Controller

About this task

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

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

Important:

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

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

Before you begin

Review Authentication prerequisites on page 203.

Procedure

1. Create a new IWA service account.

   Do not select an account associated with an existing user.

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

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

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

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

   Important:

   - If you are using Active Directory 2003, you must use `setspn -A` instead of `setspn -S`.
   - When you use `setspn -S`, the Active Directory server searches for other users with the same SPN assigned. If the server finds a duplicated SPN, see step 3 on page 204.

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

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

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

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

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

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

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

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

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

Windows Domain Controller command descriptions

Setting up the Windows Domain Controller on page 203 uses the following command values:

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

Setting up IWA on the Avaya Multimedia Messaging administration portal

About this task

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

Procedure

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

If this field is not set to `userPrincipalName`, you might encounter license issues and other unpredictable behavior.

d. Ensure that the other settings are appropriate for the LDAP configuration of your Domain Controller.

Important:

The LDAP server that you use must be the domain controller with the appropriate Active Directory version as the server type.

3. In the Configuration for Windows Authentication area, complete the following information using the same values you provided when setting up the Windows Domain Controller:

   a. In **Service Principal Name (SPN)**, type `HTTP/<FRONT—END FQDN>`.

   For example, `HTTP/amm.example.com`.

   b. Click **Import** to import the `tomcat.keytab` file transferred from the Windows Domain Controller.

   In cluster deployments, the file is transferred to all nodes in the cluster. An additional option is available to send the file to specific nodes in a cluster.

   c. In **Kerberos Realm**, type the Kerberos realm, which is usually in all uppercase letters. For example, `EXAMPLE.COM`.

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

   For example, `example.com`.

   e. **(Optional)** Select the **Use SRV Record** check box.

   f. **(Optional)** If **Use SRV Record** is not selected, in **KDC FQDN**, type the FQDN of the Domain Controller.

   This value also includes the DNS domain at the end. For example, `ad.example.com`.

   g. **(Optional)** In **KDC Port**, retain the default value of 88.

   This field is only visible if **Use SRV Record** is not selected.

   h. **(Optional)** In a cluster deployment, click **Send Keytab File** to send the `tomcat.keytab` file you imported in step 3.b on page 206 to a specific node.

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

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

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

Related links

Windows Domain Controller command descriptions on page 205
Working with the Avaya Multimedia Messaging administration portal on page 182

Avaya Multimedia Messaging multisite adapter setup

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

Connector types for the Avaya Multimedia Messaging adapter

The multisite adapter uses the following types of connectors:

Conversation ID connector

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

Messages connector

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

Message Parts connector

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

Home site ID

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

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

Note:

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

Multisite adapter field descriptions

The multisite adapter is configured for every Avaya Multimedia Messaging site. The adapter is only active if local site and remote site information is provisioned. For information about adding and editing local and remote sites, see Adding and editing local and remote sites for multisite configuration on page 190.

The following table describes the multisite adapter configuration fields:

Field	Description
Name	The Site ID. Each site must have a local site ID with at least one remote site ID. The site ID is a valid IM Gateway provisioned in System Manager. The local Site ID of one site must match a remote site ID on the remaining sites.
Address	The FQDN of the cluster or standalone server. The local address of one site must match the remote address on the remaining sites.
Port	The default port used by the Avaya Multimedia Messaging multisite adapter is 8441.
Status	This field displays the status of the connection to the remote site, and it can not be edited.
Enabled	A checkbox that indicates whether a connector is created. If the checkbox is selected, a connector is created to connect to the remote site and the interface displays `yes`. If the checkbox is not selected, no connector is created and the interface displays `no`.
Timeout	The connection alarm timeout in seconds. If a problem occurs with the connection to the remote site, the connector tries to establish a connection five times before raising an alarm. The timeout value represents the time duration between retries before the alarm is raised. This timeout allows for flexibility if different network characteristics exist between remote sites.
Long Poll Timeout	The menu that contains the **Recommended Long Poll Timeout** configuration option. Use this option for setting the value to use in the Avaya-Request-Timeout HTTP header for long-poll requests. **Important:** The long poll timeout value can be from 30 to 120. Lowering this value results in increased traffic on the server, but network configuration may require that you set a lower value. If you do not configure this parameter, the default database initialization setting is used.

Backup and restore

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

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

Important:

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

Warning:

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

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

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

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

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

Note:

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

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

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

Important:

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

Related links

Making a backup for an Avaya Multimedia Messaging node on page 210
Restoring an Avaya Multimedia Messaging node in a standalone deployment on page 211
Restoring a node from a cluster on page 212
Restoring a cluster on page 213
Lync recovery on page 216

Making a backup for an Avaya Multimedia Messaging node

About this task

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

Before you begin

Before you begin the backup of the Avaya Multimedia Messaging server, you must ensure that:

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

  You can configure SSH access by running the Avaya Multimedia Messaging configuration utility and selecting **Cluster Configuration** > **Configure SSH RSA Public/Private Keys**.
- You have the Cassandra database username and password. You will require this information if you are backing up database content.

Procedure

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

   For example:

   ```
   /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/bin/backupAMM.sh -d
   /home/avaya/backup backup2014_02_02
   ```

   In this example, the parent directory for the backup is /home/avaya/backup and backup2014_02_02 is the backup file that contains the content copied from the Avaya Multimedia Messaging server on February 2, 2014.

   If you do not provide a backup name, the backup name is generated automatically as a combination of the host name and the date and timestamp.

Example

Related links

Backup and restore on page 209
Backup command options on page 211

Backup command options

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

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

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

Related links

Making a backup for an Avaya Multimedia Messaging node on page 210

Restoring an Avaya Multimedia Messaging node in a standalone deployment

About this task

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

Before you begin

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

Procedure

1. Run the Avaya Multimedia Messaging server installation command.

   For example:

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

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

3. Proceed with the Avaya Multimedia Messaging installation.

Note:

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

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

   For example:

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

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

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

6. Start the Avaya Multimedia Messaging server.

   ```
   service AMMService start
   ```

Related links

Backup and restore on page 209

Restoring a node from a cluster

About this task

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

Before you begin

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

Procedure

1. Run the Avaya Multimedia Messaging server installation command.

   For example:

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

2. In the **General Configuration** menu, configure the following settings to `n` (no):

   - **Configure Gluster**
   - **Enable Cassandra DB initialization**

3. Proceed with the Avaya Multimedia Messaging installation.

   Note:

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

4. Run the restoreAMM command with the path to the restore file or directory as a parameter.

For example:

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

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

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

6. Restore the Gluster file system.

   The procedure that you must use depends on whether the Avaya Multimedia Messaging node was removed from the cluster or if the node is not functional.

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

8. Run the Cassandra repair command:

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

Next steps

Reestablish the alarm connection to System Manager.

Related links

Backup and restore on page 209

Restoring a cluster

About this task

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

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

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

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

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

Important:

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

Before you begin

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

Procedure

1. Run the Avaya Multimedia Messaging server installation command.

   For example:

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

2. In the **Advanced Configuration** menu, configure the following settings:

   - **Configure Gluster**:
     - set to `y` (yes) for the first node of the cluster.
   - **Enable Cassandra DB initialization**: set to `n` (no).

3. Proceed with the Avaya Multimedia Messaging installation.

   Note:

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

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

   For more information about installing additional nodes, see Installing an additional node on page 69.

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

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

   For example:

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

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

   Note:

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

8. On every node in the cluster, restore the Gluster file system.

   The procedure that you must use depends on whether the Avaya Multimedia Messaging node was removed from the cluster or if the node is not functional.

9. **(Optional)** On the last node that you are restoring, restart the Openfire server.

   ```
   sudo service AMMOpenfire restart
   ```

   Perform this step if Avaya Multimedia Messaging is federated with Presence Services.

   Warning:

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

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

```
service AMMService start
```

11. Run the Cassandra repair command:

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

Next steps

Reestablish the alarm connection to System Manager.

Related links

Backup and restore on page 209
Removing a Gluster configuration on page 215
Restoring Gluster after Gluster is properly removed on page 216

Removing a Gluster configuration

About this task

This procedure describes how to remove a Gluster configuration after a system malfunction, without properly decommissioning the corresponding Avaya Multimedia Messaging node.

Procedure

1. Ensure that Avaya Multimedia Messaging Recovery Manager is not running.

```
$ /sbin/service AMMRecoveryManager stop
```

2. Stop glusterd, glusterfsd, and any other Gluster brick processes that are running.

   For example:

```
umount /opt/Avaya/MultimediaMessaging/<version>/content_mount;
service glusterd stop;
service glusterfsd stop;
pkill -f  "/usr/sbin/glusterfs -s localhost";
rm -fr /var/lib/glusterd/;
rm -fr /media/data/content_store/brick*
```

3. Install the Avaya Multimedia Messaging node to use for restoring the node that has malfunctioned.
4. During the installation of the Avaya Multimedia Messaging server, restore the Gluster configuration.

   Note:

   You must configure the Gluster file system before you start restoring the Avaya Multimedia Messaging node.

   While the Gluster file system is restored, you must not start the AMMService process.

Related links

Restoring a cluster on page 213

Restoring Gluster after Gluster is properly removed

About this task

This procedure describes how to restore a Gluster configuration after properly removing Gluster from an Avaya Multimedia Messaging node.

After Gluster is properly removed from a node, the bricks on the remaining active nodes still have all the data, redundantly backed up.

A proper removal of Gluster from a node consists of removing all the bricks that are paired with the node.

Procedure

1. In the CLI of each active node, run the following command to identify and remove the brick directories to remove:

```
sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/glusterfs/
configGluster.sh -v
```

2. Start Gluster on the node that you restore.

```
sudo service glusterd start
```

3. Run the **`gluster peer probe`** command from one of the active nodes to rejoin the restored node.

```
sudo gluster peer probe <IP address or restored node>
```

4. Run the **`configGluster.sh`** command to auto-configure the bricks in the cluster.

   You must provide the IP address of another active node from the cluster as a parameter:

```
sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/glusterfs/
configGluster.sh -a <IP address of active node>
```

5. Run the **`glusterfsMount.sh`** script to mount the Gluster file system.

```
sudo /opt/Avaya/CAS/<version>/glusterfs/glusterfsMount.sh/opt/Avaya/
MultimediaMessaging/<version>/CAS/<version>/glusterfs/glusterfsMount.sh
```

Next steps

If you restore the Gluster file system as part of an Avaya Multimedia Messaging node recovery procedure, continue with the steps described in Restoring a node from a cluster on page 212.

Related links

Restoring a cluster on page 213

Lync recovery

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

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

Administration tools

Table 26: Administration tools for the Avaya Multimedia Messaging server

Category	Name	Description
GlusterFS tools	gluster	The Command Line utility of the Gluster File System, Gluster Console Manager. You can use this utility to check the distributed file system status for remote nodes.

Table continues…

Category	Name	Description
		For usage instructions, see the Gluster manual.
Java tools	jconsole	JConsole uses the extensive instrumentation of the Java Virtual Machine (Java VM) to provide information about the performance and resource consumption of applications running on the Java platform. You can use jconsole to monitor the following components: • Tomcat • Mobicents • Cassandra • Serviceability Agent (aka spiritAgent) For more information about using the jconsole utility, see the Oracle documentation. **Important:** JConsole is a graphical tool and can be run locally from an Avaya Multimedia Messaging node that has a graphical desktop environment installed.
Cassandra database tools	nodetool	The nodetool utility provides usage information about the Cassandra database nodes. For usage instructions, see the Cassandra database documentation.
Avaya Multimedia Messaging tools	clitool.sh	A tool that has multiple usage possibilities. The parameters specified in the command determine the usage of the clitool utility. Run the clitool utility with the dailyReport as a parameter to generate reports for the current day.
	cleanAMM.sh	The CleanAMM utility must be run on a regular basis, immediately after performing a backup, to remove closed conversations. The cleaner tool creates additional disk space by deleting the oldest closed conversations until the amount of free disk space is less than 75% of the hard disk capacity. The results of the cleaning operation are stored in the `logs/cleaner_CLF.log` file. If the cleaner tool cannot free enough disk space, you can use the web-based administration portal to change the number of days that idle conversations remain open.
	collectLogs.sh	Copies the logs from an Avaya Multimedia Messaging node to a file or to a directory specified as parameters in the command.
	collectNodes.sh	Copies the logs from all the nodes in an Avaya Multimedia Messaging cluster to the file specified in the command.
	perfLogViewer.sh	A tool for reading performance logs.

Table continues…

Category	Name	Description
		The perfLogViewer tool must be used only for first-level support. **Important:** perfLogViewer is a graphical tool and can be run locally from an Avaya Multimedia Messaging node that has a graphical desktop environment installed.
	statusAEM.sh	A tool that displays the status of the Avaya Multimedia Messaging server and of the related services. Use the statusAEM tool to verify that the Avaya Multimedia Messaging is installed properly and that the services are running. The statusAEM.sh script is located in the `/opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/bin/` directory.
Linux tools	ping	Sends an ICMP ECHO_REQUEST to network hosts.
	nslookup	Queries the internet servers interactively.
	ip	Displays and manages routing devices, policy routing and tunnels. You can use this command to identify nodes that have a virtual IP address.
	ethtool	Queries and manages network driver and hardware settings. You can use this command to confirm that the physical network adapter is enabled and available.
	wget	Downloads files from the Web. You can use this tool to perform resource discovery for a user.
	curl	Transfers a URL.

Related links

gluster volume status on page 219
nodetool on page 220
cleanAMM on page 221
clitool on page 222
collectLogs on page 223
collectNodes on page 223

gluster volume status

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

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

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

Related links

Administration tools on page 217

Usage example

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

nodetool

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

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

Related links

Administration tools on page 217

Usage example

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

For example:

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

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

Important:

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

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

```
[root@amm-1 logs]# /opt/Avaya/MultimediaMessaging/<version>/cassandra/1.2.7/bin/nodetool -
u cassandra_username -pw Cassandra_password repair
[2014-07-04 08:49:01,128] Starting repair command #1, repairing 256 ranges for keyspace
cas_common_data
[2014-07-04 08:49:04,465] Repair command #1 finished
[2014-07-04 08:49:04,492] Starting repair command #2, repairing 256 ranges for keyspace
amm_data
[2014-07-04 08:49:07,756] Repair command #2 finished
[2014-07-04 08:49:07,781] Starting repair command #3, repairing 256 ranges for keyspace
acs
[2014-07-04 08:49:11,015] Repair command #3 finished
[2014-07-04 08:49:11,024] Nothing to repair for keyspace 'system'
[2014-07-04 08:49:11,030] Starting repair command #4, repairing 256 ranges for keyspace
openfire
[2014-07-04 08:49:11,205] Repair command #4 finished
[2014-07-04 08:49:11,229] Starting repair command #5, repairing 256 ranges for keyspace
sip_notification_cql
[2014-07-04 08:49:14,468] Repair command #5 finished
[2014-07-04 08:49:14,492] Starting repair command #6, repairing 256 ranges for keyspace
amm_notification
[2014-07-04 08:49:17,727] Repair command #6 finished
[2014-07-04 08:49:17,751] Starting repair command #7, repairing 256 ranges for keyspace
amm_system
[2014-07-04 08:49:21,005] Repair command #7 finished
[2014-07-04 08:49:21,029] Starting repair command #8, repairing 256 ranges for keyspace
amm_federation
[2014-07-04 08:49:24,507] Repair command #8 finished
[2014-07-04 08:49:24,535] Starting repair command #9, repairing 256 ranges for keyspace
clusteradmin
[2014-07-04 08:49:27,776] Repair command #9 finished
[2014-07-04 08:49:27,785] Starting repair command #10, repairing 256 ranges for keyspace
system_auth
[2014-07-04 08:49:27,966] Repair command #10 finished
[2014-07-04 08:49:27,990] Starting repair command #11, repairing 256 ranges for keyspace
SIP_Notification
[2014-07-04 08:49:31,249] Repair command #11 finished
[2014-07-04 08:49:31,258] Nothing to repair for keyspace 'system_traces'
[2014-07-04 08:49:31,300] Starting repair command #12, repairing 256 ranges for keyspace
amm_schema_version
[2014-07-04 08:49:34,182] Repair command #12 finished
[2014-07-04 08:49:34,190] Starting repair command #13, repairing 256 ranges for keyspace
OpsCenter
[2014-07-04 08:49:34,352] Repair command #13 finished
```

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

cleanAMM

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

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

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

Related links

Administration tools on page 217

Usage example

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

---

clitool

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

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

Related links

Administration tools on page 217

Usage example

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

For example:

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

Note:

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

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

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

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

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

```
amm_user000007@avaya.com,                0.00,                    0,                0
amm_user000008@avaya.com,                0.00,                    0,                0
amm_user000009@avaya.com,                0.00,                    0,                0
amm_user000010@avaya.com,                0.00,                    0,                0
```

collectLogs

The **collectlogs** utility copies the logs from an Avaya Multimedia Messaging node to a file or to a directory specified as parameters in the command.

Related links

Administration tools on page 217

Usage examples

- **$ collectLogs.sh -n 2 archive_file**: creates an archive called `archive_file.tar.gz` with each of the log files to a count of two, under the current working directory. The two log files are AMM.log and AMM.log.1. To create the file in a different directory, add the path to the archive file as a prefix to the file name.
- **$ collectLogs.sh -d /tmp/ -n 2** : copies the log files to the `/tmp` directory with each of the log files to a count of two.
- **$ collectLogs.sh -d /tmp/ -n 2 archive_file**: copies the log files to the `/tmp` directory with each of the log files to a count of two. The -d parameter overrides the current `archive_file` and the `archive_file` is ignored.

collectNodes

The collectNodes.sh utility creates an archive with logs collected from the Avaya Multimedia Messaging cluster nodes.

The archive is created in the current working directory.

Warning:

Numerous log files from multiple cluster nodes can occupy a high amount of disk space. Before running the command, ensure that the current node has enough free space.

Usage examples

$ collectNodes.sh [-n <no_of_logs>] [h] <archive_name>

For example:

```
$ collectNodes.sh -n 2 archive_file.tar.gz
```

Creates an archive called archive_file.tar.gz with each of the log files to a count of two, under the current working directory. The two log files are AMM.log and AMM.log.1. To create the file in a different directory, add the path to the archive file as a prefix to the file name

Related links

Administration tools on page 217

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.

   Sudo `/opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/bin/configureAMM.sh`
3. Select **Front-end host, System Manager and certificates configuration** and edit the System Manager FQDN and enrollment password.
4. Open the Avaya Multimedia Messaging administration portal and navigate to **Server Connections** > **LDAP Configuration** > **System Manager**.
5. Edit the System Manager address and click **Save**.

Archiving

About this task

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

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

Before you begin

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

To preserve the conversations for long-term usage, you must perform a backup of the Avaya Multimedia Messaging server periodically.For more information about backups, see Backup and restore on page 209.

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

Procedure

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

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

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

```
use AMM_Data;
```

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

   For example:

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

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

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

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

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

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

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

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

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

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

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

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

     Warning:

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

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

```
h:amm_data> select messageid, body, subject, fromaddr, toaddr from messages
where conversationid='fe7a4904-5e13-4fb3-adc5-58546002c584' and
```

```
timestamp>'2014-06-24' and timestamp<'2014-06-25' and subject='subject1' allow
filtering;
```

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

```
quit;
```

Enabling and disabling TLS versions

About this task

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

Warning:

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

Perform this procedure on both the master and backup virtual IP nodes.

Procedure

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

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

   - To disable previous TLS versions:

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

   In these commands, `<version>` is the Avaya Multimedia Messaging build version you are using.

2. Run `sudo service AMMNginx reload` to reload Nginx.

   This step will not cause a service outage.

Avaya Multimedia Messaging upgrades and migrations

You can upgrade from one version to another within an Avaya Multimedia Messaging release. You must perform a migration to move to a new major release, and the operating system is changed as part of the process.

If you are migrating to a Service Pack (SP), such as Release 3.0.0.1, you must first migrate to the major release (3.0) and then upgrade to the latest SP.

Note:

When performing an upgrade, you can roll back to the previously installed Avaya Multimedia Messaging version.

The rollback feature is not supported for migrations. Instead, you must take a backup and use it to restore data.

Related links

Avaya Multimedia Messaging migration on page 227
Restoring Avaya Multimedia Messaging to the previous version if you abort migration on page 239
Migration of the Avaya Aura environment on page 240
Upgrading the Avaya Multimedia Messaging server on page 242
Checking for DRS synchronization after a migration or upgrade on page 245
Applying patches on page 245

Avaya Multimedia Messaging migration

The process to migrate from a previous release (such as R2.1.x) to R3.0 involves three main phases:

- In the first phase, preparation for the migration is performed on the cluster for the previous release.
  - Configuration values are gathered from the existing server. These values are used when preparing the servers in phase 2.
  - Avaya Multimedia Messaging backups are taken and moved to off-board locations.
  - A script from R3.0 is run to extract the required configuration data from the previous release.
  - Logs and home directory content are moved off-board.
- In the second phase, the cluster is prepared by re-installing the disk partitions and volumes that host the operating system and home directories.
  - For physical servers, this is performed on the server, leaving the media disk volume hosting the Cassandra database and media content preserved.
  - For virtual servers, this is performed by deploying R3.0 OVAs for each node in the cluster and moving the virtual disks hosting the Cassandra database and media content from the previous release to R3.0.

  The disk volumes hosting R3.0 application are left in a clean state in preparation for the third phase.
- In the third phase, the migration is completed by installing R3.0, running a script to convert Cassandra data from the previous release to the appropriate format for R3.0, then running a script to complete all remaining upgrade steps.

Important:

- Perform a migration between major releases only if you fully understand the risks and the implications of this procedure. Otherwise, contact Avaya Support.
- Use the same host name and IP address for the newly deployed physical server operating system and virtual machine OVA.
- In Release 2.1.x, Avaya Multimedia Messaging and System Manager users could be correlated if the Emailaddress mapping in Avaya Multimedia Messaging was mapped to the same attribute as the Loginname in System Manager.

  As of Release 3.0, this correlation method is not supported. The correlation must be done by comparing one of the following:

  - The Emailaddress mapping in Avaya Multimedia Messaging with the Microsoft Exchange address or other email addresses in System Manager.
  - The System Manager login name mapping in Avaya Multimedia Messaging with Loginname in System Manager.

  To avoid any service interruptions after an upgrade, ensure that you meet this new criteria for correlation.

Note:

Relocating the media (third) virtual disk for migrations involving virtual machines can take up to several hours. The following is an example of a large media disk.

```
$ df -h /media/data
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/vg_media-lg_media
                      4.9T  1.4T  3.3T  29% /media/data
```

For example images showing the migration process in vCenter, see Example images of the Avaya Multimedia Messaging migration process on page 278.

Note:

For the purposes of brevity, the three phases of the migration are described in the context of an Avaya Multimedia Messaging cluster. If you are working with a standalone Avaya Multimedia Messaging server, then the references to other nodes in the cluster can be ignored.

Preparing the server for migration (phase 1)

About this task

Use this procedure to prepare to migrate a cluster to the latest release. This procedure applies to both physical server and virtual machine clusters.

Procedure

1. Take a backup of the cluster to off-board NFS-mounted storage or external disk drives.

   For more information, see Backup and restore on page 209.

2. Log in to the shell of the seed node.

3. Run `collectNodes.sh` and copy the collected logs to the off-board storage.
4. Copy the content from the home directories to the off-board storage.
5. If you are using a physical server, then run the following command to determine the UID and GID values for the ammapp user, and record for use in phase 2:

   ```
   id ammapp
   ```

6. Run the following command to create a configuration-only backup of the existing system into the `/media/data/backup/migrate_<hostname>` directory:

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

   Type `No` when you are prompted about including media files in the backup.

   Important:

   The above command assumes that the mount point for the media data disk volume is `/media/data`. This is the case for virtual servers, and is the default for physical servers. If a physical server is using a different mount point, then replace `/media/data` in the above command with the mount point for that server's media disk. To determine the mount point for a physical server, issue the mount command, and inspect the output for the directory associated with the `/dev/sdb1` partition or its equivalent for that server.

7. Transfer the installer file for R3.0, `amm-<new release>.bin`, to the home directory of the ammapp user on the system for the previous release.
8. Log in as the ammapp user and run the following command:

   ```
   chmod 777 amm-<new release>.bin
   ./amm-<new release>.bin --tar xf -- ./migrateConfig.sh
   chmod 777 migrateConfig.sh
   sudo ./migrateConfig.sh
   ```

   Important:

   If the command `./migragteConfig.sh` is skipped or fails to complete successfully, all gluster configuration and data is lost. Do not proceed until the `migrateConfig.sh` script completes successfully.

9. Run the following commands to stop the Avaya Multimedia Messaging service and to verify that services are stopped:

   ```
   service AMMService stop
   service AMMService status
   ```

10. To determine the fully qualified host name for the Avaya Multimedia Messaging server, run the following command in the Linux shell, and record for use in phase 2:

    ```
    hostname
    ```

11. To determine the IP address and network mask, run the following command, and record for use in phase 2:

    ```
    ifconfig -a| grep inet | grep -v 127.0.0.1
    ```

12. To determine the default gateway, run the following command, and record for use in phase 2:

    ```
    netstat -nrv | grep "^0.0.0.0"
    ```

13. To determine the DNS search list and DNS server IP addresses, run the following command, and record for use in phase 2:

    ```
    cat /etc/resolv.conf
    ```

14. To determine the NTP server IP addresses, run the following command, and record for use in phase 2:

    ```
    cat /etc/ntp.conf | grep "^restrict" | grep mask
    ```

15. To determine the time zone, run the following command, and inspect the target of the symbolic link, and record for use in phase 2:

    ```
    ls -l /etc/localtime
    ```

16. Repeat steps 4 on page 229 through 15 on page 230 for each remaining node in the cluster.

Next steps

Do one of the following:

- If you are working with virtual machines, continue with preparing the virtual machines. For more information, see Preparing the virtual server (phase 2 option 1) on page 230.
- If you are working with physical servers, continue with preparing the physical servers. For more information, see Preparing the physical server for migration (phase 2 option 2) on page 234.

Preparing the virtual server (phase 2 option 1)

About this task

Use this procedure to deploy and prepare R3.0 for the third phase of migration, the media disk that is deployed by default for each virtual machine R3.0 is removed and replaced with the virtual disk from the corresponding previous release.

In the absence of virtual machine snapshots, each virtual disk of a virtual machine is represented by two files on the file system of the ESXi hypervisor.

- The virtual disk file ending in `-flat.vmdk` contains the data stored on the virtual disk.
- The virtual disk file ending in `.vmdk` file contains meta data that describes the virtual disk.

When viewing the data store from the VMware client, the disk appears in the interface as a single object with the `.vmdk` extension. The `-flat.vmdk` file is normally not visible. When a snapshot of a virtual machine is taken, a new delta file is created for each virtual disk. These delta files store disk changes that occur, on each respective disk, after the point in time when the virtual machine snapshot is created. VMware does not support the movement of a virtual disk from one virtual machine to another when these delta files are present. To perform this procedure, virtual machine snapshots cannot be present on either the previous or virtual machine R3.0.

Each Avaya Multimedia Messaging virtual machine has three virtual disks and their files, which are on the file system of the ESXi hypervisor host. These disks and their files are:

- `<vm-name>.vmdk, <vm-name>-flat.vmdk`

This is the first virtual disk, referred to as the system disk. It contains the virtual machine's bootstrap files, swap space, and operating system partition.

- `<vm-name>_1.vmdk, <vm-name>_1-flat.vmdk`

  This is the second virtual disk, referred to as the application disk. It contains the disk volumes for home directory storage and for the installed application.

- `<vm-name>_2.vmdk, <vm-name>_2-flat.vmdk`

  This is the third virtual disk, referred to as the media disk. It contains the disk volume that stores database files and media content.

During the migration process, the media disk is moved from the previous release to the virtual machine for R3.0, replacing the default media disk that is deployed with R3.0.

Before you begin

Ensure that the preparation for the migration of the previous release has been completed. For more information see Preparing the server for migration (phase 1) on page 228.

Procedure

1. Deploy a current OVA release for the seed node, using the server configuration information gathered from the previous system release.

   This configuration is limited to the operating system configuration, such as the host name, IP address, and NTP settings. Updates to the virtual hardware of the virtual machine are left until a later step in this procedure.

   Tip:

   Give R3.0 the same base name as the previous one, but make the name unique by suffixing it with the current string version. Alternatively, if the name of the previous release already had a version number string embedded, then replace that version number string with the current string version. This is referring to the name of the virtual machine as seen on the VMware interface, and is not the host name at the Linux login prompt level. The host name must remain the same as that recorded from the previous release.

2. Log in to the current system and shut down the operating system using the command:

   ```
   sudo shutdown -h now
   ```

   Important:

   If the above command does not shut down the virtual machine, then manually shut it down using the VMware interface.

3. Delete the third virtual disk, labeled SCSI(0:2), from the virtual machine for R3.0, deleting the files associated with that virtual disk from the file system of the hypervisor.

   a. Using the VMware client, click **Edit Settings**.

   b. Click **Hard disk 3** and then confirm that the disk has the virtual device node SCSI (0:2).

   c. Click **Remove** and then **Remove from virtual machine**.

   d. Select **Remove from virtual machine and delete files from disk**.

   e. Click **OK**.

4. Log in to the previous release's virtual machine and shut down the operating system using the command:

```
sudo shutdown -h now
```

   Important:

   If the above command does not shut down the virtual machine, then manually shut it down using the VMware interface.

5. Delete any existing snapshots from the previous release's virtual machine:

   a. Using the virtual machine interface, select **Snapshot** > **Snapshot Manager** for the virtual machine.

   b. If there are any snapshots, then click **Delete All** and then **Yes** when you are prompted to confirm.

   Note:

   This process could take a long time if a lot of activity has taken place since the first snapshot was taken for the virtual machine. Snapshots for virtual machines should be temporary and used for restore points. They are not for permanent backups.

6. Record memory and CPU settings and delete the third virtual disk, labeled SCSI(0:2), from the virtual machine for R3.0, preserving its virtual disk files on the file system of the hypervisor.

   a. Using the VMware client, click **Edit Settings**.

   b. Click the **Hardware** tab.

   c. Record the memory size and the number of CPUs.

   d. Click the **Resources** tab and record the CPU and memory reservation values.

   e. Click the **Hardware** tab.

   f. Click **Hard disk 3** and then confirm that the disk has the virtual device node SCSI (0:2).

   g. Click **Remove** and then **Remove from virtual machine**.

   h. Click **OK**.

7. Move the virtual disk files for the previous release's virtual machine to the folder for the virtual machine R3.0 on the ESXi host's file system.

   a. Using the VMware client, select the ESXi host.

   b. From the Summary tab, select the host data store.

   c. Right-click and select **Browse Data Store**.

   d. Select the folder for the previous release's virtual machine.

   e. Select the name of the file for the third virtual disk.

      The name of the file is in the format: `<vm-name>_2.vmdk`.

f. Select **Move To** and then click **Yes** to confirm.

g. Select the host data store.

h. Select the folder for the virtual machine R3.0.

i. Click **Move**.

Note:

This process may take an extended period of time, based on the size of the virtual disk.

Important:

Move both the `.vmdk` and the `-flat.vmdk` files for the media disk. To ensure that this has occurred, repeat step 7 on page 232, and look for the `flat.vmdk` file. If this file has not yet been moved, then it will appear in the list and you can move it. If it does not appear, then both files have been moved and you can proceed to the next step.

8. Add the disk to the virtual machine for R3.0.

   a. Using the VMware client, click **Edit Settings**.

   b. In the Hardware tab, click **Add**.

   c. In **Choose the type of device you wish to add**, click **Hard Disk**, and then click **Next**.

   d. Select **Use an existing virtual disk** and then click **Next**.

   e. Click **Browse** and then navigate to the folder for the virtual machine R3.0.

   f. Select the virtual disk that was moved from the previous release's virtual machine and then click **OK**.

   g. In **Disk File Path**, confirm the path to the virtual disk file and then click **Next**.

   h. In **Virtual Device Node**, confirm the device node is SCSI (0:2) and then click **Next**.

   i. Confirm the selected options and then click **Finish**.

   j. Click **OK**.

9. Do the following using the information in Adjusting the virtual hardware of virtual machines on page 190:

   a. Update the virtual hardware memory and CPU configuration to align with the values for the previous release.

   b. Update the size of the application disk (second disk) to 204 GB.

10. Start the virtual machine and log in as the admin user.

11. Increase the size of the `/opt/Avaya` volume to utilize all remaining space from the application disk.

    For more information, see Adjusting the size of virtual disks on page 192.

12. Verify the presence of the `config.tar` file using the following command:

```
ls -l /media/data/backup/migrate_<hostname>/config.tar
```

13. Repeat all of the above steps in this procedure for the backup node and all remaining nodes in the cluster.

Next steps

- To complete the migration, see Completing the server migration (phase 3) on page 236.
- To abort the migration, see Aborting virtual machine migration on page 237.

Preparing the physical server for migration (phase 2 option 2)

About this task

This procedure prepares the Release 2.1 physical servers for the third, and final, phase of migration of a Release 2.1.x cluster to Release 3.x. During this procedure, the operating system is re-installed and the volumes hosting home directories and application software are cleared.

Important:

For clusters of physical servers, there is no opportunity to abort the migration procedure once this task has been started.

Before you begin

- Ensure that the preparation for the migration of the Release 2.1 system has been completed by checking Preparing the server for migration (phase 1) on page 228.
- Review Installation on a physical server on page 38.

Procedure

1. To determine the partitioning map for the existing server, run the `lsblk` command.

   In the following example, the operating system (mounted at `/`), swap space, application volume (mounted at `/opt/Avaya`), and home directories (mounted at `/home`) are in volumes located in the second partition (`sda2`) of the first disk (`sda`). The database and media content (mounted at `/media/data`) are located in the first partition (`sdb1`) of the second disk (`sdb`).

   ```
   $ lsblk
   NAME                          MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
   sr0                            11:0    1  1024M  0 rom
   sda                             8:0    0 279.4G  0 disk
   ├─sda1                          8:1    0   500M  0 part /boot
   └─sda2                          8:2    0 278.9G  0 part
     ├─vg_ucaamm2-lv_root (dm-0) 253:0    0    50G  0 lvm  /
     ├─vg_ucaamm2-lv_swap (dm-1) 253:1    0  33.5G  0 lvm  [SWAP]
     ├─vg_ucaamm2-lv_app (dm-3)  253:3    0 191.5G  0 lvm  /opt/Avaya
     └─vg_ucaamm2-lv_home (dm-4) 253:4    0   3.9G  0 lvm  /home
   sdb                             8:16   0   4.9T  0 disk
   └─sdb1                          8:17   0   4.9T  0 part
     └─vg_media-lg_media (dm-2)  253:2    0   4.9T  0 lvm  /media/data
   ```

   In this example, the volumes in `sda2` must be re-installed. The volume in `sdb1` must be left unaffected so its content can be migrated to the new Avaya Multimedia Messaging release.

2. Perform a fresh installation of the Red Hat Enterprise Linux (RHEL) server.

   a. Make sure you choose **Custom Layout** at the start of the partitioning process.

b. Make sure that the **Format** check box is selected for the following partitions: `/`, `/opt/Avaya`, and `/home`.

   These partitions are reformatted and existing data is lost.

c. Make sure that the **Format** check box is not selected for the `/media/data` partition.

   This partition is not formatted.

Note:

For the new Avaya Multimedia Messaging release, include the openjdk Java component either during or after the installation. For more information about performing a physical server installation, see Installation on a physical server on page 38.

3. Run the following commands to verify that the ucapp user name, the 652 UID, and the 1005 UID are not currently in use:

```
cat /etc/passwd | grep ucapp
cat /etc/passwd | grep 652
cat /etc/passwd | grep 1005
```

   Run the following commands to verify that the ucgrp group name, the 1002 GID, and the 1005 GID are currently not in use:

```
cat /etc/group | grep ucgrp
cat /etc/group | grep 1002
cat /etc/group | grep 1005
```

   Note:

   The Avaya Multimedia Messaging installer creates users and groups with the names and ids listed above. The UID 652 and GID 1002 are fixed across releases and across cluster nodes, and ensures that the Gluster file system has consistent user IDs among servers.

4. After the OS installation is complete, create an administrative user and group with full sudo permissions.

   Use the UID and GID values obtained in step 5 on page 229.

   For more information, see Creating non-root users on page 41 and Granting sudo permissions to non-root users on page 42.

5. Verify that presence of the file `config.tar` using the following command:

```
ls -l /media/data/backup/migrate_<hostname>/config.tar
```

6. Repeat steps 1 on page 234 thorugh 5 on page 235 for the backup node and all remaining nodes of the cluster.

Next steps

To complete the migration, see Completing the server migration (phase 3) on page 236.

Completing the server migration (phase 3)

About this task

Use this procedure to complete the migration process.

Important:

- This procedure does not retain the From Forking configuration. The From Forking configuration is re-enabled manually at the end of this procedure.
- For clusters of virtual machines, the migration can be aborted prior to starting this task. See Aborting virtual machine migration on page 237. Once this phase has been started, you cannot abort the migration procedure.
- Migration from R2.1 to R3.0 uses the R3.0.0.0 Avaya Multimedia Messaging application. For virtual machines, this is embedded in the OVA. Upgrading to the R3.0.0.1 version of the server is performed after the migration has been completed.

Before you begin

- If you are working with a cluster of virtual machines, ensure the virtual machines are prepared for migration. For more information, see Preparing the virtual server (phase 2 option 1) on page 230.
- If you are working with a cluster of physical servers, ensure the physical servers are prepared for migration. For more information, see Preparing the physical server for migration (phase 2 option 2) on page 234.

Procedure

1. If you are working with physical servers, transfer R3.0 installer file installer file, `amm-<new release>.bin`, to the `/opt/Avaya` directory on the seed node cluster for R3.0.

   For virtual machines, the `amm-<new release>.bin` file is written to `/opt/Avaya` as part of the OVA deployment.

2. Log into the seed node as an administrator, and run the following commands:

   ```
   chmod 750 /opt/Avaya/amm-<version>.bin
   sudo /opt/Avaya/amm-<version>.bin -- --migrate /media/data/backup/
   migrate_<hostname>/config.tar
   ```

   Note:

   `<hostname>` is the host name of the machine on which the command is being run

3. Repeat the steps above for the backup node, then for all remaining nodes in the cluster.
4. Log in to the seed node as an administrator, and run the following commands:

   ```
   cd /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/misc
   sudo ./migrateData.sh --migrate
   ```

Note:

The `migrateData.sh` command rewrites all the Cassandra database data. For large amounts of data, this process can take up to several hours.

If the SSH session expires, log in as an administrator in a new SSH session and check on the status of the script by running the following command:

```
sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/misc/
migrateData.sh --status
```

5. Repeat step 4 on page 236 for all remaining nodes in the cluster.

   Tip:

   You can perform this step on all nodes at the same time.

6. Log in to the seed node and run the following command:

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

7. Repeat step 6 on page 237 for the backup node and all remaining nodes in the cluster.
8. To configure the Serviceability Agent, log in to the seed node as an administrator and run the following command:

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

9. Configure the following values:
   - System Manager host
   - System Manager port
   - Enrollment password, which is the same as on System Manager
   - Keystore password, which must be at least six characters long
10. Select **Apply** to save the changes.
11. Select **Continue**, and then **Yes** to restart the Avaya Multimedia Messaging service.
12. Repeats steps 8 on page 237 to 11 on page 237 for the backup node and all remaining nodes in the cluster.
13. To configure the SSH/RSA Public and Private keys for the cluster, see Installing an Avaya Multimedia Messaging cluster on page 65.

Aborting virtual machine migration

About this task

Use this procedure to abort the migration of a cluster of virtual machines after you have performed the procedure Preparing the virtual server (phase 2 option 1) on page 230.

Procedure

1. Log in to the seed node of the server for R3.0, and shut down the operating system, using the following command:

   ```
   sudo shutdown -h now
   ```

2. Do the following to delete the third virtual disk, labeled SCSI(0:2), preserving its virtual disk files on the file system of the hypervisor:
   a. Using the VMware client, click **Edit Settings**.
   b. Click the **Hardware** tab.
   c. Click **Hard disk 3** and then confirm that the disk has the virtual device node SCSI (0:2).
   d. Click **Remove** and then **Remove from virtual machine**.
   e. Click **OK**.
3. Move the virtual disk files from the virtual machine for R3.0 to the folder for the previous release's virtual machine on the ESXi host's file system.
   a. Using the VMware client, select the ESXi host.
   b. From the Summary tab, select the host data store.
   c. Right-click and select **Browse Data Store**.
   d. Select the folder for the virtual machine R3.0.
   e. Select the name of the file for the third virtual disk.

      The name of the file is in the format: `<vm-name>_2.vmdk`.
   f. Select **Move To** and then click **Yes** to confirm.
   g. Select the host data store.
   h. Select the folder for the previous release's virtual machine.
   i. Click **Move**.

   This process might take an extended period of time, based on the size of the virtual disk.

   Important:

   Move both the `.vmdk` and the `-flat.vmdk` files for the media disk. To ensure that this has occurred, repeat step 7 on page 232, and look for the `flat.vmdk` file. If this file has not yet been moved, then it will appear in the list and you can move it. If it does not appear, then both files have been moved and you can proceed to the next step.
4. Add the disk to the virtual machine for the previous release.
   a. Using the VMware client, click **Edit Settings**.
   b. In the Hardware tab, click **Add**.
   c. In **Choose the type of device you wish to add**, click **Hard Disk**, and then click **Next**.
   d. Select **Use an existing virtual disk** and then click **Next**.
   e. Click **Browse**, then navigate to the folder for the previous release's virtual machine.
   f. Select the virtual disk that was moved from the virtual machine R3.0, then click **OK**.
   g. In **Disk File Path**, confirm the path to the virtual disk file and then click **Next**.
   h. In **Virtual Device Node**, confirm the device node is SCSI (0:2) and then click **Next**.

i. Confirm the selected options and then click **Finish**.

j. Click **OK**.

5. Start the virtual machine and log in as the ammapp user.
6. Repeat the previous steps in this procedure for the backup node and all remaining nodes in the cluster.

Restoring Avaya Multimedia Messaging to the previous version if you abort migration

About this task

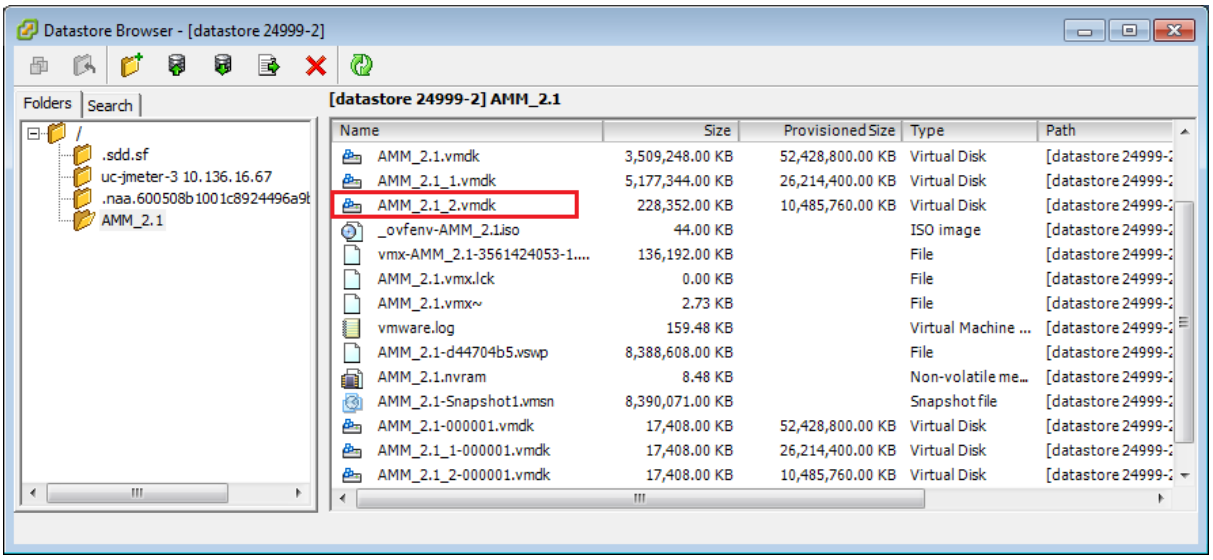
If you consider aborting the migration to the new version, this can be done safely after the new virtual machine is created and powered, as long as Completing the server migration (phase 3) on page 236 has not been performed.

Procedure

1. Power off the virtual machine.
2. Create a temporary holding folder.
3. Select the virtual drive and move it to the temporary folder.

   If you are using vSphere, the virtual drive is managed as two `.vmdk` files, but it might appear as a single object. Make sure both files are moved.

   If you are using vCenter, you just need to move one file.



4. Delete the new virtual machine.
5. Restore the initial name to the previous virtual machine.
6. Move the virtual drive from the temporary folder to the initial datastore folder.

7. Start the virtual machine.

Migration of the Avaya Aura® environment

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

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

See the following documents for more information on migrating:

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

Migrating the Data Replication Service

Before you begin

Complete the Avaya Multimedia Messaging update.

Procedure

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

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

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

Presence Services federation migration

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

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

Procedure

1. Obtain the Presence Services Presence Services Certificate Authority.

   You can usually download this certificate from System Manager.

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

   Important:

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

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

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

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

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

Procedure

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

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

   Important:

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

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

2. In the left panel, select **Server Connections** > **Federation Configuration**.
3. Open the XMPP Adaptor page.

4. Note the following:
   - The values in the **Routing Domain**, **Remote Domains**, and **Timeout** fields.
   - Whether the **Send Presence Ping** check box is selected.
5. Disable the adaptor. .
   a. Select the **Adapter Enabled** check box.
   b. Click **Save**.

   The application restarts.
6. Go back to the Federation Configuration page.
7. In **HTTPS REST to Avaya Presence Services Connection Adaptors**, click **Add**.
8. In the new Adaptor page, do the following:
   a. Select the **XEP-0033** protocol.

      Note:

      Only the XEP-0033 protocol is supported.
   b. Select the **Adaptor Enabled** check box.
   c. Enter the previously noted and new values in the corresponding fields for **HTTPS REST to Avaya Presence Services Connection Adaptors**.

      For details on configuration of HTTPS REST adaptor, see Configuring the HTTPS REST interface in Avaya Multimedia Messaging for federation with Presence Services on page 133.
   d. **(Optional)** In the **Port** field, update the port number.

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

   Note:

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

   The application restarts.

Upgrading the Avaya Multimedia Messaging server

About this task

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

Multimedia Messaging server while also adding a new node to the cluster, see Adding a new node while performing an Avaya Multimedia Messaging upgrade on page 73.

Note:

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

Before you begin

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

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

Important:

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

Procedure

1. On the Avaya Multimedia Messaging node, download or copy the latest Avaya Multimedia Messaging binary build.
2. Run the installer of the latest build, as if performing a new installation.

   For more information about running the installer, see Installing the Avaya Multimedia Messaging server on page 48.

   When you run the installer for the latest Avaya Multimedia Messaging build, the system prompts you to confirm that you want to perform an upgrade. Select **Yes** and press `Enter` to start the upgrade.

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

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

Next steps

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

```
service AMMService start
```

Related links

Avaya Multimedia Messaging upgrades and migrations on page 226
Rollback operations on page 244

Rollback operations

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

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

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

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

Warning:

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

Related links

Upgrading the Avaya Multimedia Messaging server on page 242

Restoring a previous version of the Avaya Multimedia Messaging server

About this task

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

Note:

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

Before you begin

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

Procedure

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

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

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

```
service AMMService start
```

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

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

Checking for DRS synchronization after a migration or upgrade

About this task

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

Procedure

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

Applying patches

About this task

Use the following procedure to apply a patch. In a cluster deployment, you must repeat the steps on each node.

Procedure

1. Log in to the Avaya Multimedia Messaging server CLI as a non-root user.
2. Obtain and transfer the patch to the Avaya Multimedia Messaging server.

   You can use a tool such as wget or SCP for Linux.
3. Ensure the patch file is executable by running the following command:

   ```
   chmod 0755 Notification_threadpool_patch.bin
   ```
4. Execute the patch by running the following command:

   ```
   sudo ./Notificiation_threadpool_patch.bin
   ```
5. When prompted to continue, enter `y`.

   The patch shuts down Avaya Multimedia Messaging if it is running.
6. When all nodes are patched, start the Avaya Multimedia Messaging service by running the following command:

   ```
   sudo /etc/init.d/AMMService start
   ```

Result

The Avaya Multimedia Messaging interface displays the patched product version and information about the patch applied.

Chapter 8: Troubleshooting

Troubleshooting best practices for IWA

Condition

This information can be useful in tracking down problems.

Solution

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

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

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

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

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

An Avaya Multimedia Messaging node has malfunctioned and been inactive for an extended period of time

If an Avaya Multimedia Messaging server has been inactive for an extended period of time after a system malfunction, the information in the database can become inaccurate.

Repairing the database inconsistencies

Procedure

1. Open the Avaya Multimedia Messaging server CLI.
2. Type the following command:

```
$ sudo <installation_directory>/cassandra/1.2.7/bin/nodetool -u
<cassandra_username> -pw <cassandra_password> repair
```

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

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

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

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

Cause

When the Avaya Multimedia Messaging server cannt connect to Presence Services, the Avaya Multimedia Messagingraises alarm code 00064. The Avaya Multimedia Messaging server maintains the outgoing messages in its buffer, to later send the messages when the connection is restored. The accumulation of messages in the internal buffer occupies Avaya Multimedia Messaging server memory in time.

Solution

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

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

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

Condition

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

Solution

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

Client cannot connect to the Avaya Multimedia Messaging server

Solution

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

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

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

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

4. If the web page displays an error or you are unable to download the file, perform the following actions:

   a. If the page displays `Error Code 401`, the password that you have entered is not correct.

   b. If the page displays `Error Code 403`, the user does not have the privileges required for gaining access to the Avaya Multimedia Messaging client interface. You must add the respective user to the Admin group configured in the LDAP structure.

   c. If the page displays `Error Code 500`, ensure that the Avaya Multimedia Messaging server is running.

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

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

      Note:

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

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

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

Failure to retrieve System Manager user settings

Condition

The System Manager login ID has a different user name and domain name than the email address in LDAP.

Solution

The Microsoft Exchange address must be added as a communication address in the System Manager user account.

Gluster configuration failure

Condition

The configuration of the gluster “bricks” across a cluster might fail. When this failure occurs, you see a message similar to: `Staging failed on <IP>. . Error: Host <IP> not connected`.

Cause

This problem is usually caused by network issues.

Solution

After your network issues are resolved, rerun the gluster brick configuration. You might see another error message, such as: `/media/data/content_store/brick0 exists, and should be removed ("rm -fr /media/data/content_store/brick0")`. If this occurs, do the following:

1. From the shell, run the suggested command using the sudo prefix.
2. Go back to the post-installation tool using the `configureAMM.sh` script.
3. Rerun the brick configuration steps.

Gluster rebalancing fails when you add a new node

Condition

When you add a new node to a cluster, gluster rebalancing fails and the Avaya Multimedia Messaging service stops.

Cause

The data store on the new node is smaller than it is on other existing nodes.

Solution

Ensure that the data store on the new node is sufficient. You can also try pairing gluster bricks for two nodes with smaller data stores.

HTTP services disabled due to storage capacity reaching critical threshold

Condition

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

- `avAMMDBStorageReachedCriticalThreshold`
- `avAMMMediaStorageReachedCriticalThreshold`

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

Cause

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

Solution

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

   Important:

   Do not perform the backup on the full disk.

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

   Note:

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

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

Troubleshooting License error

Condition

When a licensing error occurs because of insufficient available server node licenses, the next error message is displayed in the administration portal: `A License problem has been detected. Invalid feature capacity error.`

Information about this error might be stored in the Avaya Multimedia Messaging logs. For details, see Logs and alarms on page 197.

Solution

Ensure sufficient server node licenses.

Troubleshooting LDAP server authentication problems

When a user does not succeed connecting to the Avaya Multimedia Messaging services or to use the administration portal, you can perform the following troubleshooting tasks:

- Test the LDAP configuration using an LDAP browser.
- Disable the secure LDAP setting.
- Enable trace-level logging and view the log files

Logging trace-level messages for security-related classes

About this task

The following procedure describes a few different methods to log TRACE-level messages on the Avaya Multimedia Messaging server.

Important:

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

Procedure

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

   For example:

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

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

   a. Make a capture with the .pcap format.

   b. Run the **`tcpdump`** command:

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

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

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

   For details, see Updating logging levels on page 190.

Long poll timeout for Avaya Equinox™ client connections to the Avaya Multimedia Messaging server

Condition

The Avaya Equinox™ client connection to the Avaya Multimedia Messaging server closes at fixed time intervals when the user connects through Avaya Session Border Controller for Enterprise.

Cause

The Avaya Session Border Controller for Enterprise timeout is less than the value of the Avaya Multimedia Messaging long poll timeout setting.

Solution

1. Run the Avaya Multimedia Messaging configuration utility.

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

2. Select **Advanced Configuration**.
3. Configure the long poll timeout with a value that is less than the Avaya Session Border Controller for Enterprise timeout.

Troubleshooting Lync federation issues

System Manager certificate on Lync edge server is missing or invalid

Condition

The external communication between Lync and Avaya Multimedia Messaging fails in the following cases:

- Lync to Avaya Multimedia Messaging: After an IM text is sent, the Lync client displays the alert `This message wasn't sent to _IM_user_ID_`.
- Lync conference to Avaya Multimedia Messaging is not created.
- Avaya Multimedia Messaging to Lync: After a second, the Avaya Multimedia Messaging client shows that the Lync user has left the conversation.

Solution

Follow the procedures to obtain and install the System Manager certificate on the Lync Edge. For details, see Downloading the System Manager certificate on page 171.

Lync certificate on System Manager or Session Manager is missing or invalid

Condition

The external communication between Lync and Avaya Multimedia Messaging fails in the following cases:

- Lync to Avaya Multimedia Messaging: After an IM text is sent, the Lync client displays the alert `This message wasn't sent to _IM_user_ID_`.
- Lync conference to Avaya Multimedia Messaging is not created.
- Avaya Multimedia Messaging to Lync: After a second, the Avaya Multimedia Messaging client shows that the Lync user has left the conversation.

Solution

See Adding the Lync certificate to System Manager on page 136.

Lync certificate on Avaya Multimedia Messaging is missing or invalid

Condition

The internal communication between Lync and Avaya Multimedia Messaging fails in the following cases:

- Lync to Avaya Multimedia Messaging: After an IM text is sent, the Lync client displays the alert `This message wasn't sent to _IM_user_ID_`.
- Lync conference to Avaya Multimedia Messaging is not created.
- Avaya Multimedia Messaging to Lync: After a second, the Avaya Multimedia Messaging client shows that the Lync user has left the conversation.

Solution

See Importing the Lync front-end server certificate into the trust store on page 109.

System Manager certificate on Lync Front end server is missing or invalid

Condition

The internal communication between Lync and Avaya Multimedia Messaging fails in the following cases:

- Lync to Avaya Multimedia Messaging: After an IM text is sent, the Lync client displays the alert `This message wasn't sent to _IM_user_ID_`.
- Lync conference to Avaya Multimedia Messaging is not created.
- Avaya Multimedia Messaging to Lync: After a second, the Avaya Multimedia Messaging client shows that the Lync user has left the conversation.

Solution

Follow the procedures to obtain and install the System Manager certificate on the Lync Edge. For details, see Downloading the System Manager certificate on page 171.

SIP Adapter for Session Manager is not enabled or with a misconfigured IP address

Condition

Both the internal and external communication between Lync and Avaya Multimedia Messaging fail in the following cases:

- Lync to Avaya Multimedia Messaging: After an IM text is sent, the Lync client displays the alert `This message wasn't sent to _IM_user_ID_`.
- Lync conference to Avaya Multimedia Messaging is not created.
- Avaya Multimedia Messaging to Lync: After a second, the Avaya Multimedia Messaging client shows that the Lync user has left the conversation.

Solution

1. Configure the Session Manager SIP adapter. For details, see Configuring SIP adapters on page 143.
2. To use the new configuration, restart Avaya Multimedia Messaging.

SIP Adapter for Session Manager is not enabled or enabled with a misconfigured IP address

Condition

The internal communication between Lync and Avaya Multimedia Messaging fails in the following cases:

- Lync to Avaya Multimedia Messaging: After an IM text is sent, the Lync client displays the alert `This message wasn't sent to _IM_user_ID_`.
- Lync conference to Avaya Multimedia Messaging is not created.
- Avaya Multimedia Messaging to Lync: After a second, the Avaya Multimedia Messaging client shows that the Lync user has left the conversation.

Solution

1. Configure the Lync SIP adapter. For details, see Configuring SIP adapters on page 143.
2. To use the new configuration, restart Avaya Multimedia Messaging.

Avaya Multimedia Messaging node is not a trusted host on Lync

Condition

The internal communication between Lync and Avaya Multimedia Messaging fails in the following cases:

- Lync to Avaya Multimedia Messaging: After an IM text is sent, the Lync client displays the alert `This message wasn't sent to _IM_user_ID_`.
- Lync conference to Avaya Multimedia Messaging is not created.
- Avaya Multimedia Messaging to Lync: After a second, the Avaya Multimedia Messaging client shows that the Lync user has left the conversation.

At the same time, SIP adapter for Lync is disconnected.

Solution

- Verify that the Avaya Multimedia Messaging cluster nodes are trusted hosts on the Lync server.
- Add a node as a trusted host on Lync, using Adding each Avaya Multimedia Messaging server node and front-end FQDN as a trusted application to Lync Standard Edition on page 146.

LyncAdaptation is missing from Avaya Multimedia Messaging SIP entity

Condition

The internal communication between Lync and Avaya Multimedia Messaging fails in the following cases:

- Lync to Avaya Multimedia Messaging: After an IM text is sent, the Lync client displays the alert `This message wasn't sent to _IM_user_ID_`.
- Lync conference to Avaya Multimedia Messaging is not created.
- Avaya Multimedia Messaging to Lync: After a second, the Avaya Multimedia Messaging client shows that the Lync user has left the conversation.

After you add an Avaya Multimedia Messaging user to the Lync client, the error `Invitation to _user_ expired` is displayed.

Solution

Add the LyncAdaptation to the SIP entity with the Avaya Multimedia Messaging front end FQDN. For details, see Adding the Lync adapter file in System Manager on page 136.

Lync Adaptation is missing from Lync Edge remote server

Condition

Lync point to point to Avaya Multimedia Messaging works.

Avaya Multimedia Messaging to Lync works.

The external communication between Lync conference to Avaya Multimedia Messaging fails. In this case, 40 seconds later from adding an Avaya Multimedia Messaging user, the Lync client displays: `invitation to XXX expired`..

Solution

On System Manager, add the LyncAdaptation to the SIP entity belonging to the Lync Edge.

The routing pattern to Avaya Multimedia Messaging is missing or incorrect

Conditions

Lync point to point to Avaya Multimedia Messaging fails.

Both the internal and external communication between Lync and Avaya Multimedia Messaging fail under the following circumstances:

- The Lync message reaches the Avaya Multimedia Messaging client.

- The Lync client displays the message `The meeting you are trying to join doesn't exist or has ended`.
- No messages from the Avaya Multimedia Messaging client reach the Lync client.
- Subsequent messages from Lync continue to reach Avaya Multimedia Messaging client.
- After a minute, the Avaya Multimedia Messaging client shows that the Lync user left the conversation.
- The next message from the Lync client creates a new Avaya Multimedia Messaging client conversation window.

Avaya Multimedia Messaging to Lync fails.

Both the internal and external communication between Avaya Multimedia Messaging and Lync fail under the following circumstances:

- The Lync client receives in a pop-up window the invitation from Avaya Multimedia Messaging and the Lync user accepts the invitation.
- The Lync client displays the message `The meeting you are trying to join doesn't exist or has ended`.
- No messages can be exchanged in either direction.
- Each message from Avaya Multimedia Messaging client creates a new Lync client pop-up.
- After a minute, the Avaya Multimedia Messaging client shows that the Lync user left the conversation.

Lync conference to Avaya Multimedia Messaging works.

Solution

Add the routing patterns in System Manager for Avaya Multimedia Messaging. For details, see Routing policies and regular expressions on page 140.

The routing pattern to Lync Edge is missing or incorrect

Condition

The external communication with Lync Edge fails in the following cases:

- Lync point-to-point to Avaya Multimedia Messaging: The Avaya Multimedia Messaging client receives the first message from the Lync client. After a second, the Avaya Multimedia Messaging client shows that the Lync user left the conversation.

  Each subsequent message from the Lync client creates a new conversation with the same outcome as above.
- Avaya Multimedia Messaging to Lync: A second after sending a message or adding a Lync user, the Avaya Multimedia Messaging client shows that the Lync user left the conversation.
- Lync conference to Avaya Multimedia Messaging: After you add an Avaya Multimedia Messaging user to the Lync client, the system displays an error: `Invitation to 15 _user_ expired`.

Solution

On System Manager, add the routing pattern for routing to Lync Edge.

Note:

You might need to create a routing policy for Lync Edge.

Route to the destination domain is missing

Condition

The internal communication between Lync and Avaya Multimedia Messaging fails in the following cases:

- Lync point to point to Avaya Multimedia Messaging: After an IM message is sent, the Lync client displays the following alert: `We couldn't reach _IM_user_ID_ to send this message.`
- Avaya Multimedia Messaging to Lync: The Lync client receives the invitation from Avaya Multimedia Messaging in a pop-up window, and the Lync user accepts the invitation. The Lync client displays the message: `The meeting you are trying to join doesn't exist or has ended`. Aftter one minute, the Avaya Multimedia Messaging client shows that the Lync user left the conversation.
- Lync conference to Avaya Multimedia Messaging: After you add an Avaya Multimedia Messaging user to the conference, the Lync client displays the following alert: `_IM_user_ID_ cannot be found. Please check the address and check again.`

Solution

1. Add a static route for the domain of the recipient on the Lync server. See Adding Avaya Multimedia Messaging as the destination of a static route on page 149.
2. If you already added a static route, run `nslookup` in a command prompt to check whether the FQDN used is added to the DNS server that the Lync server uses.

Avaya Multimedia Messaging front-end FQDN is not administered as a SIP federated provider

Condition

The internal communication between Lync and Avaya Multimedia Messaging fails in the following cases:

- Lync point to point to Avaya Multimedia Messaging: After an IM message is sent, the Lync client displays the following alert: `We couldn't reach _IM_user_ID_ to send this message.`
- Avaya Multimedia Messaging to Lync: The Lync client receives the invitation from Avaya Multimedia Messaging in a pop-up window, and the Lync user accepts the invitation. The Lync client displays the message: `The meeting you are trying to join doesn't exist`

`or has ended`. Aftter one minute, the Avaya Multimedia Messaging client shows that the Lync user left the conversation.

- Lync conference to Avaya Multimedia Messaging: After you add an Avaya Multimedia Messaging user to the conference, the Lync client displays the following alert: `_IM_user_ID_ cannot be found. Please check the address and check again.`

Solution

1. Open the Lync server control panel.
2. In **Federation and External Access**, click **SIP Federated Providers.**
3. Add the Avaya Multimedia Messaging front-end FQDN as a new public provider.
4. To use the new configuration, restart the Lync front-end service.

Avaya Multimedia Messaging user does not have presence or IM handle

Condition

Both the internal and external communication between Lync and Avaya Multimedia Messaging fail in the following circumstances:

- Lync point-to-point to Avaya Multimedia Messaging: After the Lync client sends an IM, the Avaya Multimedia Messaging client receives an incoming voice call.
- Avaya Multimedia Messaging to Lync: After a second, the Avaya Multimedia Messaging client shows that the Lync user has left the conversation.
- Lync conference to Avaya Multimedia Messaging: After the Lync client sends an IM, the Avaya Multimedia Messaging client receives an incoming voice call.

Solution

1. In System Manager, edit the communication profile of the user to add the Presence/IM handle.
2. If the user already has a Presence/IM handle, see Avaya Multimedia Messaging user does not have presence or IM handle on page 260.

System Manager data is inaccessible

Condition

Both internal and external communication between Lync and Avaya Multimedia Messaging fail in the following circumstances:

- Lync point-to-point to Avaya Multimedia Messaging: The Lync client displays the alert `The following can't receive IMs right now: _IM_user_ID_` or `This message wasn't sent to _IM_user_ID_`.
- Avaya Multimedia Messaging to Lync: After a second, the Avaya Multimedia Messaging client shows that the Lync user has left the conversation.

- Lync conference to Avaya Multimedia Messaging: The Avaya Multimedia Messaging client sees that it was added to a conversation. However, the Avaya Multimedia Messaging client does not receive any message sent by the Lync client. The first message sent from the Avaya Multimedia Messaging client is immediately followed by the Avaya Multimedia Messaging client showing that the Lync user left the conversation.

Solution

1. In System Manager, on the replication page, in the right-hand column, find the replica group that contains Avaya Multimedia Messaging.
2. Check whether Avaya Multimedia Messaging needs repair, and if it does, click the repair button.
3. If the status of Avaya Multimedia Messaging is `Synchronized`, then open an Avaya Multimedia Messaging console and do the following:
   a. Go to **Server Connections** > **LDAP Configuration page**.
   b. Select **Force LDAP Sync** and wait for 5 minutes.
   c. Send an IM.
   d. **(Optional)** If the IM is not sent, contact Avaya Support.

LDAP data is inaccessible

Condition

The internal communication between Lync and Avaya Multimedia Messaging fails in the following cases:

-
- Lync point-to-point to Avaya Multimedia Messaging: The Lync client displays the alert `The following can't receive IMs right now: _IM_user_ID_` or `This message wasn't sent to _IM_user_ID_`.
- Avaya Multimedia Messaging to Lync: The Lync contact does not display an IM bubble or the Avaya Multimedia Messaging client opens a pop-up window with the message: `The following selected contact(s) do not have a valid messaging address: _IM_user_ID_`.
- Lync conference to Avaya Multimedia Messaging: After adding an Avaya Multimedia Messaging user, the Lync client displays: `_IM_user_ID_ cannot be found. Please check the address and try again.`

Solution

1. On the machine running Active Directory, run the refresh command to ensure that the Active Directory is updated.
2. In the Avaya Multimedia Messaging console, go to **Server Connections** > **LDAP Configuration** and do the following:
   a. Select **Force LDAP Sync** and wait for 5 minutes.
   b. Send an IM.

c. **(Optional)** If the IM is not sent, contact Avaya Support.

Problem in System Manager administration of Avaya Multimedia Messaging SIP entities

Condition

One or more Lync clients continually log out.

Cause

The Lync client requests presence information from one or more of its contacts that are Avaya Aura® users. The requests are challenged for a password. The Lync client does not handle the password challenges and logs out, and then logs in. This sequence is cyclically repeated. Session Manager might receive a `SUBSCRIBE` request that could come from more than one SIP entity.

Solution

On System Manager, check the Avaya Multimedia Messaging SIP entity links.

If the same IP address is obtained from more than one SIP entity, then both ports in each entity link must be different from the corresponding port in an Entity that resolves to the same address. For instance, one SIP entity might be using an IP address while the other uses an FQDN.

Avaya Multimedia Messaging lost Lync session information

Condition

Both internal and external communication fails between Avaya Multimedia Messaging and Lync when, after sending an IM, the Lync client displays an alert: `The action couldn't be completed. Please try again later.`

Solution

1. Send a message from an Avaya Multimedia Messaging client.

   A pop-up window with an invitation to join the conversation opens for the Lync client.

2. Accept the invitation.

   The Lync client reconnects to the conversation. If the Lync client is not added to the conversation, the Avaya Multimedia Messaging client shows that the Lync user left the conversation.

3. If Avaya Multimedia Messaging shows that the Lync user left the conversation, add the Lync user back to the conversation.

User did not acknowledge message receipt

Condition

Both internal and external communication fail between Lync and Avaya Multimedia Messaging when, after sending an IM, the Lync client displays an alert: `This message wasn't sent to everyone.`

Solution

No workaround is available.

Lync front-end server cannot start

Condition

The Lync front-end server is unable to start and the event log contains the error SIPPROXY_E_MULTIPLE_INCOMPATIBLE_TRUST_OPTIONS with the code C3E93C66.

Cause

SIP TCP is enabled.

Solution

1. Open Topology Builder.
2. Navigate to **Lync Server 2013/ Enterprise Edition Front End Servers**.
3. Click **Lync Server 2013 Enterprise Front End Server** and right-click **Edit properties**.
4. Click **Limit Service usage to Selected IP addresses**.
5. Add the IP address of the front-end server manually to the **Primary address** field.

   The PSTN IP address uses the same value.
6. Click **OK** and then **Publish Topology**.

Networking issues after upgrading

Condition

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

Solution

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

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

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

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

3. Restart the Avaya Multimedia Messaging server.

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

OpenFire log displays Requested node not found in cluster error

Condition

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

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

Cause

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

Solution

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

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

   Note:

   This command prevents Recovery Manager from restarting OpenFire automatically.

3. Restart OpenFire on the first node using the following command:

   ```
   sudo service AMMOpenfire start
   ```

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

   ```
   Members [1] {
       Member [ip of the 1st node]:5701
   }
   ```

5. Start OpenFire on the second node.

6. Wait until you see the following on the `/opt/openfire/log/stderror.log` log file:

```
Members [2] {
   Member [ip of the 1st node]:5701
    Member [ip of the 2nd node]:5701
}
```

7. Start OpenFire on the third node.
8. Wait until you see the following on the `/opt/openfire/log/stderror.log` log file:

```
Members [3] {
    Member [ip of the 1st node]:5701
    Member [ip of the 2nd node]:5701
    Member [ip of the 3rd node]:5701
}
```

9. Re-enable the watchdog functionality on each node using the following command:

```
sudo service AMMRecoveryManager enableWatchdog
```

Participant has invalid messaging address

Condition

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

Solution

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

The resource discovery operation returns error code 404

If the resource discovery operation returns error code 404: Invalid Userid, the user ID is not configured in the LDAP server.

To perform the resource discovery operation, the system administrator of the LDAP server must configure the email attribute of the users and then you must perform a Force Update of the LDAP server using the administration portal.

Performing a force update of the LDAP configuration

Procedure

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

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

   Important:

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

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

2. Select **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.
3. Click **Force Update**.
4. Click **Save**.

Special characters displayed incorrectly when playing multimedia attachment

Condition

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

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

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

Cause

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

Solution

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

Creating this file on the Desktop and naming it using special characters will force the operating system to load the font sets next time at startup.

2. Log off and then log in to your computer or restart the operating system.
3. Click the attachment URL in one-X Communicator to retrieve the attachment.

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

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

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

Activating the Avaya Multimedia Messaging server

Procedure

1. Log in to the Avaya Aura® System Manager Admin Viewer.
2. In the left panel, click **Inventory** > **Agents** > **Serviceability Agents**.
3. Click the **Selected Agents** tab.
4. In the Agent List, select the Avaya Multimedia Messaging server, using the host name or the IP address of the server.
5. If the status of the Avaya Multimedia Messaging server is *inactive*, click the **Activate** button.

Configuring an SNMP trap

Procedure

1. Log in to the Avaya Aura® System Manager Admin Viewer.
2. In the left panel, click **Inventory** > **Agents** > **Serviceability Agents**.
3. Click the **SNMP Target Profiles** tab.
4. In the **Assignable Profiles** and **Removable Profiles** fields, identify the SNMP traps that might be related to the Avaya Multimedia Messaging server.

   For more information about viewing and adding SNMP traps, consult the *Administering Avaya Aura® System Manager* document.

5. On the Avaya Multimedia Messaging server, view the content of the `snmpd.conf` file and ensure that the file reflects the SNMP trap destination defined in Avaya Aura® System Manager Admin Viewer.

   Example:

```
# cat /var/net-snmp/snmpd.conf | grep 1.2.3.4
targetAddr 1.2.3.4_V2_1 .1.3.6.1.6.1.1 0x8714f61227b2 3000 3 "1.2.3.4_V2_1"
1.2.3.4_V2_1 3 1
targetParams 1.2.3.4_V2_1 1 2 public 1 3 1
```

Unable to view Avaya Multimedia Messaging logs using Log Viewer

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

Configuring the Avaya Aura® System Manager FQDN

Procedure

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

Upgrade fails when trace logging is turned on

Condition

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

Cause

The logging level is set to TRACE.

Solution

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

User is unable to log in to the Avaya Multimedia Messaging server

Solution

1. Ensure that the necessary certificate, from Avaya Aura® System Manager or from a third party CA, has been installed on the Avaya Multimedia Messaging enabled client.
2. Ensure that the Avaya SIP CA certificate, used for communications with Session Manager, has been installed on the Avaya Multimedia Messaging client.
3. Ensure that the System Manager certificate has been created using the FQDN of the Avaya Multimedia Messaging server, and not the IP address.

User is unable to send message from an Avaya Multimedia Messaging enabled client

Condition

A user is unable to send an Avaya Multimedia Messaging message from an Avaya Multimedia Messaging enabled client to another Avaya Multimedia Messaging enabled client.

The client application displays a red icon with the message `Correct certificate needs to be installed on AMM server`.

Solution

1. Ensure that the necessary certificate, from Avaya Aura® System Manager or from a third party CA, has been installed on the Avaya Multimedia Messaging enabled client.
2. Ensure that the System Manager certificate has been created using the FQDN of the Avaya Multimedia Messaging server, and not the IP address.

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

Condition

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

The correct behavior in this context is the following:

- The Avaya one-X® Communicator user that uses the Avaya one-X® Communicator client receives an IM containing an URL link from the Avaya Multimedia Messaging user

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

If the Avaya Multimedia Messaging enabled client shows an error to the Sender saying that the Avaya one-X® Communicator participant is not a valid a messaging address, perform the following actions:

Solution

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

Virtual IP node is inaccessible

Condition

The virtual IP seed node or backup node has become permanently inaccessible and you cannot configure the virtual IP function for another node.

Cause

The node is inaccessible, but the registration of the node remains in the system.

Solution

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

   ```
   <AMM install directory>/CAS/*/misc/clitool.sh clear <IP of the node to deregister>
   ```

2. Configure the virtual IP on the desired node.

Chapter 9: Resources

Documentation

The following table lists related documentation for Avaya Multimedia Messaging. All Avaya documentation is available at http://support.avaya.com.

Table 27: 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 **Note:** *Administering Avaya Equinox™ for Android, iPad, iPhone, and Windows* has been restructured and replaced with this document in Release 3.0.	• 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, administer, and troubleshoot Avaya Multimedia Messaging.	Implementation personnel
Maintaining		

Table continues…

Title	Use this document to	Audience
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
Using		
Using Avaya Equinox™ for Android, iOS, Mac, and Windows	Install and use your Avaya Equinox™ client.	Enterprise users
Avaya Equinox™ Contact Management Quick Reference	Understand how to work with contacts in Avaya Equinox™.	Enterprise users

Table 28: 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

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

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

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

Note:

Videos are not available for all products.

Support

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

Related links

Using the Avaya InSite Knowledge Base on page 274

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 at no extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base to look up 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 Support page appears.
3. Under **Support by Product**, click **Product-specific support**.
4. Enter the product in **Enter Product Name** text box and press Enter.
5. Select the product from the drop down list and choose the relevant release.
6. Select 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

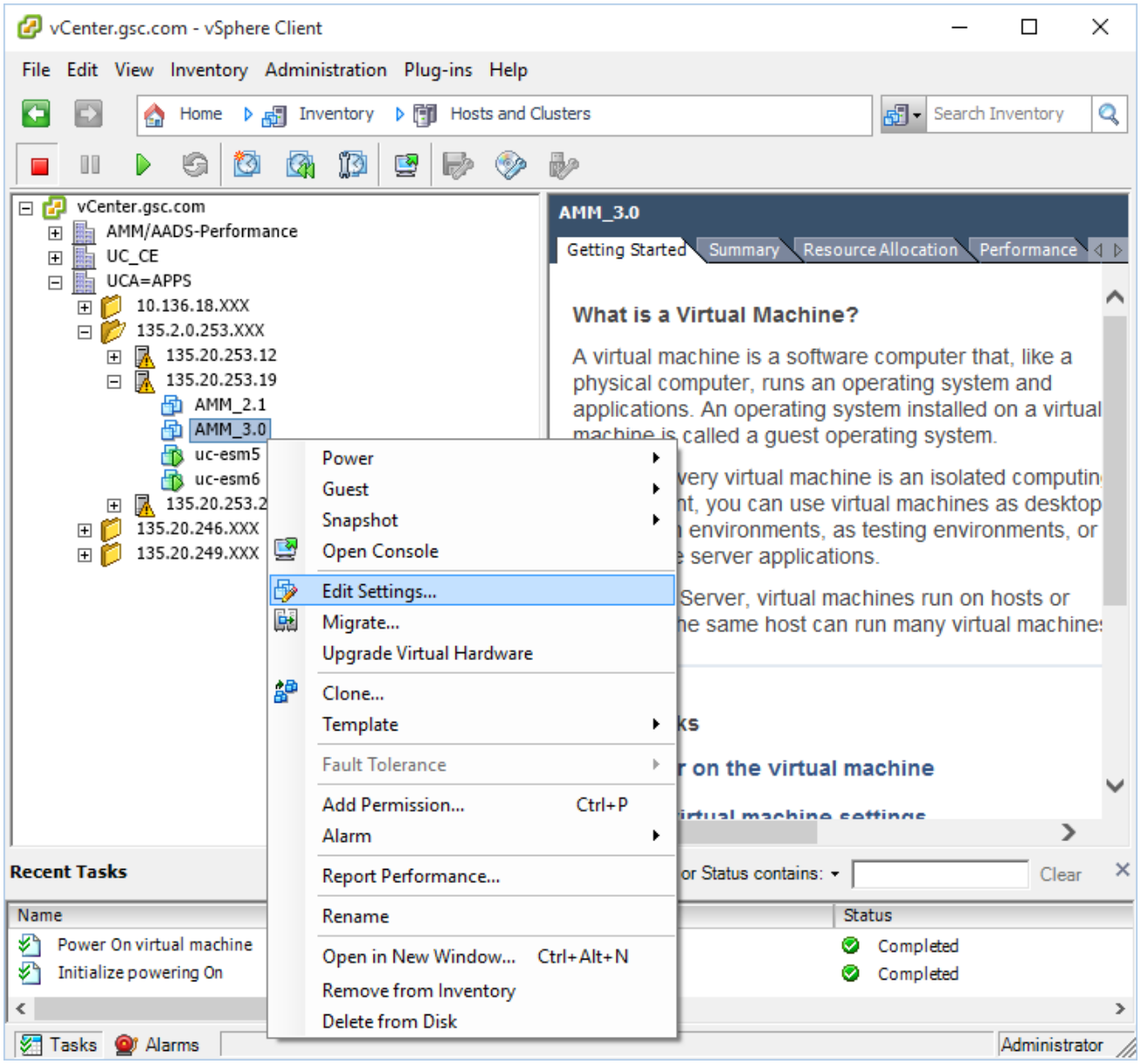
```
# Binding parameters
ldapUrl=ldaps://gdc.global.example.com:3269
bindDN=global\AMMAssistant
bindCredential=admin123

# 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
```

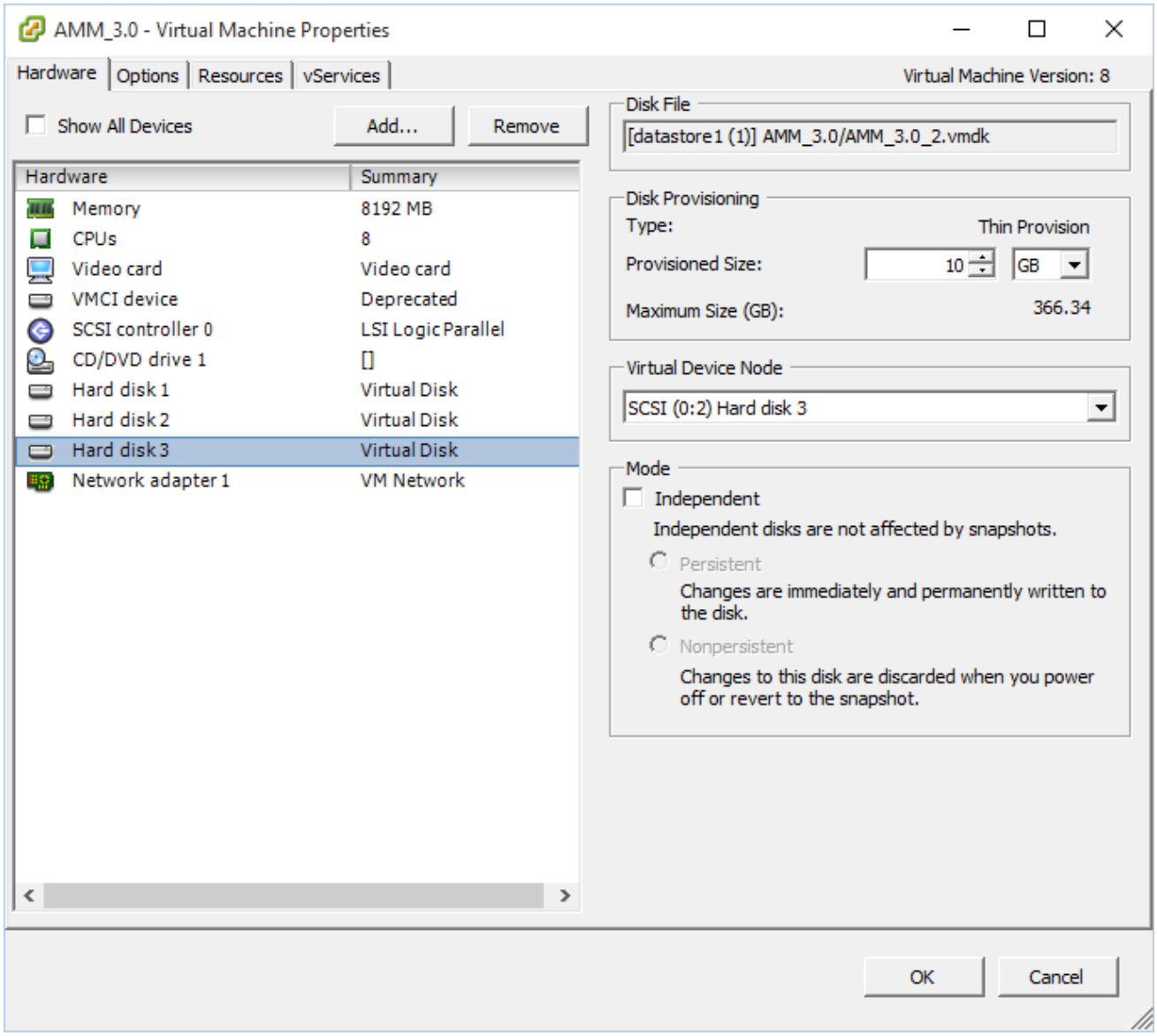
Appendix B: Example images of the Avaya Multimedia Messaging migration process

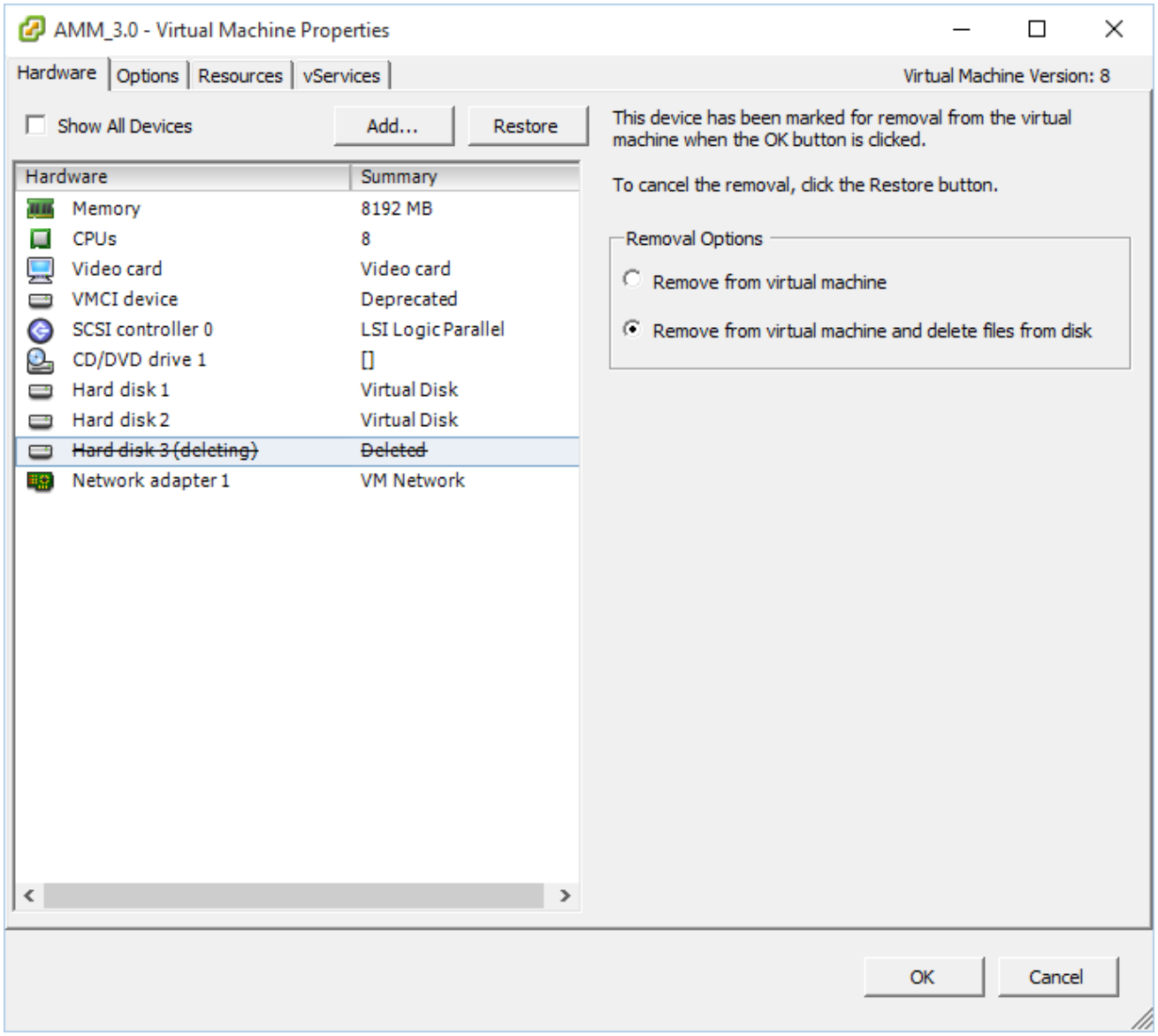
Deleting media disk from Release 3.0 virtual machine

The following images show the removal of the media disk from the Release 3.0 virtual machine, including deleting the corresponding files for the virtual disk on the file system of the host ESXi hypervisor.


vCenter.gsc.com - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home
Inventory
Hosts and Clusters
Search Inventory
vCenter.gsc.com
AMM/AADS-Performance
UC_CE
UCA=APPS
10.136.18.XXX
135.2.0.253.XXX
135.20.253.12
135.20.253.19
AMM_2.1
AMM_3.0
uc-esm5
uc-esm6
135.20.253.2
135.20.246.XXX
135.20.249.XXX
AMM_3.0
Getting Started
Summary
Resource Allocation
Performance
What is a Virtual Machine?
A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual
called a guest operating system.
Power
Guest
Snapshot
Open Console
Edit Settings...
Migrate...
Upgrade Virtual Hardware
Clone...
Template
Fault Tolerance
Add Permission... Ctrl+P
Alarm
Report Performance...
Rename
Open in New Window... Ctrl+Alt+N
Remove from Inventory
Delete from Disk
Recent Tasks
Name
Status
Power On virtual machine
Completed
Initialize powering On
Completed
Tasks
Alarms
Administrator

Example images of the Avaya Multimedia Messaging migration process

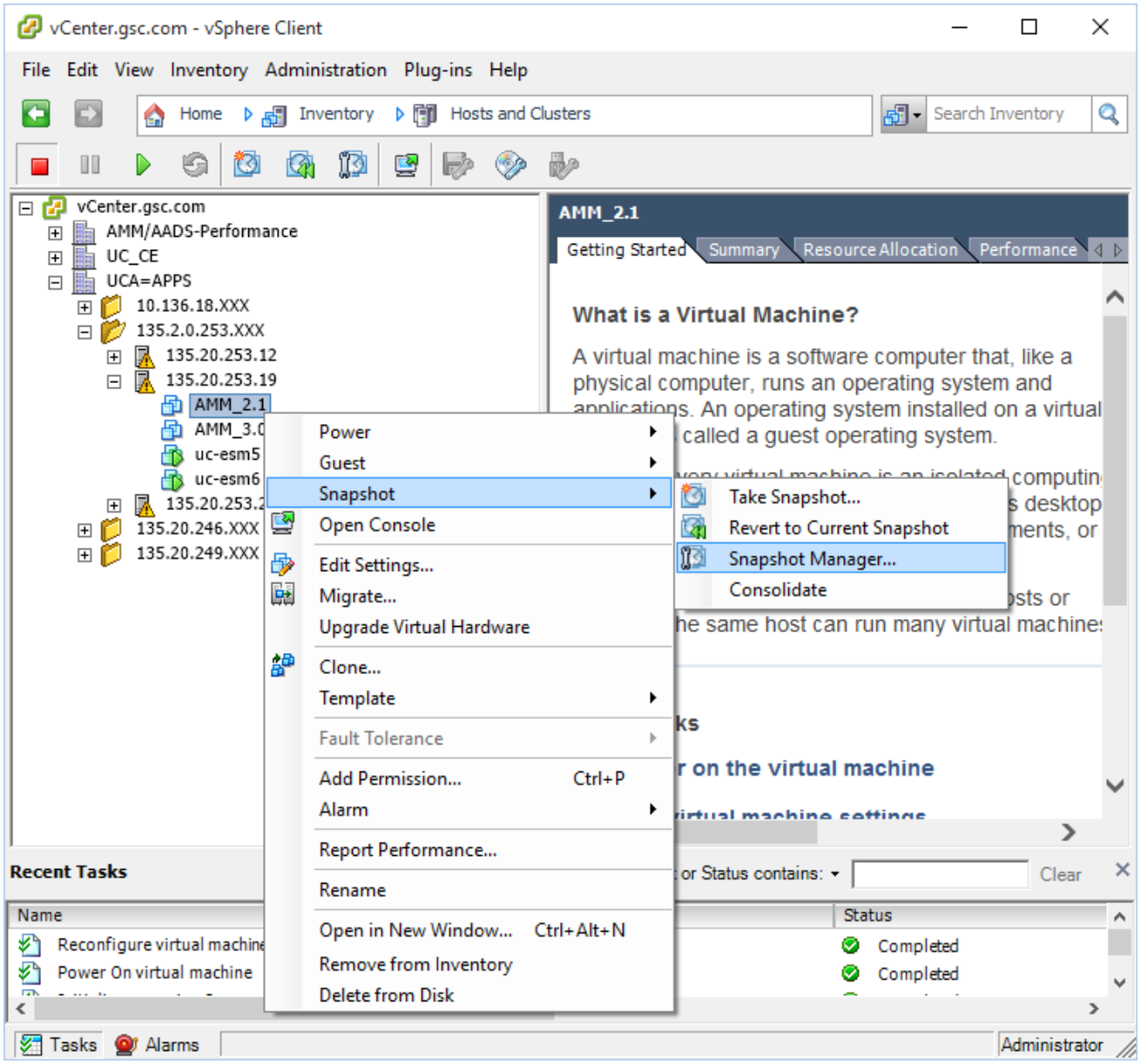


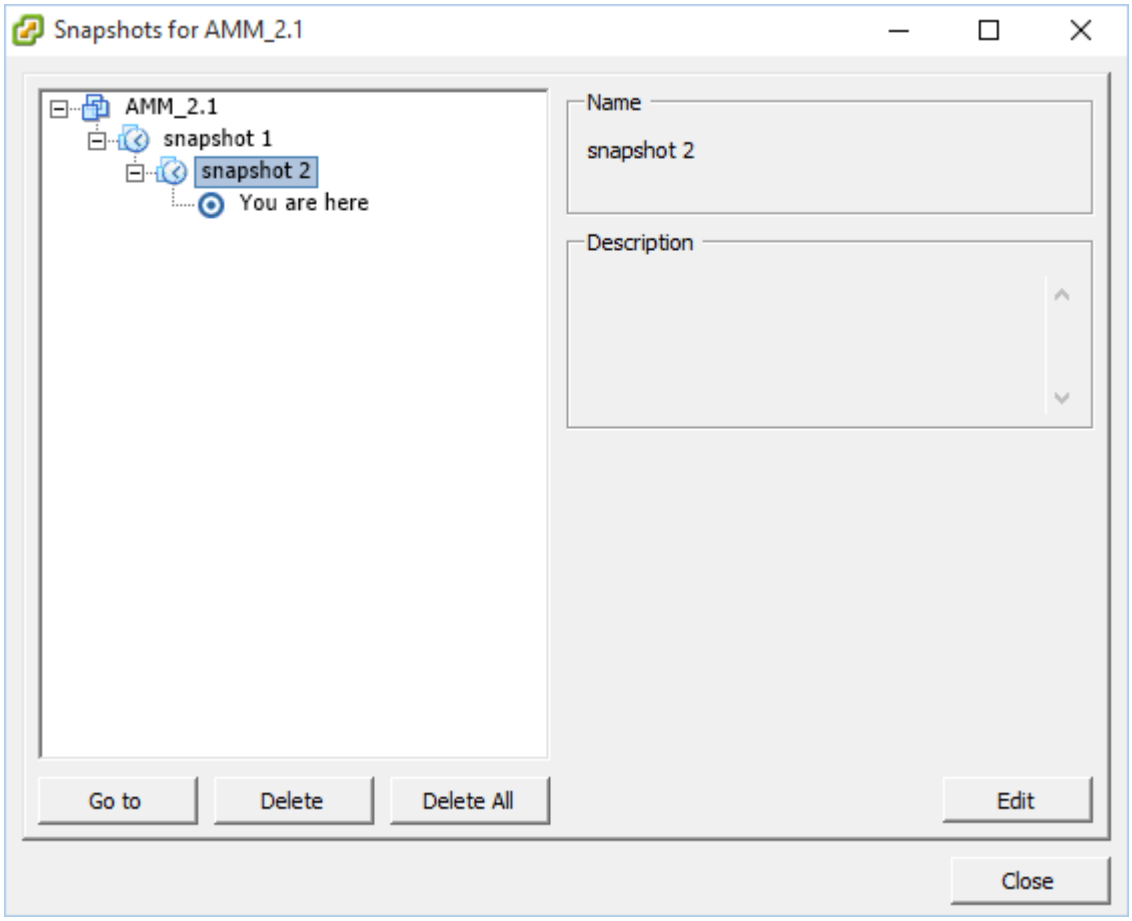


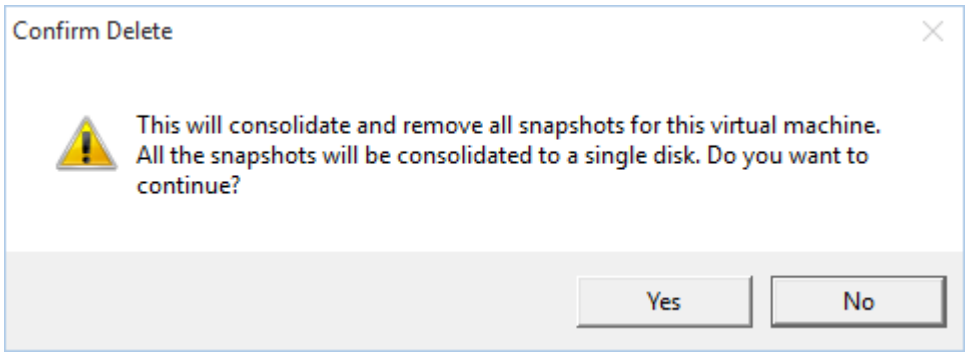
Deleting snapshots present on Release 2.1 virtual machine

The following images show the removal of all snapshots on the Release 2.1 virtual machine

Example images of the Avaya Multimedia Messaging migration process



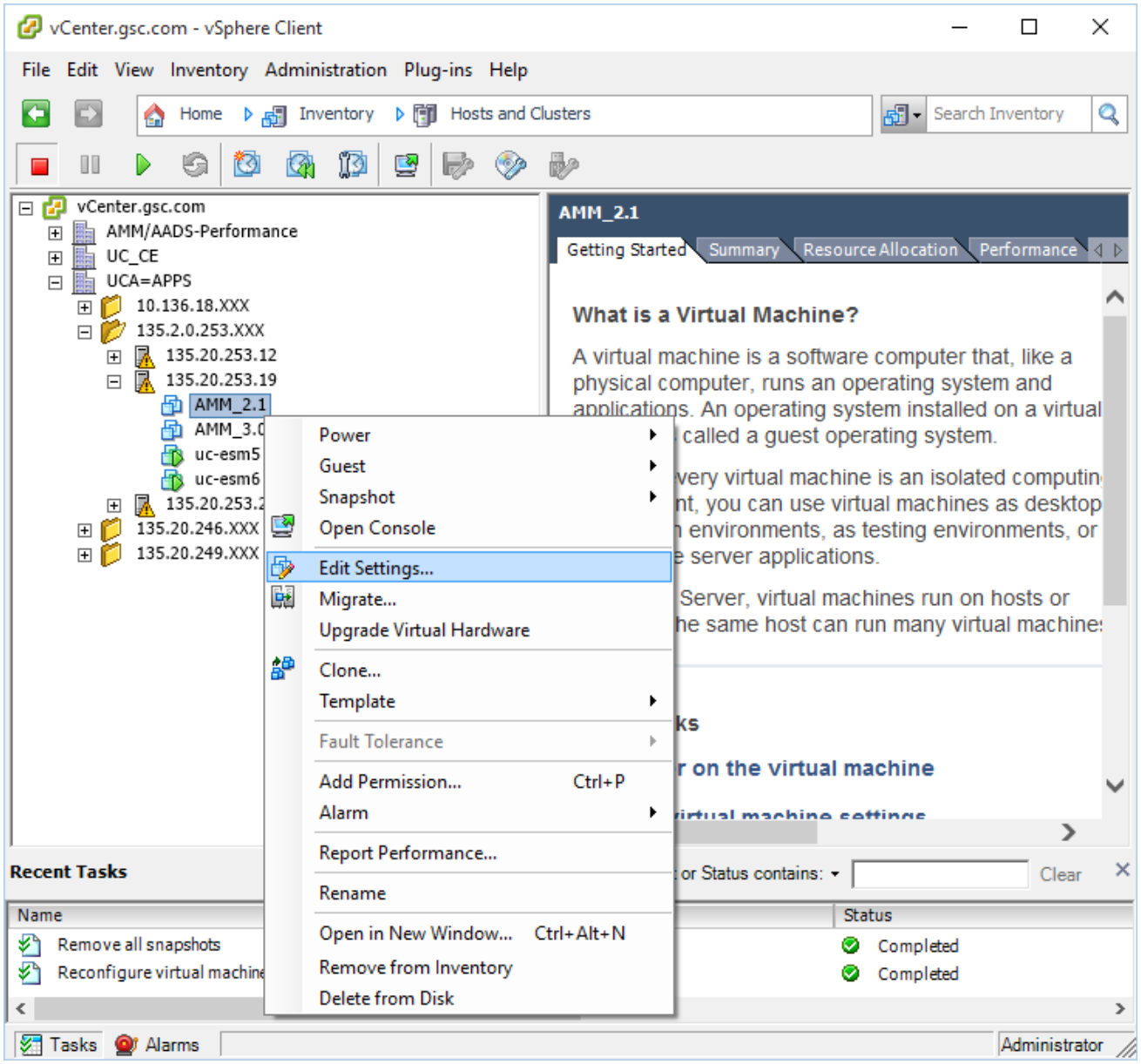


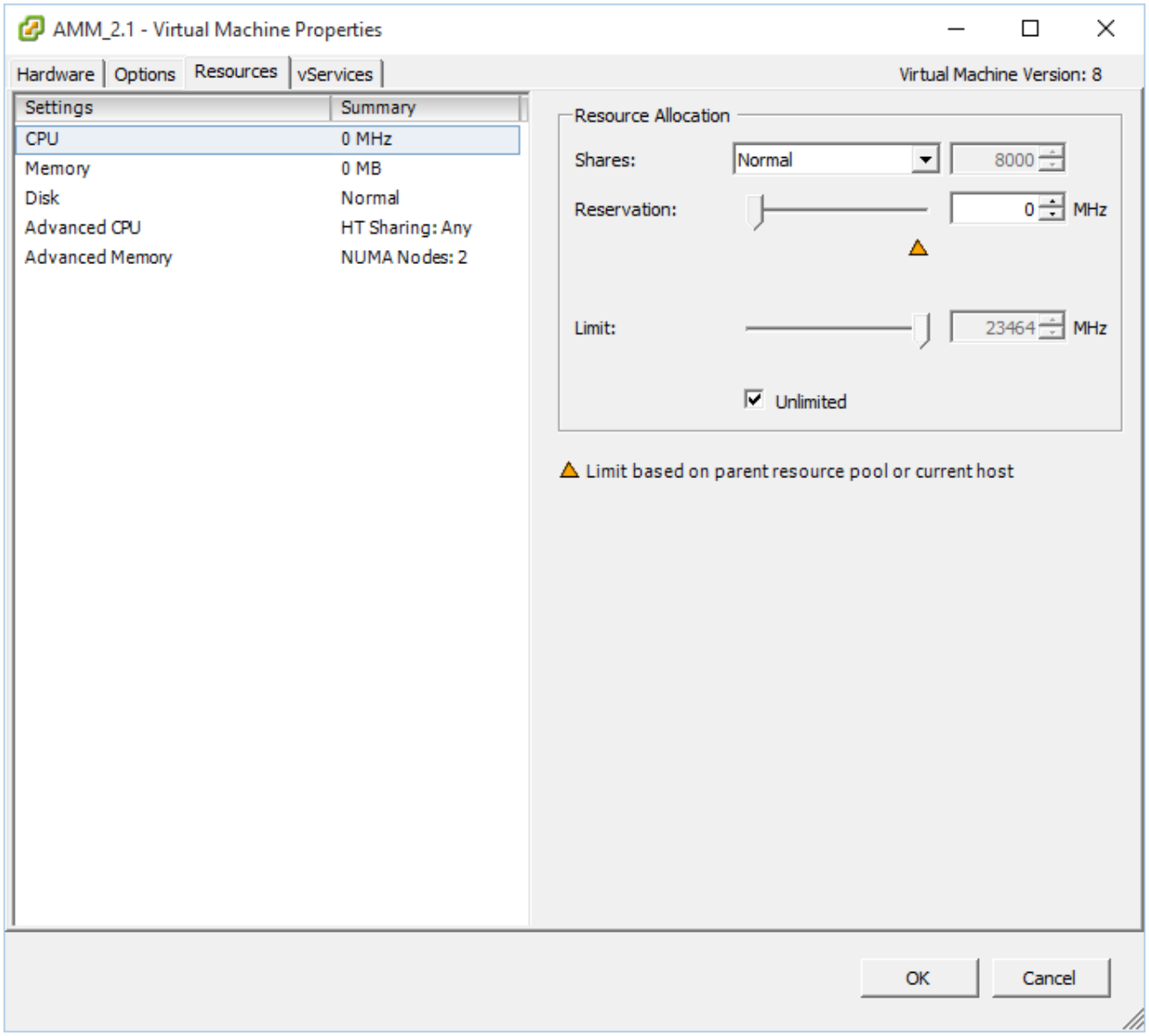


Removing media disk from Release 2.1 virtual machine

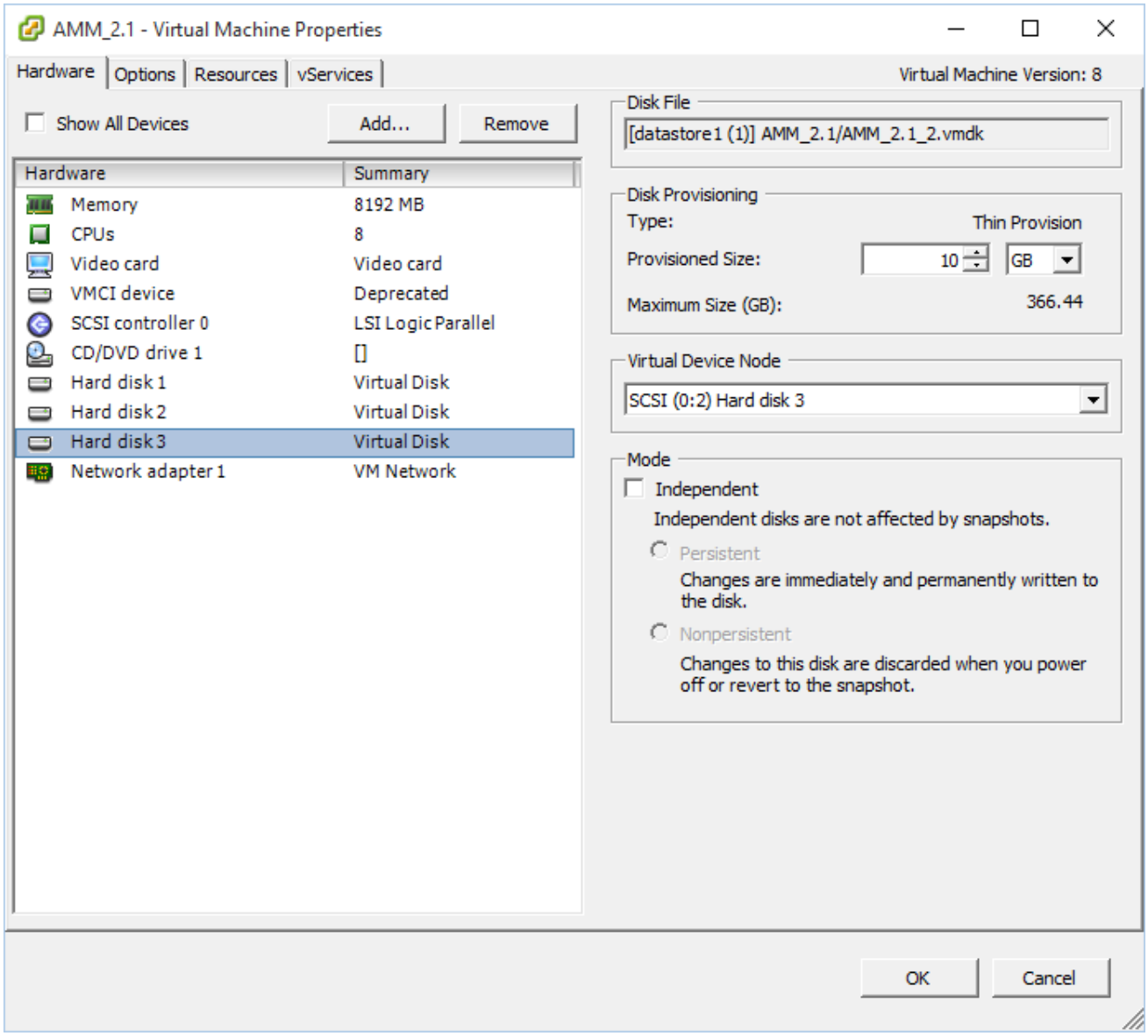
The following images show the removal of the media disk from the Release 2.1 virtual machine. The files for this virtual disk are retained on the file system of the hosting ESXi hypervisor.

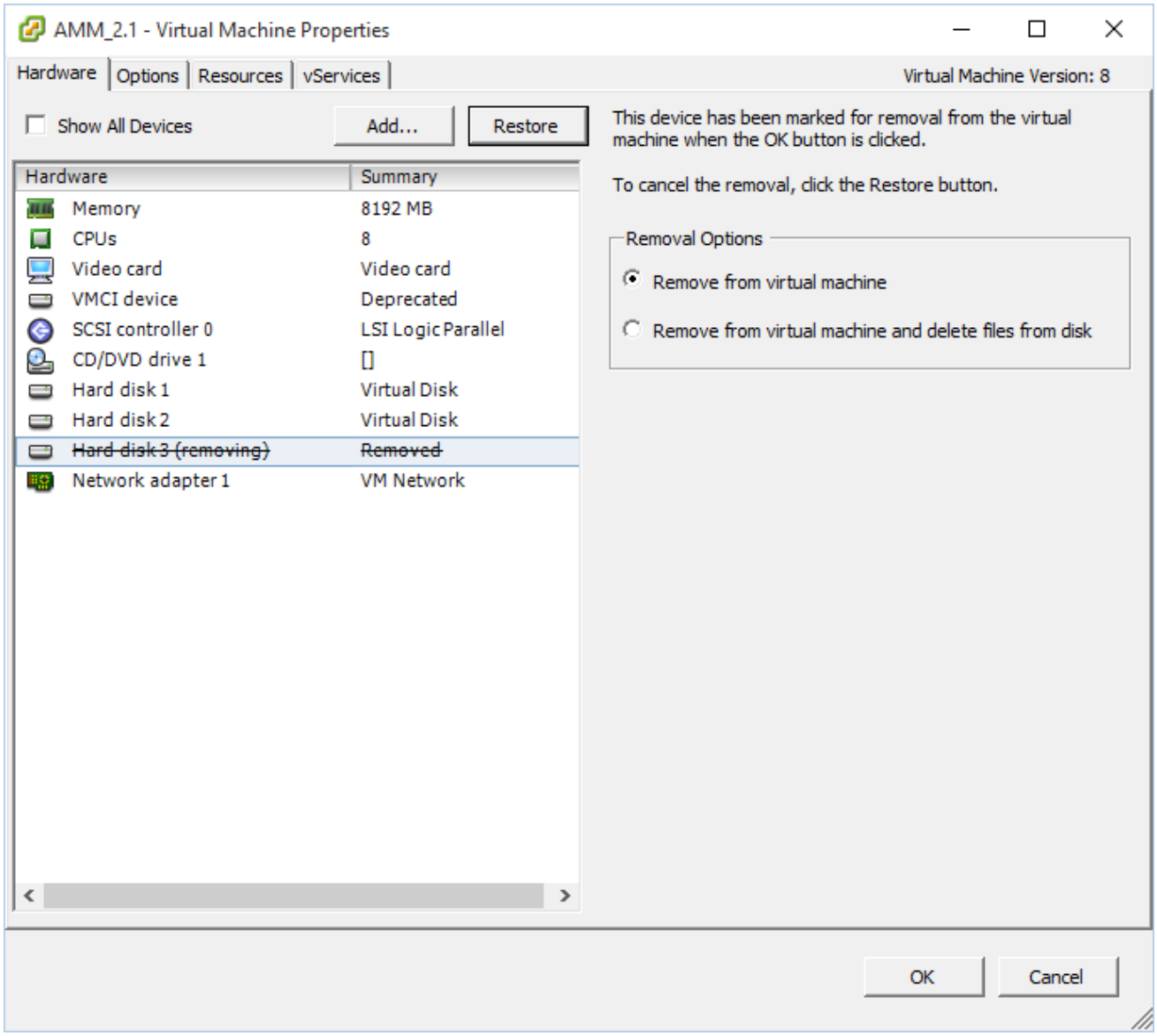
Example images of the Avaya Multimedia Messaging migration process




AMM_2.1 - Virtual Machine Properties
Hardware
Options
Resources
vServices
Virtual Machine Version: 8
Settings
Summary
CPU
0 MHz
Memory
0 MB
Disk
Normal
Advanced CPU
HT Sharing: Any
Advanced Memory
NUMA Nodes: 2
Resource Allocation
Shares:
Normal
8000
Reservation:
0
MHz
Limit:
23464
MHz
Unlimited
Limit based on parent resource pool or current host
OK
Cancel

Example images of the Avaya Multimedia Messaging migration process

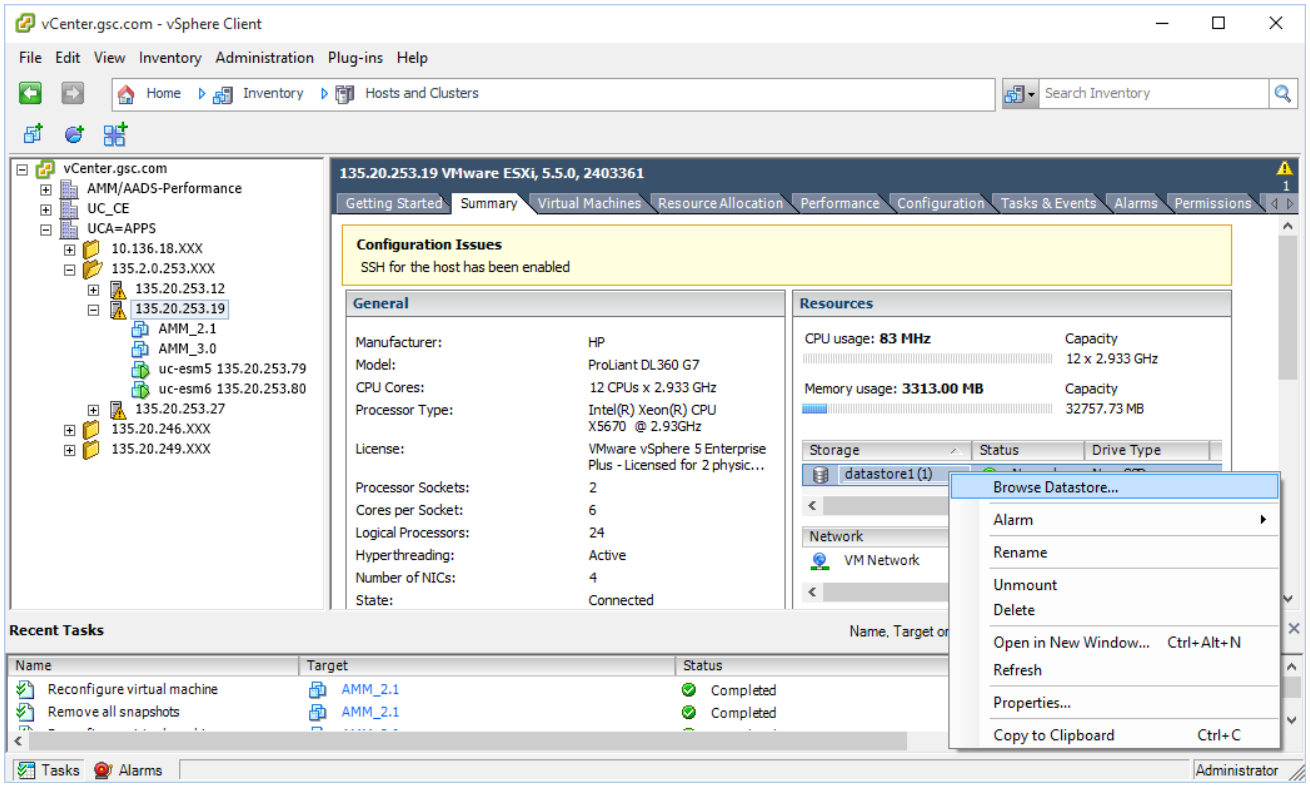


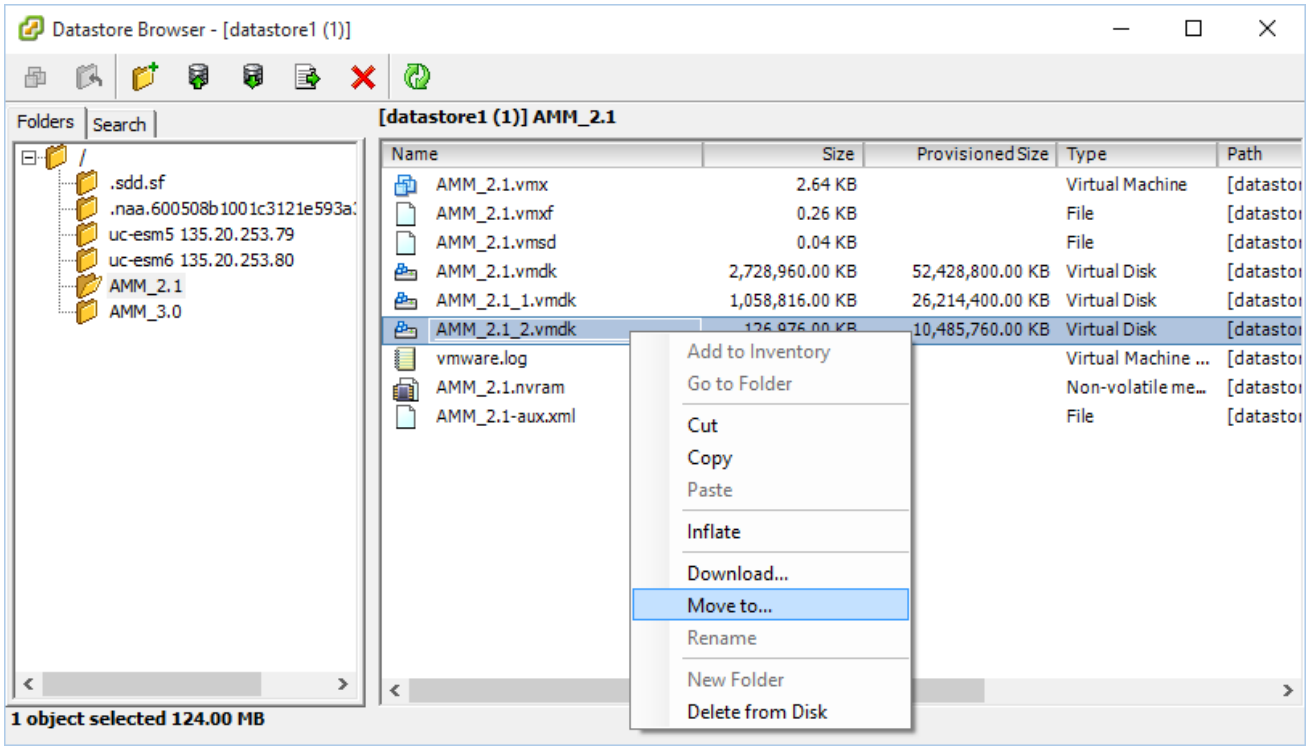


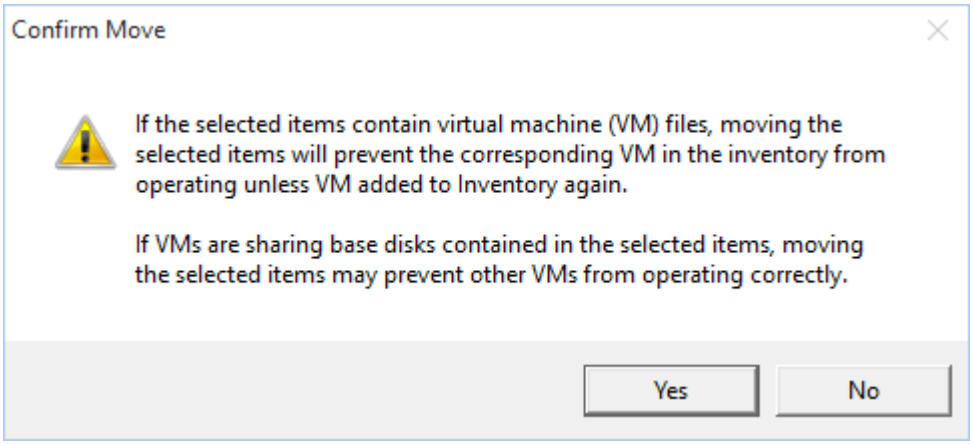
Moving media disk files from Release 2.1 to Release 3.0 virtual machine folder

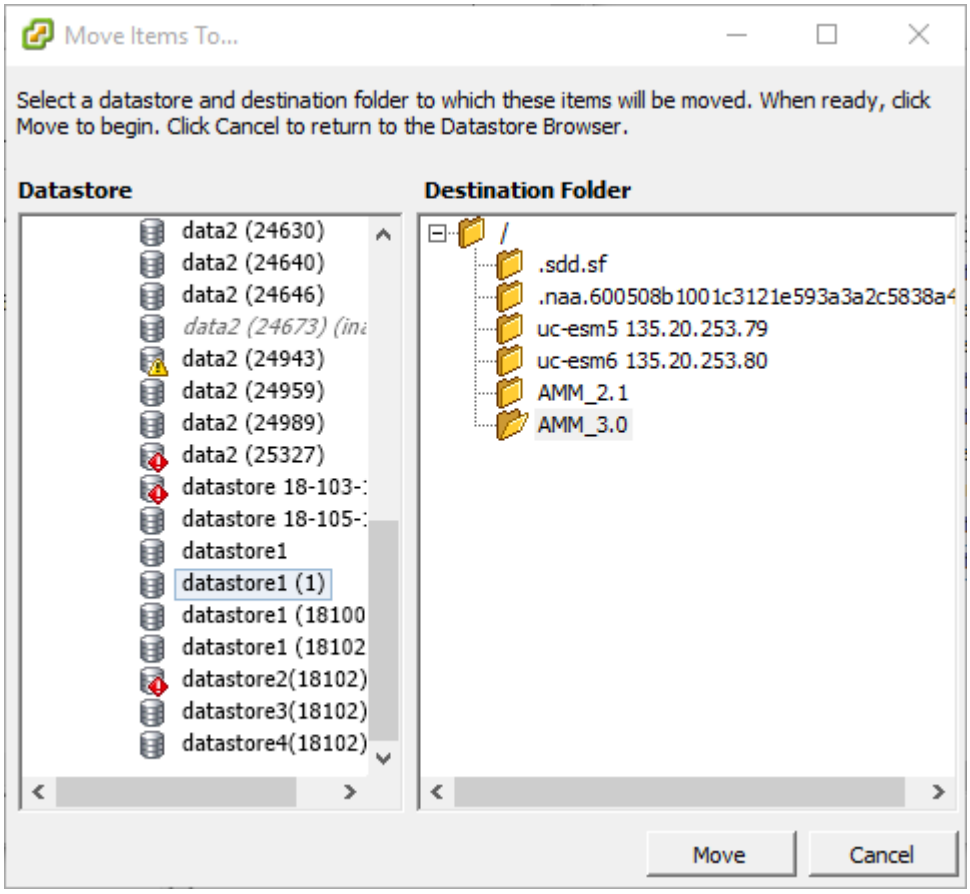
The following images show the relocation of the files that implement the media disk from the folder for the Release 2.1 virtual machine to the folder for the Release 3.0 virtual machine.

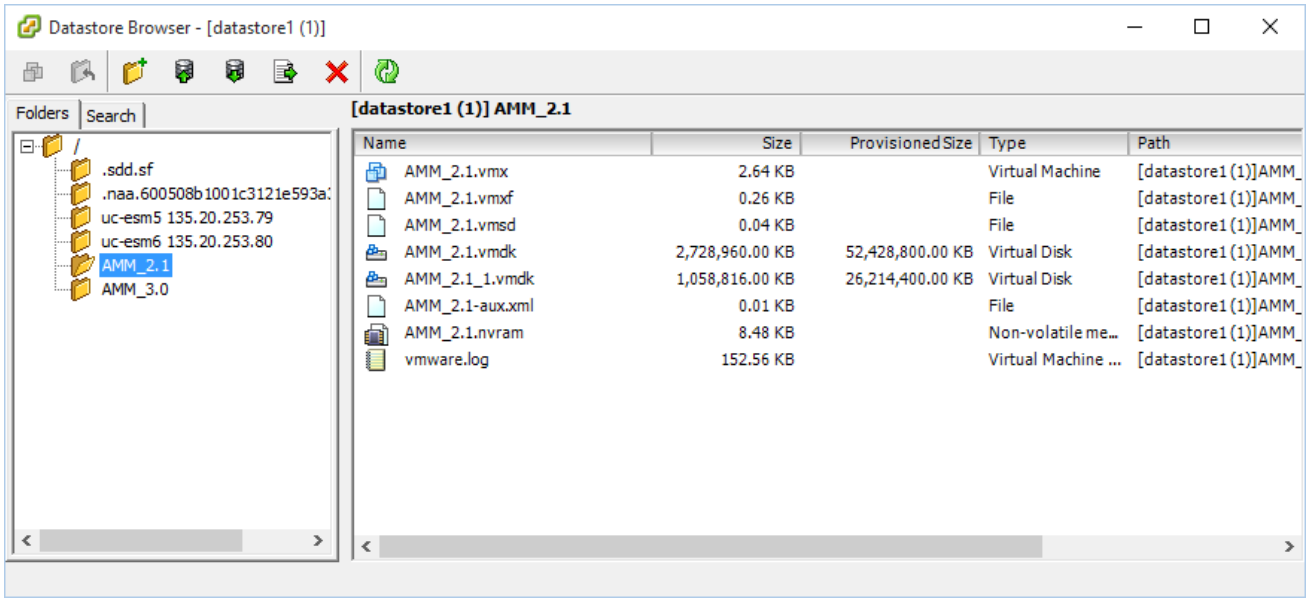
Example images of the Avaya Multimedia Messaging migration process

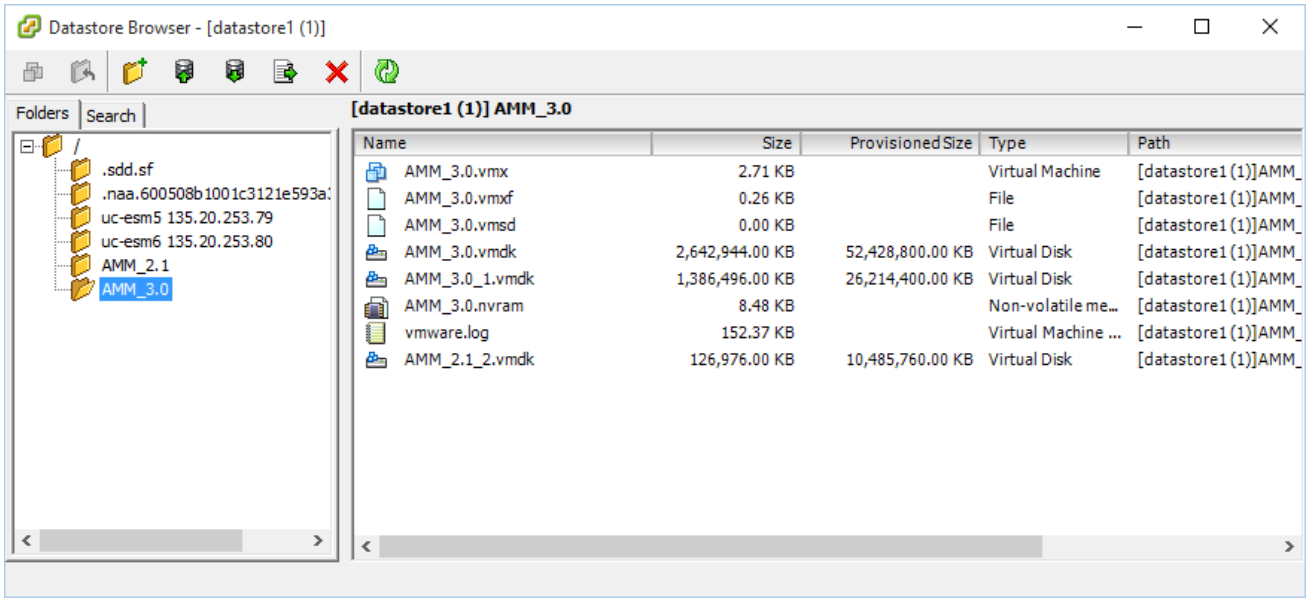





Confirm Move
If the selected items contain virtual machine (VM) files, moving the selected items will prevent the corresponding VM in the inventory from operating unless VM added to Inventory again.
If VMs are sharing base disks contained in the selected items, moving the selected items may prevent other VMs from operating correctly.
Yes
No

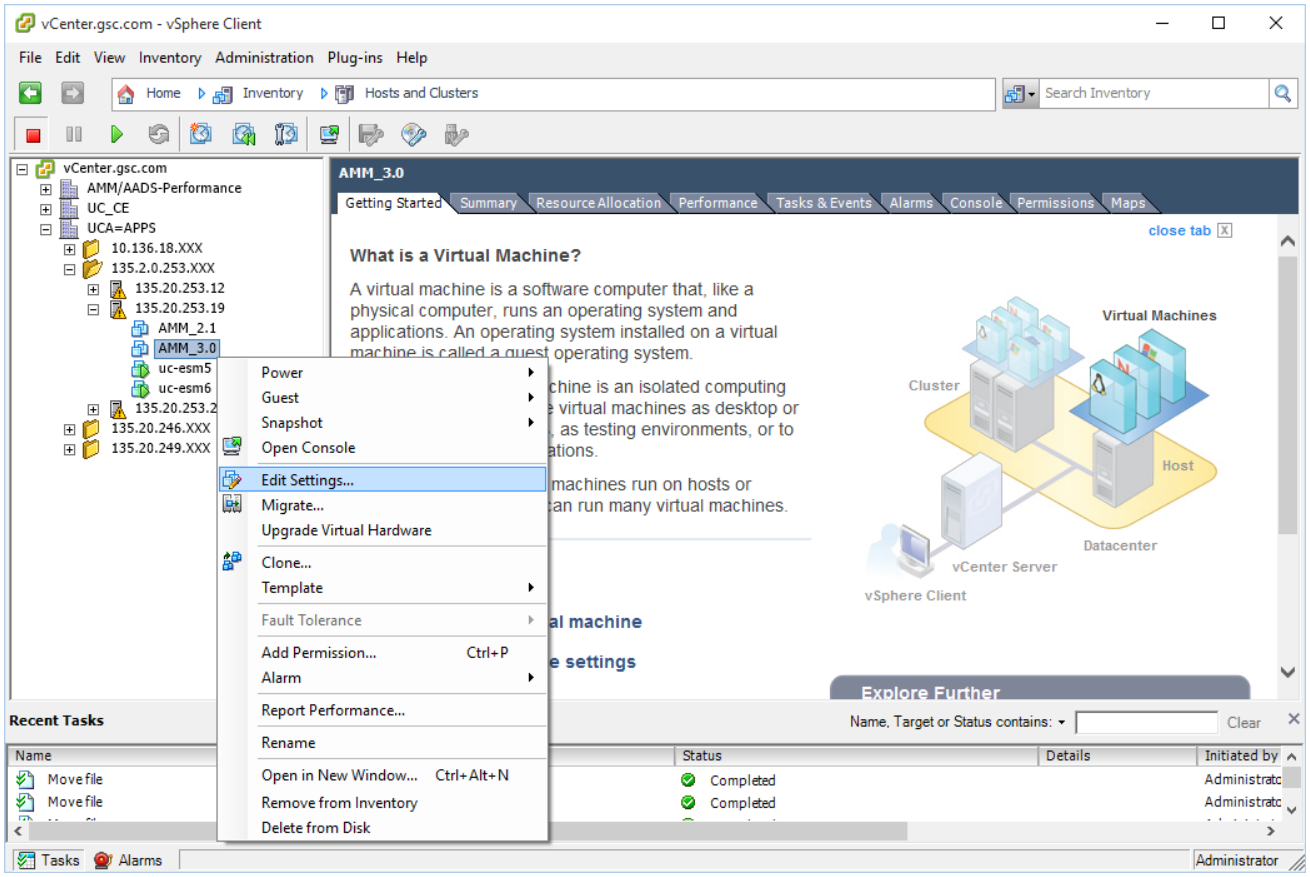

Move Items To...
Select a datastore and destination folder to which these items will be moved. When ready, click Move to begin. Click Cancel to return to the Datastore Browser.
Datastore
Destination Folder
data2 (24630)
data2 (24640)
data2 (24646)
data2 (24943)
data2 (24959)
data2 (24989)
data2 (25327)
datastore1
datastore1 (1)
datastore2(18102)
datastore3(18102)
datastore4(18102)
/
.sdd.sf
uc-esm5 135.20.253.79
uc-esm6 135.20.253.80
AMM_2.1
AMM_3.0
Move
Cancel



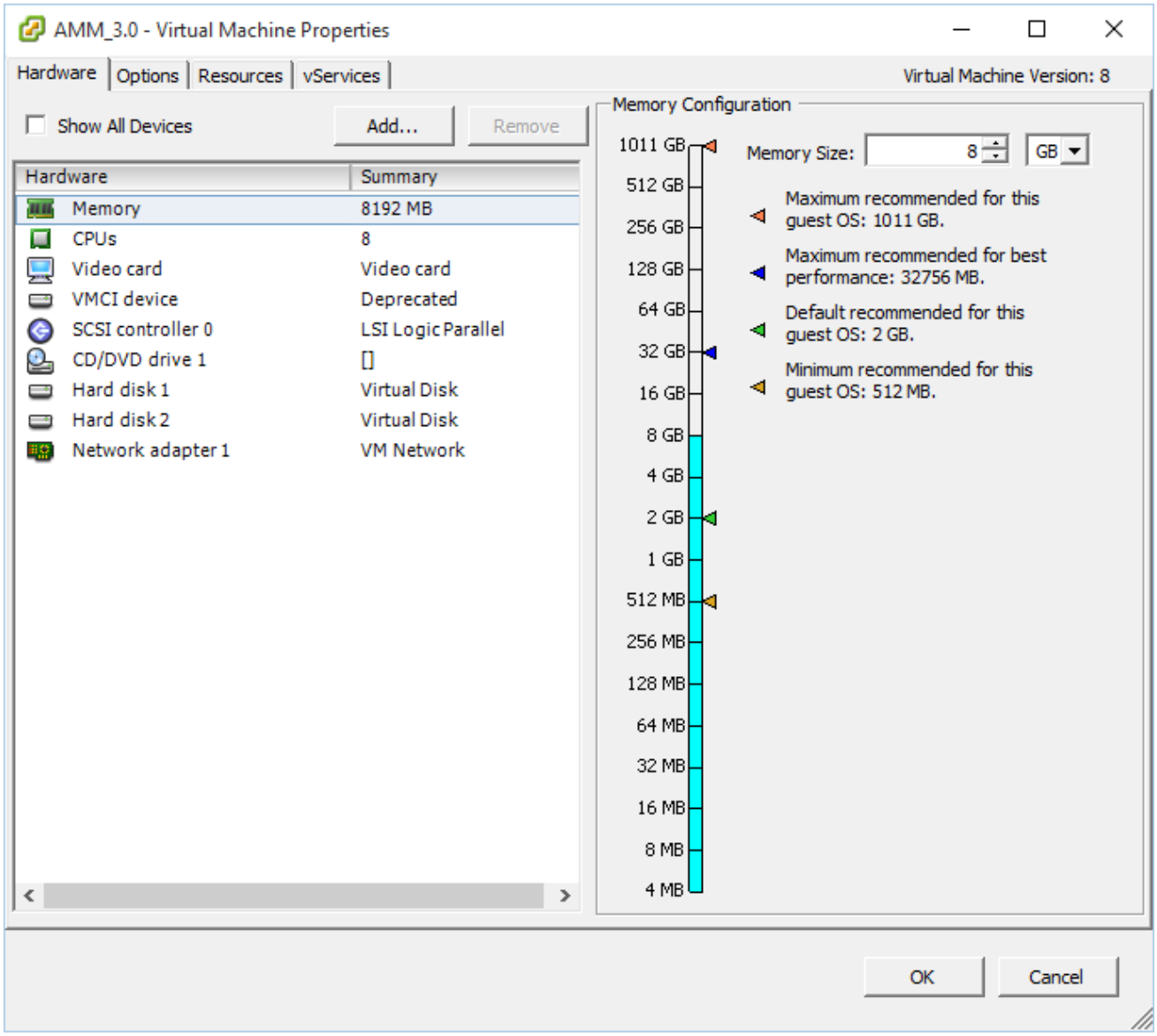


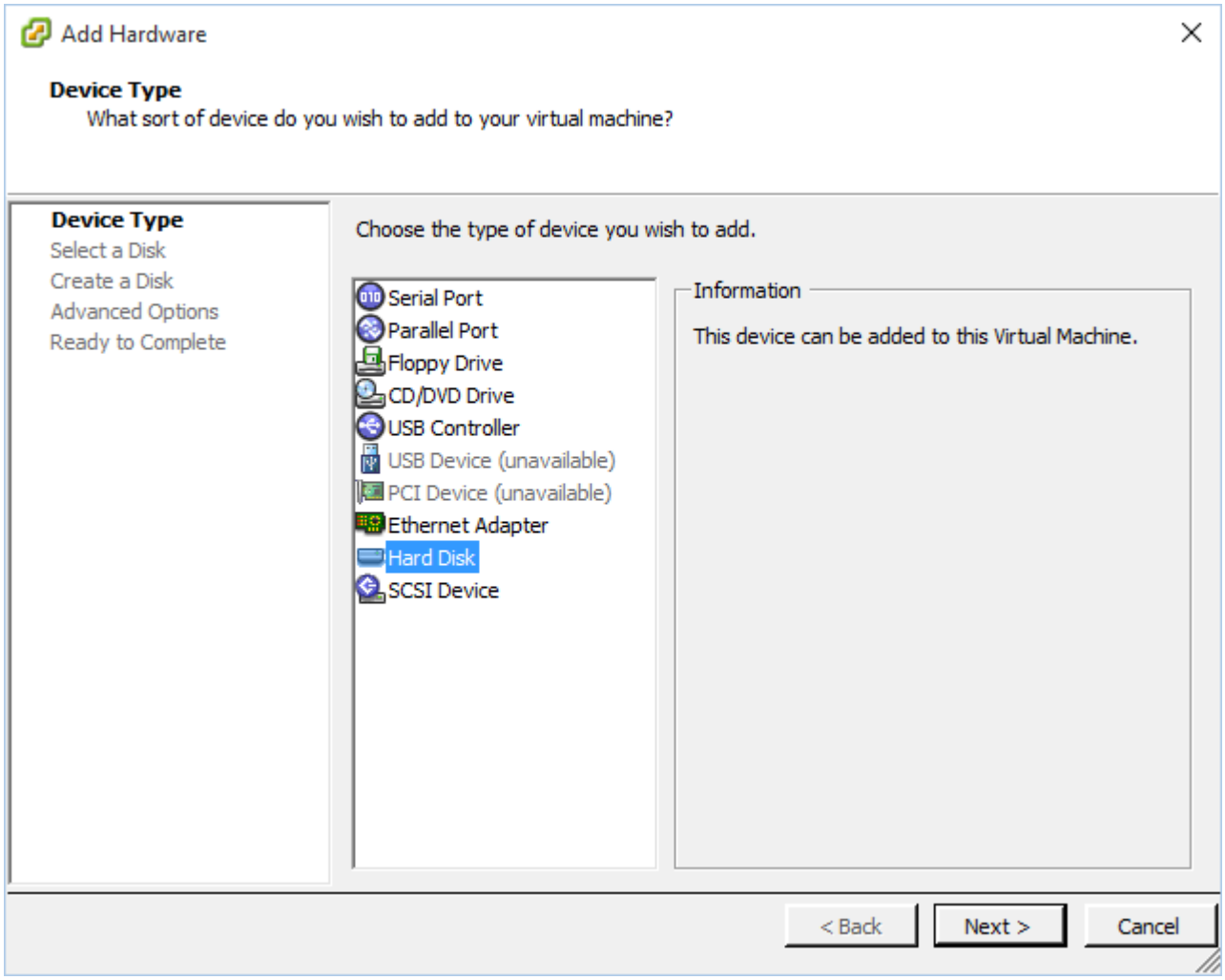
Adding the relocated disk to the Release 3.0 virtual machine

The following images show how to add the relocated virtual disk to the Release 3.0 virtual machine.

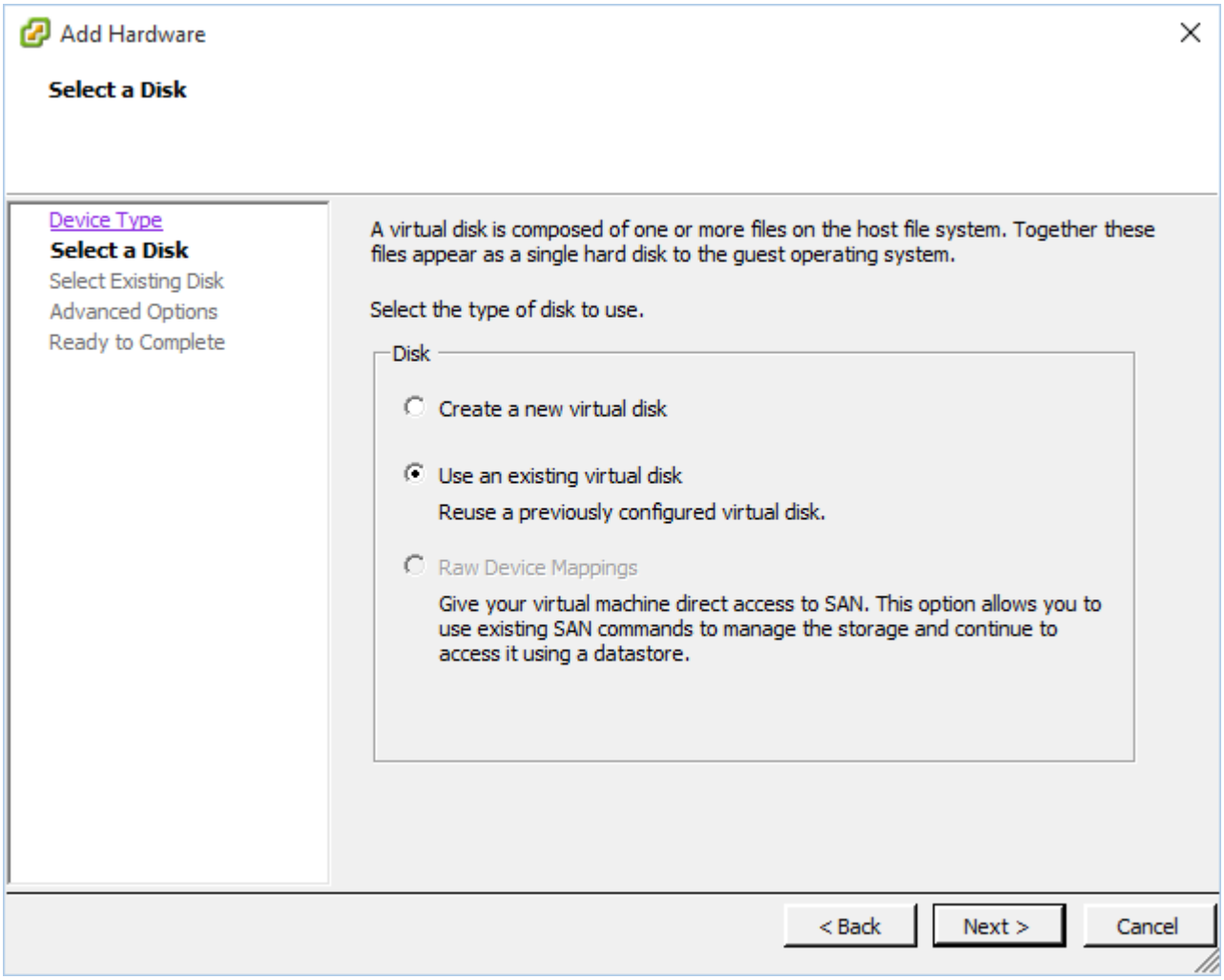

vCenter.gsc.com - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home
Inventory
Hosts and Clusters
Search Inventory
vCenter.gsc.com
AMM/AADS-Performance
UC_CE
UCA=APPS
10.136.18.XXX
135.2.0.253.XXX
135.20.253.12
135.20.253.19
AMM_2.1
AMM_3.0
uc-esm5
uc-esm6
135.20.253.2
135.20.246.XXX
135.20.249.XXX
AMM_3.0
Getting Started
Summary
Resource Allocation
Performance
Tasks & Events
Alarms
Console
Permissions
Maps
close tab
What is a Virtual Machine?
A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.
Virtual Machines
Cluster
Host
Datacenter
vCenter Server
vSphere Client
Explore Further
Power
Guest
Snapshot
Open Console
Edit Settings...
Migrate...
Upgrade Virtual Hardware
Clone...
Template
Fault Tolerance
Add Permission... Ctrl+P
Alarm
Report Performance...
Rename
Open in New Window... Ctrl+Alt+N
Remove from Inventory
Delete from Disk
Recent Tasks
Name, Target or Status contains:
Clear
Name
Status
Details
Initiated by
Move file
Completed
Move file
Completed
Tasks
Alarms
Administrator

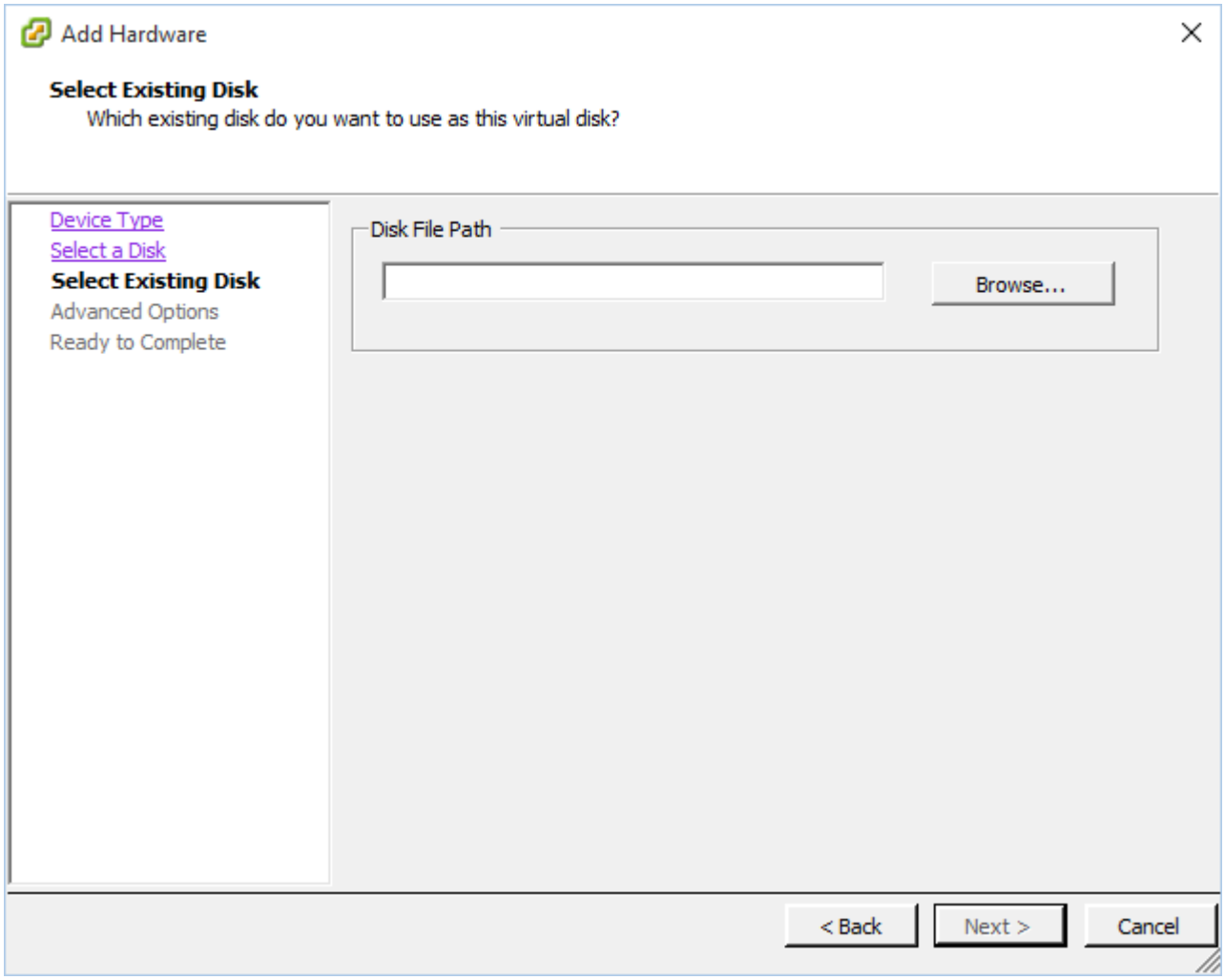
Example images of the Avaya Multimedia Messaging migration process



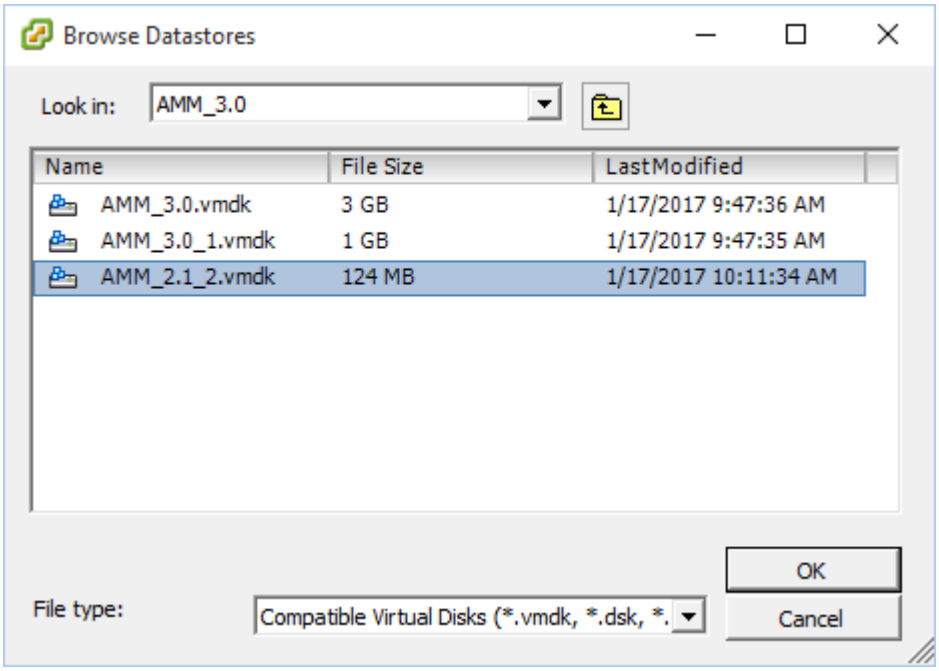

Add Hardware
Device Type
What sort of device do you wish to add to your virtual machine?
Device Type
Select a Disk
Create a Disk
Advanced Options
Ready to Complete
Choose the type of device you wish to add.
Serial Port
Parallel Port
Floppy Drive
CD/DVD Drive
USB Controller
USB Device (unavailable)
PCI Device (unavailable)
Ethernet Adapter
Hard Disk
SCSI Device
Information
This device can be added to this Virtual Machine.
< Back
Next >
Cancel

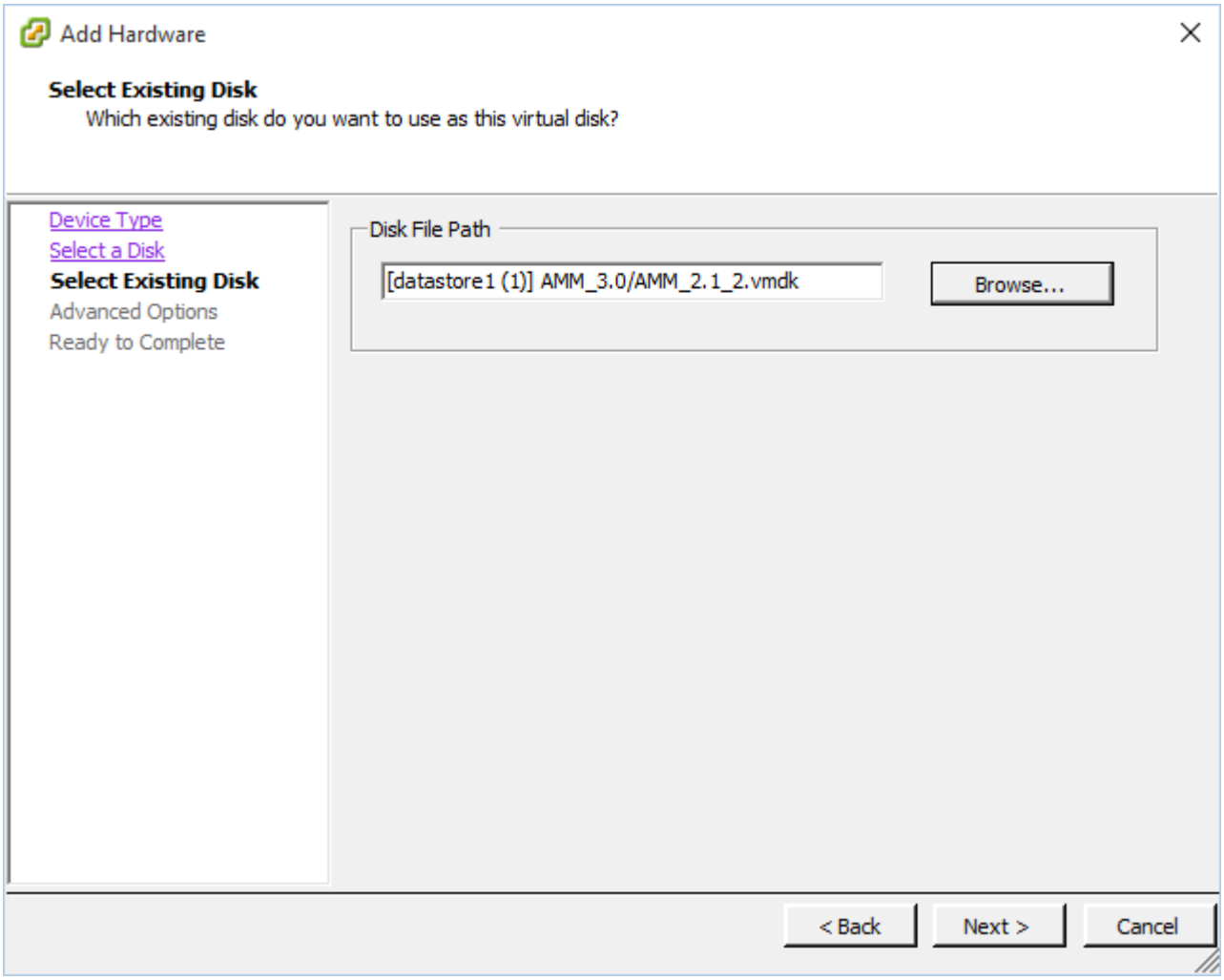
Example images of the Avaya Multimedia Messaging migration process

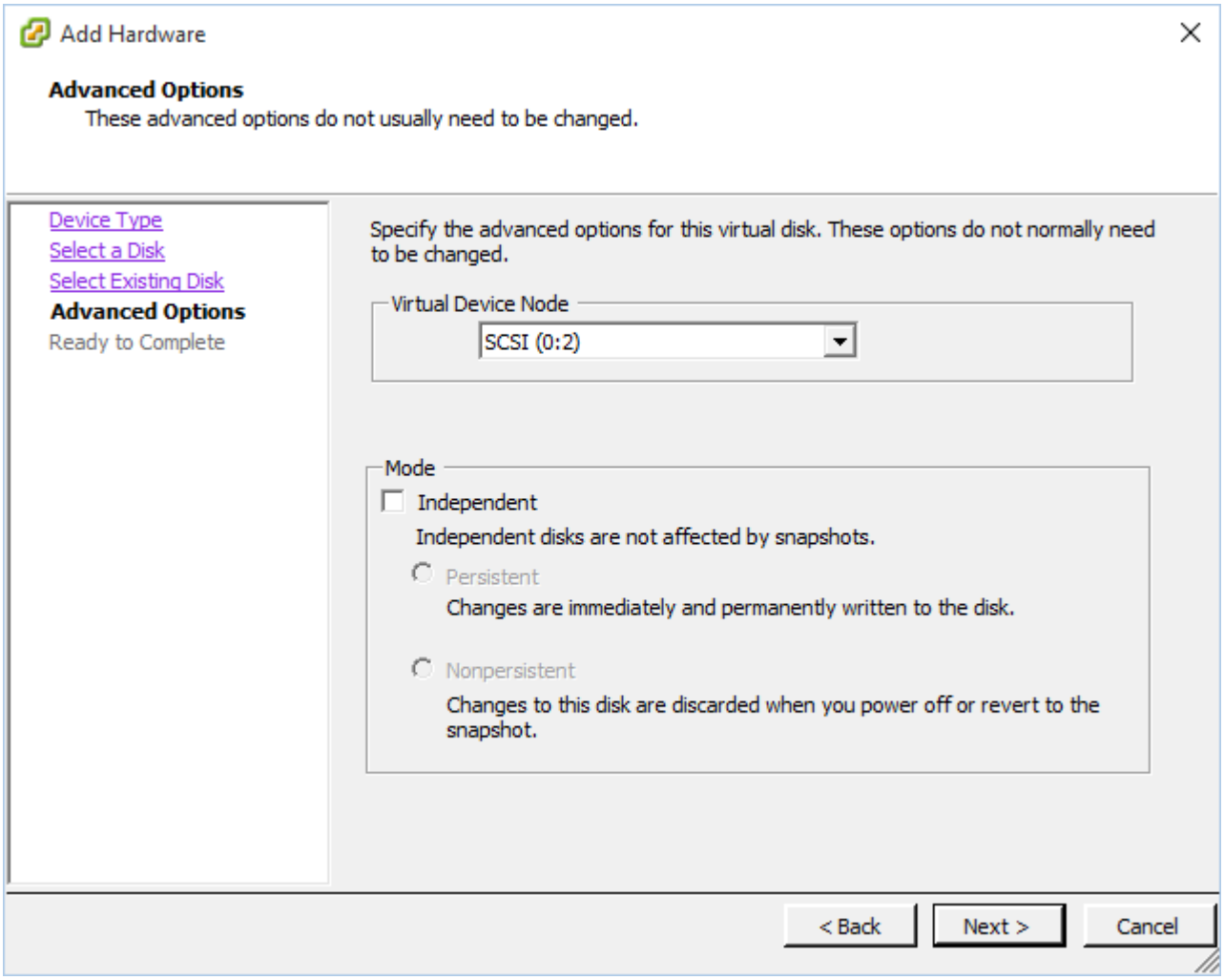


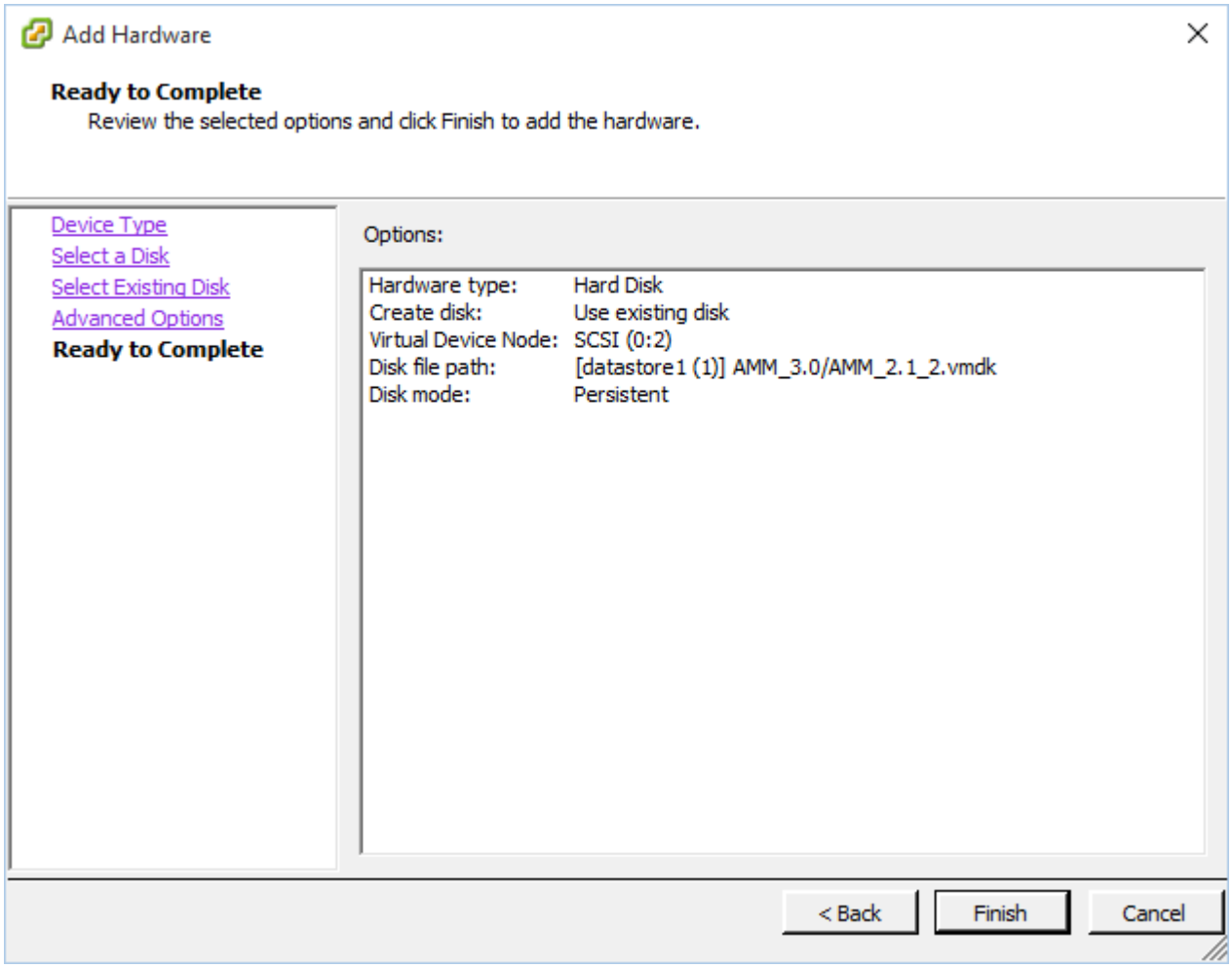

Add Hardware
Select Existing Disk
Which existing disk do you want to use as this virtual disk?
Device Type
Select a Disk
Select Existing Disk
Advanced Options
Ready to Complete
Disk File Path
Browse...
< Back
Next >
Cancel

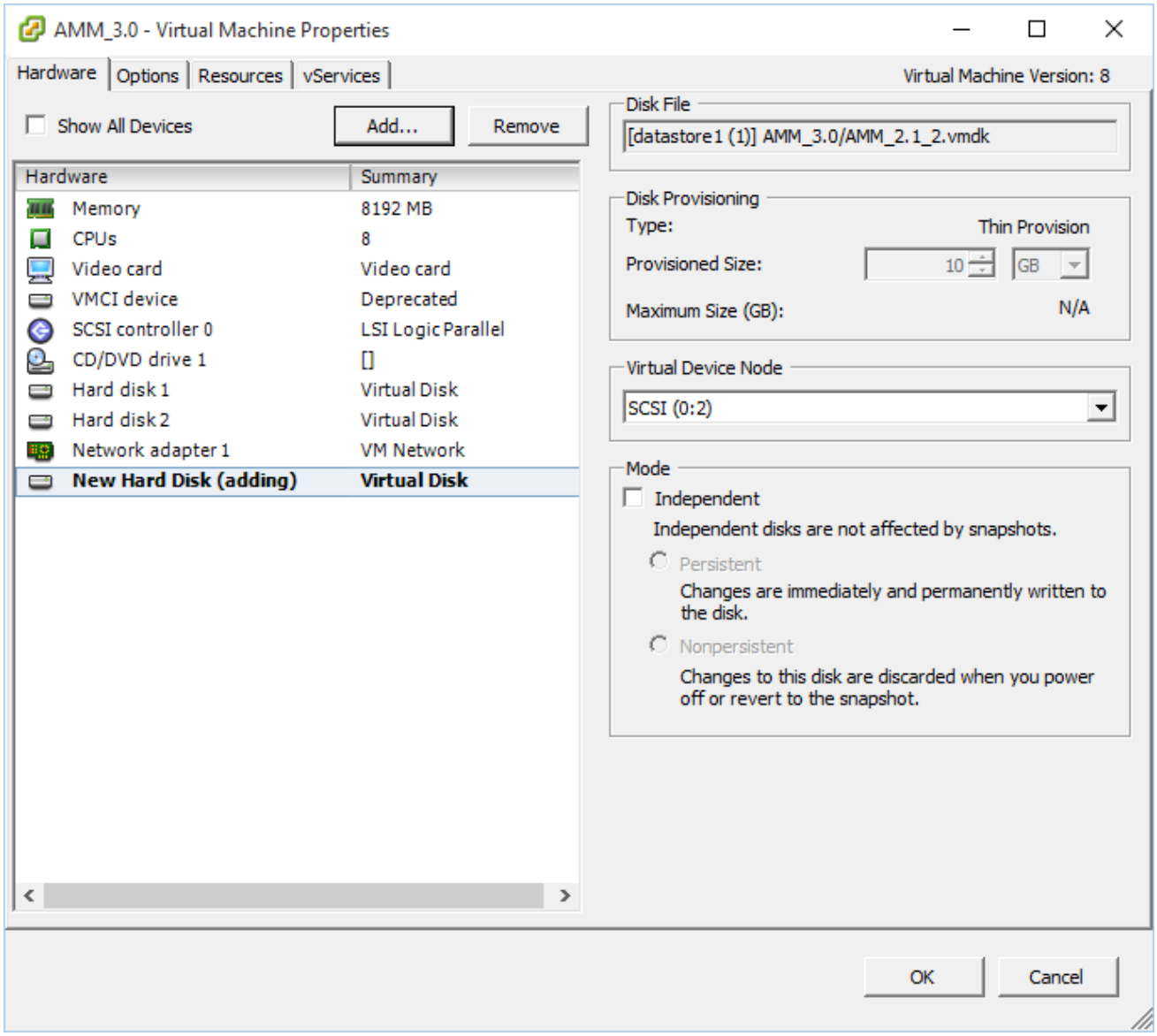
Example images of the Avaya Multimedia Messaging migration process




Add Hardware
Select Existing Disk
Which existing disk do you want to use as this virtual disk?
Device Type
Select a Disk
Select Existing Disk
Advanced Options
Ready to Complete
Disk File Path
[datastore1 (1)] AMM_3.0/AMM_2.1_2.vmdk
Browse...
< Back
Next >
Cancel

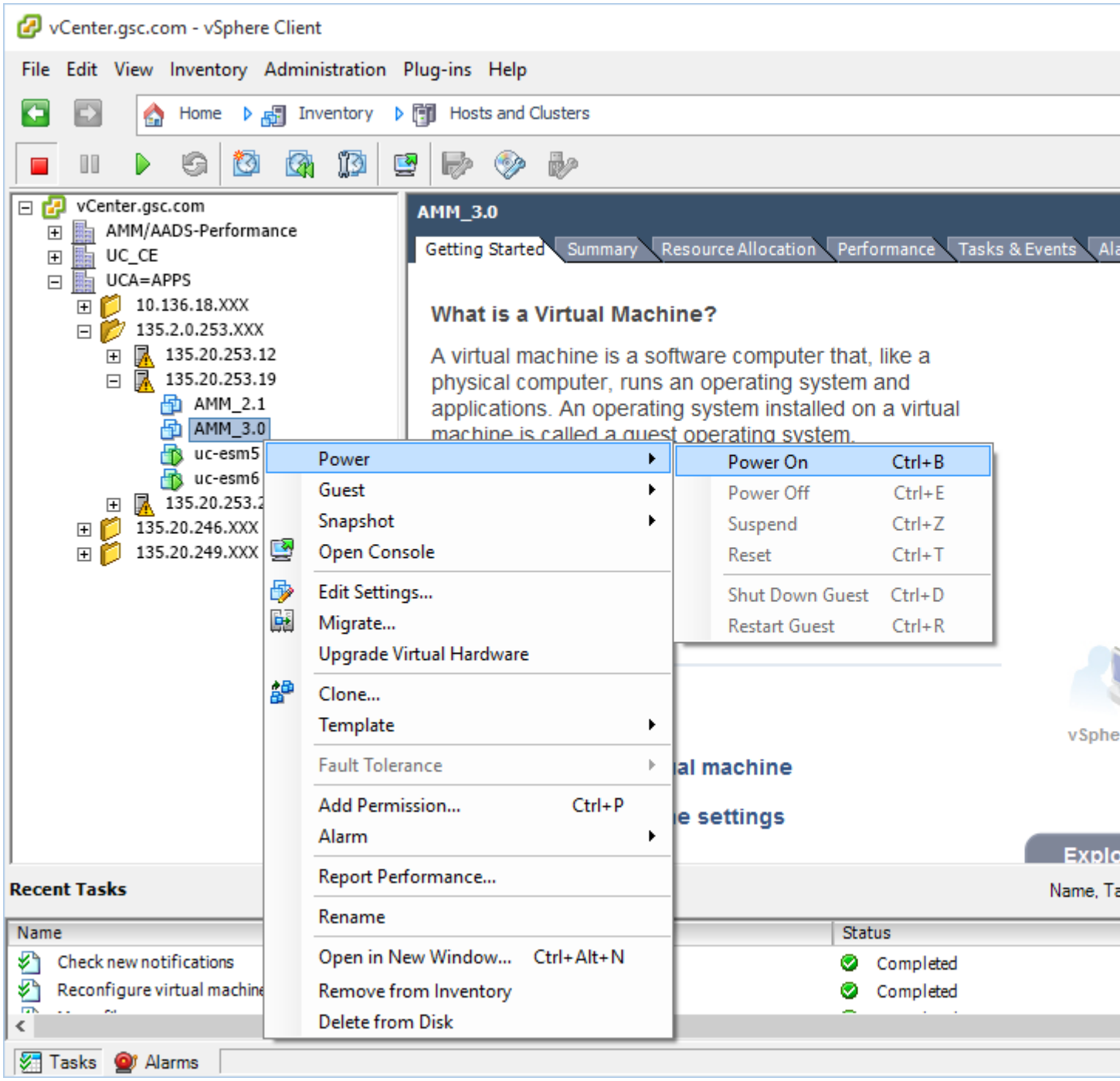

Add Hardware
Advanced Options
These advanced options do not usually need to be changed.
Device Type
Select a Disk
Select Existing Disk
Advanced Options
Ready to Complete
Specify the advanced options for this virtual disk. These options do not normally need to be changed.
Virtual Device Node
SCSI (0:2)
Mode
Independent
Independent disks are not affected by snapshots.
Persistent
Changes are immediately and permanently written to the disk.
Nonpersistent
Changes to this disk are discarded when you power off or revert to the snapshot.
< Back
Next >
Cancel


Add Hardware
Ready to Complete
Review the selected options and click Finish to add the hardware.
Device Type
Select a Disk
Select Existing Disk
Advanced Options
Ready to Complete
Options:
Hardware type: Hard Disk
Create disk: Use existing disk
Virtual Device Node: SCSI (0:2)
Disk file path: [datastore1 (1)] AMM_3.0/AMM_2.1_2.vmdk
Disk mode: Persistent
< Back
Finish
Cancel



Powering on the Release 3.0 virtual machine

The following image shows how to power on the virtual machine. After the virtual machine is powered up, the contents at the `/media/data` mount point are those that were previously at that mount point on the Release 2.1 virtual machine.


vCenter.gsc.com - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home
Inventory
Hosts and Clusters
vCenter.gsc.com
AMM/AADS-Performance
UC_CE
UCA=APPS
10.136.18.XXX
135.2.0.253.XXX
135.20.253.12
135.20.253.19
AMM_2.1
AMM_3.0
uc-esm5
uc-esm6
135.20.246.XXX
135.20.249.XXX
AMM_3.0
Getting Started
Summary
Resource Allocation
Performance
Tasks & Events
What is a Virtual Machine?
A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.
Power
Guest
Snapshot
Open Console
Edit Settings...
Migrate...
Upgrade Virtual Hardware
Clone...
Template
Fault Tolerance
Add Permission... Ctrl+P
Alarm
Report Performance...
Rename
Open in New Window... Ctrl+Alt+N
Remove from Inventory
Delete from Disk
Power On Ctrl+B
Power Off Ctrl+E
Suspend Ctrl+Z
Reset Ctrl+T
Shut Down Guest Ctrl+D
Restart Guest Ctrl+R
Recent Tasks
Name
Status
Check new notifications
Reconfigure virtual machine
Completed
Completed
Tasks
Alarms

Glossary

API	Application Programming Interface
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).
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.
Lightweight Directory Access Protocol (LDAP)	An application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.
Network Management System	A system that lets you monitor the health and status of devices on your data network.
NTP (Network Time Protocol)	A protocol used to synchronize the real-time clock in a computer.
REST	Representational state transfer. This is a software architectural style used with Application Programming Interfaces (APIs).
RSA	A public-key cryptographic system used for secure data transmission.
Secure Shell (SSH)	Secure Shell (SSH) is a group of standards and an associated network protocol that the system can use to establish a secure channel between a

	local and a remote computer. SSH uses public-key cryptography to mutually authenticate a user and a remote computer. SSH uses encryption and message authentication codes to protect the confidentiality and integrity of the data that is exchanged between the two computers.
Service record (SRV record)	A specification of data in the Domain Name System defining the location, i.e. the hostname and port number, of servers for specified services.
Simple Network Management Protocol (SNMP)	A protocol for managing devices on IP networks.
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

A

Aborting virtual machine migration 237
adaptation
    Lync 136
adapter
    fields 208
    Lync 136
add certificate to Lync 150
Add End Entity 167
adding
    AMM nodes to local host resolution table 137
    Lync adapter 136
    Lync certificate to each node 109
    Lync user 159
    reverse proxy 177
    static route destination 149
adding Lync certificate
    Avaya Multimedia Messaging cluster 110
adding to truststore
    Presence Services certificate 241
additional security information 23
Adjusting the CPU resource of a virtual machine 191
Adjusting the memory resource of a virtual machine 191
adjusting the size
    disk volumes 193
    Linux commands 195
Adjusting the size of virtual disks 192
Adjusting the virtual hardware of virtual machines 190
Adjusting the virtual network interface 192
administration
    LDAP attribute mappings 187
    multisite configuration 190
    rollback operations 244
    secondary System Manager 224
administration portal
    performance 188
administration tools 217
    cleanAMM.sh 221
    clitool 222
    collectLogs 223
    collectNodes 223
    gluster volume status 219
    nodetool 220
application media attributes
    setting 139
applying
    Avaya Multimedia Messaging patches 245
archiving 224
assigning certificate 154
attribute mapping use cases 32
attributes
    users 160
audit audispd logs 202
Avaya Multimedia Messaging
    cluster with configuration with Lync federation 157
    Lync 135
    Lync trusted server 145
    server 146, 147
    SIP entities 138
    trusted Lync server 146, 147
Avaya Multimedia Messaging cluster
    adding Lync certificate 110
    configuration with Lync Federation 157
    configuring users 139
Avaya Multimedia Messaging server
    DNS host 150
    host name 142

B

backup
    certificates 111
backup and restore 209, 212
    backupAMM.sh 211
    backup of a node 210
    remove gluster 215
    remove gluster after gluster is formally removed 216
    restore cluster 213
    restore standalone node 211

C

CA certificate
    trust store 155
certificate
    invalid 253
    Lync 111
    missing 253
certificate authority 108
Certificate Enrollment 168
certificate file
    uploading 169
certificates 102
    backing up in Firefox 111
    intermediate CA certificate 107
    local certificates 105
    System Manager certificate 105
certificate template
    creating 153
certificate using CSR
    create 168
checklist
    Avaya Multimedia Messaging configuration for Lync . 142
    cluster configuration with Lync federation 157
    planning 18

checklist *(continued)*
pre-configuration 18
user configuration 159
client administration
adding messaging domains 183
deleting a messaging domain 183
client settings
adding a new domain 183
client settings
deleting a messaging domain 183
messaging domains 183
cluster
add node 73
change cassandra password 74
change cassandra username 74
change LDAP parameters after install 75
changing seed node 75
install additional cluster node 69
installation 64
install cluster 65
installing cluster node 67
rebalance gluster 73
cluster installation 64
command values
Windows Domain Controller 205
communication profile
users 140
complete migration 236
Completing the server migration 236
configuration
active directory 203
advanced configuration 100
Avaya SBCE for remote access 163
certificates 84
cluster configuration 98
database settings 97
DNS 28
external configurations 162
firewall configuration 101
front-end host 84
import secure LDAP certificate 114
internal domain Lync server 145
IWA 203
LDAP configuration 87
LDAP settings 113
local site 190
Lync trusted server 145
Lync users 160
messaging domains 112, 113
multisite 190
multisite adapter 207
Presence 129
remote access 163
remote site 190
routing domain selection 27
system manager 84
System Manager 135
update Linux kernel 45
Windows Domain Controller 203
configuration prerequisites 25
configuration tasks 82
configure
managed elements 33
message playback login message 161
messaging domains 97
NTP server 46
run configuration script 83
System Manager 33
configuring
from forking 102
static route destination 149
configuring external systems 25
configuring Presence federation 131
connector
multisite adapter 207
creating
client profile 175
CSR 165
Gluster 72
new TLS server profile 172
creating an end entity 167
creating certificate template 153
Creating certificate using certificate signing request 168
creating keystore
from System Manager 110
with subject-alt-name 110

D

daily reports 222
Data Replication Service 240, 245
migration 240
Data Replication Service synchronization 245
deploying OVA image
deploy OVA to a vCenter 50
vCenter 50
Deploying the AMM OVA to a standalone ESXi host 51
Deployment options 50
deployment process 17
Deploy OVA to a standalone host 51
disabling
enhanced access security gateway 61, 178
disk volume adjustment 193
DNS
configuration 28
DNS configuration 25
Avaya Multimedia Messaging server 157
Lync client 156
Lync server 156
DNS service records 156
Lync client 156
document changes 11
domain
reachable 26

domain configuration
address types ... 26
domains ... 154
for Lync address ... 140
downloading software ... 21
downloading the system manager certificate ... 171

E

enabled port
Lync server ... 145
enabling
enhanced access security gateway ... 61, 178
enabling EASG
physical server ... 62, 179
end entry
create ... 167
enterprise directory settings ... 186
expanding
Gluster ... 72
Extending disk volumes ... 60

F

feature entitlements ... 185
federation
Lync ... 108
federation configuration
HTTPS REST interface ... 133
presence ... 129
Presence server GUI ... 129
using admin portal ... 132
XMPP interface ... 132
federation connections ... 187
federation settings ... 187
field description
TLS Certificates screen ... 166
field descriptions
cluster nodes ... 188
feature entitlements ... 185
new profile ... 175
new server profile screen ... 173
file system
Gluster ... 72
FQDN ... 30

G

getting
Lync certificate from CA ... 108
Gluster ... 72

H

hardware
physical deployment ... 16
VMWare ... 16
home site ID
multisite needfs to review from an intadapter ... 207
host name
Avaya Multimedia Messaging server ... 142
HTTPS REST interface
federation configuration ... 133

I

importing
Lync certificate ... 109
IM SIP entity ... 138
initial setup ... 36
InSite Knowledge Base ... 274
install
configuration settings ... 53
disable selinux ... 44
hosts file ... 45
on VMware ... 52
run install binary ... 48
silent install ... 59
SSH configuration ... 47
installation
OVA ... 49
physical server ... 38
VMware ... 49
installation tasks
OVA ... 36
physical server ... 36
installing
CA certificate ... 172
certificate to SBCE ... 170
Lync certificate ... 136
Lync certificate on cluster ... 111
installing a patch ... 81
installing EASG
physical server ... 62, 179
integrated Windows authentication ... 203
inventory
adding a patch ... 80
removing a patch ... 81
uninstalling a patch ... 81
IWA
active directory ... 203
administration portal ... 205
prerequisites ... 203
Windows Domain Controller setup ... 203

K

knowledge ... 24

L

LDAP configuration

LDAP configuration *(continued)*
Active Directory authentication parameters 118
Active Directory binding parameters 117
Active Directory internationalization parameters 122
Active Directory role search parameters 119
Active Directory user management parameters 123
attribute mapping 124
attribute mapping use case 127, 128
change LDAP parameters after installing cluster 75
import secure LDAP certificate 115
Microsoft Active Directory 115
property file examples 276
System Manager login name use cases 124
LDAP troubleshooting
LDAP configuration forced update 266
license
error 252
licensing 21
local host resolution table
adding AMM nodes 137
logging levels 190
logs and alarms 197
lync
interoperability 134
Lync 149
adaptation 136
adapter 136
add certificate 150
certificate 111
certificate on Avaya Multimedia Messaging cluster 111
Enterprise Edition 147
recovery 216
root signing certificate 150
server configuration 145, 155
Standard Edition 146
trusted server 146, 147
Lync attributes 155
Lync certificate 108, 152
importing 109
missing 254
server and client authentication 152
truststore 109
Lync certificate from CA
getting 108
obtaining 108
Lync certificate to each node
adding 109
Lync configuration
external domain 155
internal domain 145
Lync domain
external 155
internal 145
Lync edge 141
server 141
Lync edge server 141
Lync federation
Avaya Multimedia Messaging cluster 157
certificates 108
troubleshooting 253, 255–263
Lync interoperability
user configuration 158
Lync server
assigning certificate 154
enabled port 145
internal domain configuration 145
Lync trusted
Avaya Multimedia Messaging server 145
configuration 145
Lync user
adding 159
Lync users
configuration 160

M

main values
SIP entity 138
manage storage 183
managing
trusted hosts 187
messaging domain
adding a new messaging domain 183
deleting a messaging domain 183
migration 226, 227
Avaya Aura environment 240
Data Replication Service 240
physical server 234
preparing 228
Presence federation 241
process 278
restore to previous version 239
vCenter screenshots 278
migration from XMPP based
Presence Services federation 241
migration to REST based
Presence Services federation 241
missing
Lync certificate 254
multisite
port 190
multisite adapter
connector 207
fields 208
home site ID 207

N

node
static route destination 149

O

obtaining
    Lync certificate from CA 108
overview 13

P

patch 245
patches 245
patch setup 79
performance 188
physical server 202
    migration 234
planning 18
    LDAP server configuration 34
planning tasks 18
PLDS 20
    downloading software 21
populating
    SIP adapters 143
pre-configuration
    checklist 38
preparation
    physical server migration 234
preparing
    migration 228
Preparing the virtual server 230
prerequisites 24, 43
    adding non-root users 41
    directory structure 40
    disk space requirements 39
    IWA 203
    JDK 43
    libraries 43
    RHEL installation 39
    sudo permissions 42
    System Manager configuration for federation 31
Presence federation
    migration 241
Presence Services certificate
    adding to truststore 241
Presence Services federation
    migration from XMPP based 241
    migration to REST based 241
preventing
    creation of audit audispd logs 202

Q

querying patch status 80

R

reachable
    domain 26
recovery
    Lync 216
regular expressions
    System Manager 140
related documentation 271
relay SIP entity 138
removing EASG 64, 181
replacing
    XMPP with HTTPS REST 241
restarting services
    Lync 151
restore node in cluster 212
retrieve user conversations 224
reverse proxy
    checklist 164
routing policies
    System Manager 140

S

security requirements 23
server
    Lync edge 141
server configuration
    updating trusted hosts 187
Server node license
    tracking 22
server settings
    updating trusted hosts 187
session manager
    multiple 144
setting
    application media attributes 139
setting up
    IWA 205
setup
    LDAP 143
    System Manager 143
signing certificate
    Lync 150
SIP adapters
    populating 143
SIP entities
    Avaya Multimedia Messaging 138
SIP entity
    IM 138
    main values 138
    relay 138
SIP federation provider
    front-end FQDN 151
skills 24
start service 183
static route destination 149
statistics 188
stop service 183
storage management 183
support 274

synchronizing
certificate to SBCE 170
System Manager
configuration 135
domains 140
system manager certificate; download 171
System Manager configuration
address types 26
System Manager user settings 250

T

TLS scripts 226
TLS versions
disable 226
enable 226
topology 13
components 15
tracking
server node license 22
training 273
troubleshooting
AC client long poll timeout 253
cannot login to the web-based administration portal using Internet Explorer 10 248
cluster nodes 188
connection to AMM server 249
cookie cannot locate the session 248
database storage full 251
front-end server does not start 263
gluster failure 250
gluster rebalancing fails 250
HTTP services disabled 251
installer is not waiting long enough 268
Lync federation 253, 255, 258–263
Lync server does not start 263
media storage full 251
networking issues after upgrade 263
new node 250
OpenFire cluster error 264
participant has invalid address 265
post-install difficulties with gluster 250
rebalancing fails 250
special characters 266
startup timed out 268
trace logging 268
upgrade fails when trace logging is on 268
user cannot send message to non-AMM PS client 269
user login 269
user unable to send message from AMM client 269
troubleshooting Cassandra database
periodic repair of database inconsistencies 197
repairing database inconsistencies 247
server has been inactive for an extended period of time 247
troubleshooting core messaging application
resource discovery returns 404 error 265
troubleshooting LDAP authentication
trace-level logging 252
troubleshooting LDAP server
authentication 252
troubleshooting System Manager alarms 267
activating a server 267
configuring SNMP trap 267
troubleshooting System Manager logs
configuring System Manager FQDN 268
unable to view logs using Log Viewer 268
trusted Lync server 146, 147
trusted server
Lync 146, 147
truststore
Lync certificate 109

U

uninstall 79
uninstall cluster
remove node 76
update entitlements 185
updating
Avaya Multimedia Messaging 245
trusted hosts 187
upgrade 226, 242
add node 73
restore previous version 244
rollback 244
upgrades
rolling back to the previous version 244
upload
certificate file 169
user configuration
checklist 159
Lync interoperability 158
users
in multiple domains 154
System Manager 140
User settings 250

V

verify cluster nodes 188
videos 273
VMware 24

X

XMPP
replace with HTTPS REST 241
XMPP interface
configuration 132