Troubleshooting Avaya Multimedia Messaging

Release 3.3
Issue 1
December 2017

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “Named

User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

Contents

Chapter 1: Introduction

Purpose

This document describes known Avaya Multimedia Messaging issues.

Change history

Issue	Date	Summary of changes
Release 3.3, Issue 1	December 2017	This is a new document. The relevant troubleshooting information that used to be in *Deploying Avaya Multimedia Messaging* and *Administering Avaya Multimedia Messaging* has been moved into this document and reorganized. New troubleshooting information has also been added.

Chapter 2: Troubleshooting fundamentals

Before using this document, ensure that you follow the instructions in the following documents to prevent problems:

- Planning, installation, and initial configuration instructions are in *Deploying Avaya Multimedia Messaging*.
- General administration, maintenance, migration, and upgrade instructions are in *Administering Avaya Multimedia Messaging*.

Logs and alarms

Logs

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

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

Alarms

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

Important:

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

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

Table 1: Avaya Multimedia Messaging alarms

Name	Description	Severity
avESMComponentNotRunning	The system raises this alarm when a component has stopped functioning, does not start, or does not restart: • Cassandra	Major

Table continues…

Name	Description	Severity
	• Nginx • Tomcat • Mobicents • snmpd • spiritAgent • glusterd/glusterfsd • keepalived	
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 authentication, authorization and identity management.	Major
avAMMDataStoreAccessFailed	The system raises this alarm if the Avaya Multimedia Messaging application cannot connect to the database or the database cluster. This alarm is triggered by an audit process performed every 60 seconds.	Major
avAMMMediaStoreAccessFailed	The system raises this alarm if the Avaya Multimedia Messaging application cannot connect to the distributed file system, GlusterFS. This alarm is triggered by an audit process performed every 60 seconds. Under this alarm condition, the end users are only able to send text messages. Multimedia and generic attachments are rejected by the Avaya Multimedia Messaging server.	Major
avAMMDBStorageReachedCriticalThreshold	The system raises this alarm when the disk partition size where the Cassandra database is hosted exceeds 95% of the total size. The disk audit is performed every 60 minutes.	Critical
avAMMRESTCertificateFault	The system raises this alarm if the REST certificate is about to expire, has expired or if the application is unable to read the certificate file. The certificate audit is performed every 60 seconds.	Major

Table continues…

Name	Description	Severity
avAMMOAMCertificateFault	The system raises this alarm if the OAM certificate is about to expire, has expired or if the application is unable to read the certificate file. The certificate audit is performed every 60 seconds.	Major
avAMMSIPCertificateFault	The system raises this alarm if the SIP certificate is about to expire, has expired or if the application is unable to read the certificate file. The certificate audit is performed every 60 seconds.	Major
avAMMLicenseErrorModeActive	The system raises this alarm if one or more license errors are present.	Major
avAMMLicenseRestrictedModeActive	The system raises this alarm if one or more license errors are present and the 30 day grace period has expired.	Critical
avAMMRemoteDomainConnectionLost	The system raises this alarm if the Avaya Multimedia Messaging application is unable to ping one or more remote domains. The audit is performed every 30 seconds.	Major
avAMMVirtualIPAcquiredFromPrimary	The system raises this alarm when the primary node hosting the virtual IP address of the application has stopped.	Major
avAMMSMGRLDAPServerConnectionLost	The system raises this alarm if the application cannot establish connectivity with the Avaya Aura® System Manager LDAP server. This alarm can be triggered manually by testing the LDAP connectivity through the Avaya Aura® System Manager administration portal or as the result of an audit that is being performed every 60 seconds.	Major
avAMMMediaStorageReachedWarningThreshold	The system raises this alarm when the disk partition size where the media files are stored exceeds 90% of the total size. The disk audit is performed every 60 minutes.	Minor
avAMMMediaStorageReachedCriticalThreshold	The system raises this alarm when the disk partition size where the media files are stored exceeds 95% of the total size. The disk audit is performed every 60 minutes.	Critical
avAMMTimeServerSynchronizationLost	The system raises this alarm if the Avaya Multimedia Messaging application does not have time synchronization with one or multiple NTP servers.	Major

Table continues…

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

Chapter 3: Troubleshooting features

This chapter describes known troubleshooting issues.

Connectivity issues

Information in the database is inaccurate after server inactivity

Condition

If the 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.

Solution

1. Open the Avaya Multimedia Messaging server CLI.
2. Type the following command:

   ```
   $ sudo <installation_directory>/cassandra/2.1.17/bin/nodetool -u
   <cassandra_username> -pw <cassandra_password> repair
   ```

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

   `<cassandra_username>` and `<cassandra_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.

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.

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.

Cannot log in to the Avaya Multimedia Messaging server

Cause

You cannot login to the Avaya Multimedia Messaging server due to certificate issues.

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.

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** > **Security**.

2. Do one of the following:
    - Select **Enable Protected Mode**.
    - Add the server URL to the Local Intranet sites list.

Unable to collect logs using the Avaya Multimedia Messaging administration portal

Condition

You cannot collect logs from a node using the Avaya Multimedia Messaging administration portal because the node list is empty.

Cause

The Avaya Multimedia Messaging administration portal cannot retrieve the status of the node from the Cassandra database.

Solution

Collect logs directly from the node.

1. Log in to the Avaya Multimedia Messaging CLI.
2. Run the **`app collectlogs`** command along with any relevant details.

    For example, if you run the following command, two logs will be downloaded from the 10.10.10.1 node:

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

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

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

Cause

When the Avaya Multimedia Messaging server cannot connect to Presence Services, the Avaya Multimedia Messaging raises alarm code 00064.

If you are using a Presence Services release older than 7.0, the Avaya Multimedia Messaging server maintains the outgoing messages in its buffer, to later send the messages when the connection is restored. Over time, the accumulation of messages in the internal buffer occupies Avaya Multimedia Messaging server memory.

Solution

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

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

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

When the database or media partition is low on free space but does not reach the critical threshold, Avaya Multimedia Messaging starts to generate alerts. To avoid a service outage, perform the following steps as soon as you receive such alerts.

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 administration portal.

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

Condition

The resource discovery operation returns error code 404.

Solution

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

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

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

   ❗ **Important:**

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

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

2. Select **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.
3. Click **Force LDAP Sync**.
4. Click **Save**.

Client issues

Cannot send message from an Avaya Multimedia Messaging enabled client

Condition

Users cannot send a message from one 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.

Participant has invalid messaging address

Condition

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

Solution

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

Client does not support the latest TLS version

Condition

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

⚠ **Warning:**

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

Solution

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

1. Run one of the following commands:
   - To enable previous TLS versions:
     ```
     sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/misc/
     allowLegacyTLS.sh on
     ```
   - To disable previous TLS versions:
     ```
     sudo /opt/Avaya/MultimediaMessaging/<version>/CAS/<version>/misc/
     allowLegacyTLS.sh off
     ```

In these commands, `<version>` is the Avaya Multimedia Messaging build version that you are using.

2. Run `svc nginx reload` to reload Nginx.

   This step will not cause a service outage.

Client cannot connect to the Avaya Multimedia Messaging server

Condition

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

Solution

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

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

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

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

4. Address any errors that are displayed.

Error	Description	Solution
Error Code 401	You entered a wrong password.	Verify the password.
Error Code 403	You do not have the privileges required for gaining access to the Avaya Multimedia Messaging client interface.	Add the respective user to the Admin group in the LDAP structure.
Error Code 500	An error occurred on the Avaya Multimedia Messaging server	Log in to the Avaya Multimedia Messaging server to determine the exact issue.

Table continues…

Error	Description	Solution
	and it cannot process your request.	For additional information about `Error Code 500`, see Mail attribute is not configured on page 23.
Connection time out	The Avaya Multimedia Messaging server is not running.	Contact Avaya support. You can use the **`ping`** command to verify that the client can access the machine running the Avaya Multimedia Messaging server: `ping <amm-server.domain.com>`

5. On the Avaya Equinox™ client, navigate to **Settings** > **Services** > **Multimedia Messaging** and ensure that Avaya Multimedia Messaging is enabled.
6. 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.

Special characters displayed incorrectly when playing multimedia attachment

Condition

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

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

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

Cause

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

Solution

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

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

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

Condition

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

The correct behavior in this context is the following:

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

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

Solution

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

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.

Gluster file system issues

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.

Licensing issues

License error: Invalid feature capacity

Condition

When a licensing error occurs because of insufficient available server node licenses, the following 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 information about logs and alarms, see *Administering Avaya Multimedia Messaging*.

Solution

Ensure that there are sufficient server node licenses.

Related links

Logs and alarms on page 8

Setup and upgrade issues

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
   ```

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**.

Common LDAP configuration issues

Mail attribute is not configured

Condition

When users try to log in to `https://<amm-server:8443>/aem/resources`, they get an `HTTP status 500` error.

Cause

The root cause is most likely one of the following:

- The *mail* attribute is not configured in Active Directory with a valid email address.
- The email address for the user is not configured in Avaya Aura® System Manager.
- The email address attribute is not mapped correctly in Enterprise Directory Mappings on Avaya Multimedia Messaging.

Solution

1. Configure the mail attribute in Microsoft Active Directory with a valid email address.
2. The email address configured in Avaya Aura® System Manager for the user can be of the following types:
   - Microsoft Exchange
   - Avaya Aura® System Manager email
   - Other email
3. Ensure that the email address attribute in Avaya Multimedia Messaging is mapped to a valid mail attribute in Active Directory.

Messaging domains are missing or incorrect

Condition

When you try to log in to Avaya Multimedia Messaging, you get an `Invalid UserId 'user@domain.com'` error message.

A message similar to the following can be found in the log files: `New user email user@domain.com not in messaging domains [other.domain.com].`

Cause

The Messaging Domain List on the Client Settings page in the Avaya Multimedia Messaging web administration portal is not configured properly.

Solution

Update the Messaging Domain List. For example, if the user ID is `user@domain.com`, then add `domain.com` to the Messaging Domain List.

Login and access issues occur when you are not part of the configured Avaya Multimedia Messaging groups

Condition

One of the following issues occurs:

- You cannot log in to the Avaya Multimedia Messaging web administration portal.
- You can log in to the Avaya Multimedia Messaging web administration portal but cannot access `https://<amm-server>:8443/aem/resources` and cannot log in to the client.

Cause

You are not part of the configured Avaya Multimedia Messaging User or Admin groups, or the group names are not properly configured.

Solution

Group names can be configured either on the Avaya Multimedia Messaging web administration portal by navigating to **Server Connections** > **Enterprise LDAP Server Configuration**, or using the `configureAMM.sh` utility.

Important:

- Group names are case sensitive.
- To access the Avaya Multimedia Messaging web administration portal, you must be part of the configured Administrator role.
- To log in to `https://<amm-server>:8443/aem/resources` and to the clients, you must be part of the configured User role.

LDAP server authentication problems and logging trace-level messages for security-related classes

Condition

You cannot connect to the Avaya Multimedia Messaging server or use the administration portal.

Solution

- Test the LDAP configuration using an LDAP browser.
- Disable the secure LDAP setting.
- Enable trace-level logging and view the log files. For more information, see *Administering Avaya Multimedia Messaging*.

Viewer issues in Avaya Aura® System Manager

Unable to view Avaya Multimedia Messaging logs using Log Viewer

Condition

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

Solution

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

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

Condition

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

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

Solution

1. Do the following to activate the Avaya Multimedia Messaging server.
    1. Log in to the Avaya Aura® System Manager web console as described in *Administering Avaya Aura® System Manager*.
    2. Navigate to **Home** > **Services** > **Inventory**
    3. In the left panel, click **Manage Serviceability Agents** > **Serviceability Agents**.
    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.
2. Do the following to configure an SNMP trap.
    1. Log in to the Avaya Aura® System Manager web console.
    2. Navigate to **Home** > **Services** > **Inventory**.
    3. In the left panel, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
    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, see *Administering Avaya Aura® System Manager*.
    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
        ```

Troubleshooting best practices for Integrated Windows Authentication

Try the following solutions if you experience problems with Integrated Windows Authentication (IWA).

Solution

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

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

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

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

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

Microsoft federation issues

Certificate issues

Cannot upload the Lync or Skype for Business certificate on an Avaya Multimedia Messaging cluster

Condition

On an Avaya Multimedia Messaging cluster configuration with Microsoft Lync or Skype for Business federation, importing the front-end certificate on the seed node might fail with the following error: `keytool error: java.io.IOException: Keystore was tampered with, or keystore password was incorrect. Failed to update truststore password`. This might result in the SIP Adaptor for System Manager and the Lync or Skype for Business front-end server displaying the `DISCONNECTED` status for some nodes.

Solution

1. To reestablish the SIP connection to System Manager, do the following:

   a. Run the following commands to start the Avaya Multimedia Messaging configuration utility:

   ```
   cdto bin
   sudo ./configureAMM.sh
   ```

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

2. Download the front-end CA certificate to `/tmp/`.

3. Run the following command:

   ```
   sudo keytool -importcert -file /tmp/<FE_CA_cert_name> -keystore /opt/Avaya/
   MultimediaMessaging/<AMM_version>/CAS/<AMM_version>/cert/mss-ssl-ts.jks -
   storepass <keystore_password> -alias lync-ca-cert -trustcacerts
   ```

   - `<FE_CA_cert_name>` is the name of the Microsoft front-end CA certificate you downloaded.
   - `<keystore_password>` is the password created for the Avaya Multimedia Messaging keystore when running the configuration utility.

4. When the `Trust this certificate` message is displayed, type `yes`.
5. Run the following command:

   ```
   grep trustStorePassword /opt/Avaya/MultimediaMessaging/<AMM_version>/mss/
   7.0.4.452_8.0.26/conf/catalina.properties
   ```

6. If the password does not match the Avaya Multimedia Messaging keystore password, run the following command:

   ```
   sudo sed -i -e '/javax.net.ssl.trustStorePassword=/ s/=.*/
   =<keystore_password>/'/opt/Avaya/MultimediaMessaging/<AMM_version>/mss/
   7.0.4.452_8.0.26/conf/catalina.properties
   ```

7. To restart the Lync or Skype for Business service on Avaya Multimedia Messaging, run the following command:

   ```
   svc lyncim restart
   ```

System Manager certificate on Lync or Skype for Business edge server is missing or invalid

Condition

The external communication between Lync or Skype for Business and Avaya Multimedia Messaging fails in the following cases:

- Lync or Skype for Business to Avaya Multimedia Messaging: After an IM text is sent, the Lync or Skype for Business client displays the alert `This message wasn’t sent to _IM_user_ID_`.
- Lync or Skype for Business conference to Avaya Multimedia Messaging is not created.
- Avaya Multimedia Messaging to Lync or Skype for Business: After a second, the Avaya Multimedia Messaging client shows that the Lync or Skype for Business user has left the conversation.

Solution

1. On the System Manager web console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **CA Structure & CRLs**.
4. Click **Download PEM file**.

   The system downloads the `.pem` file on your system.

Lync or Skype for Business certificate on System Manager or Session Manager is missing or invalid

Condition

The external communication between Lync or Skype for Business and Avaya Multimedia Messaging fails in the following cases:

- Lync or Skype for Business to Avaya Multimedia Messaging: After an IM text is sent, the Lync or Skype for Business client displays the alert `This message wasn’t sent to _IM_user_ID_`.

- Lync or Skype for Business conference to Avaya Multimedia Messaging is not created.
- Avaya Multimedia Messaging to Lync or Skype for Business: After a second, the Avaya Multimedia Messaging client shows that the Lync or Skype for Business user has left the conversation.

Solution

Add the Lync or Skype for Business certificate to System Manager. For more information, see *Deploying Avaya Multimedia Messaging*.

Lync or Skype for Business certificate on Avaya Multimedia Messaging is missing or invalid

Condition

The internal communication between Lync or Skype for Business and Avaya Multimedia Messaging fails in the following cases:

- Lync or Skype for Business to Avaya Multimedia Messaging: After an IM text is sent, the Lync or Skype for Business client displays the alert `This message wasn’t sent to _IM_user_ID_`.
- Lync or Skype for Business conference to Avaya Multimedia Messaging is not created.
- Avaya Multimedia Messaging to Lync or Skype for Business: After a second, the Avaya Multimedia Messaging client shows that the Lync or Skype for Business user has left the conversation.

Solution

Import the Lync or Skype for Business front-end server certificate into the Avaya Multimedia Messaging trust store. For more information, see *Deploying Avaya Multimedia Messaging*.

System Manager certificate on Lync or Skype for Business Front end server is missing or invalid

Condition

The internal communication between Lync or Skype for Business and Avaya Multimedia Messaging fails in the following cases:

- Lync or Skype for Business to Avaya Multimedia Messaging: After an IM text is sent, the Lync or Skype for Business client displays the alert `This message wasn’t sent to _IM_user_ID_`.
- Lync or Skype for Business conference to Avaya Multimedia Messaging is not created.
- Avaya Multimedia Messaging to Lync or Skype for Business: After a second, the Avaya Multimedia Messaging client shows that the Lync or Skype for Business user has left the conversation.

Solution

1. On the System Manager web console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **CA Structure & CRLs**.

4. Click **Download PEM file**.

   The system downloads the `.pem` file on your system.

Connectivity and accessibility issues

System Manager data is inaccessible

Condition

Both internal and external communication between Lync or Skype for Business and Avaya Multimedia Messaging fail in the following circumstances:

- Lync or Skype for Business point-to-point to Avaya Multimedia Messaging: The Lync or Skype for Business 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 or Skype for Business: After a second, the Avaya Multimedia Messaging client shows that the Lync or Skype for Business user has left the conversation.
- Lync or Skype for Business 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 or Skype for Business client. The first message sent from the Avaya Multimedia Messaging client is immediately followed by the Avaya Multimedia Messaging client showing that the Lync or Skype for Business 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 or Skype for Business and Avaya Multimedia Messaging fails in the following cases:

- Lync or Skype for Business point-to-point to Avaya Multimedia Messaging: The Lync or Skype for Business 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 or Skype for Business: The Lync or Skype for Business 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 or Skype for Business conference to Avaya Multimedia Messaging: After adding an Avaya Multimedia Messaging user, the Lync or Skype for Business 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:
    1. Select **Force LDAP Sync** and wait for 5 minutes.
    2. Send an IM.
    3. **(Optional)** If the IM is not sent, contact Avaya Support.

Avaya Multimedia Messaging lost Lync or Skype for Business session information

Condition

Both internal and external communication fails between Avaya Multimedia Messaging and Lync or Skype for Business when, after sending an IM, the Lync or Skype for Business 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 or Skype for Business client.
2. Accept the invitation.

   The Lync or Skype for Business client reconnects to the conversation. If the Lync or Skype for Business client is not added to the conversation, the Avaya Multimedia Messaging client shows that the Lync or Skype for Business user left the conversation.
3. If Avaya Multimedia Messaging shows that the Lync or Skype for Business user left the conversation, add the Lync or Skype for Business user back to the conversation.

Configuration issues

SIP Adaptor for Session Manager is not enabled or enabled with a misconfigured IP address

Condition

Both the internal and external communication between Lync or Skype for Business and Avaya Multimedia Messaging fail in the following cases:

- Lync or Skype for Business to Avaya Multimedia Messaging: After an IM text is sent, the Lync or Skype for Business client displays the alert `This message wasn’t sent to _IM_user_ID_`.
- Lync or Skype for Business conference to Avaya Multimedia Messaging is not created.
- Avaya Multimedia Messaging to Lync or Skype for Business: After a second, the Avaya Multimedia Messaging client shows that the Lync or Skype for Business user has left the conversation.

Solution

1. Configure the Session Manager SIP adaptor.

   For more information, see *Deploying Avaya Multimedia Messaging*.
2. To use the new configuration, restart Avaya Multimedia Messaging.

SIP Adaptor for Lync or Skype for Business is not enabled or enabled with a misconfigured IP address

Condition

The internal communication between Lync or Skype for Business and Avaya Multimedia Messaging fails in the following cases:

- Lync or Skype for Business to Avaya Multimedia Messaging: After an IM text is sent, the Lync or Skype for Business client displays the alert `This message wasn’t sent to _IM_user_ID_`.
- Lync or Skype for Business conference to Avaya Multimedia Messaging is not created.
- Avaya Multimedia Messaging to Lync or Skype for Business: After a second, the Avaya Multimedia Messaging client shows that the Lync or Skype for Business user has left the conversation.

Solution

1. Configure the Lync or Skype for Business SIP adaptor.

   For more information, see *Deploying Avaya Multimedia Messaging*.
2. To use the new configuration, restart Avaya Multimedia Messaging.

Avaya Multimedia Messaging node is not a trusted host on Lync or Skype for Business

Condition

The internal communication between Lync or Skype for Business and Avaya Multimedia Messaging fails in the following cases:

- Lync or Skype for Business to Avaya Multimedia Messaging: After an IM text is sent, the Lync or Skype for Business client displays the alert `This message wasn’t sent to _IM_user_ID_`.
- Lync or Skype for Business conference to Avaya Multimedia Messaging is not created.
- Avaya Multimedia Messaging to Lync or Skype for Business: After a second, the Avaya Multimedia Messaging client shows that the Lync or Skype for Business user has left the conversation.

At the same time, SIP adaptor for Lync or Skype for Business is disconnected.

Solution

- Verify that the Avaya Multimedia Messaging cluster nodes are trusted hosts on the Lync or Skype for Business server.
- Add a node as a trusted host on Lync or Skype for Business.

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

Problem in System Manager administration of Avaya Multimedia Messaging SIP entities

Condition

One or more Lync or Skype for Business clients continually log out.

Cause

The Lync or Skype for Business 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 or Skype for Business 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.

LyncAdaptation is missing from Avaya Multimedia Messaging SIP entity

Condition

The internal communication between Lync or Skype for Business and Avaya Multimedia Messaging fails in the following cases:

- Lync or Skype for Business to Avaya Multimedia Messaging: After an IM text is sent, the Lync or Skype for Business client displays the alert `This message wasn’t sent to _IM_user_ID_`.
- Lync or Skype for Business conference to Avaya Multimedia Messaging is not created.
- Avaya Multimedia Messaging to Lync or Skype for Business: After a second, the Avaya Multimedia Messaging client shows that the Lync or Skype for Business user has left the conversation.

After you add an Avaya Multimedia Messaging user to the Lync or Skype for Business 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.

Lync Adaptation is missing from Lync or Skype for Business Edge remote server

Condition

Lync or Skype for Business point to point to Avaya Multimedia Messaging works.

Avaya Multimedia Messaging to Lync or Skype for Business works.

The external communication between Lync or Skype for Business conference to Avaya Multimedia Messaging fails. In this case, 40 seconds later from adding an Avaya Multimedia Messaging user, the Lync or Skype for Business client displays: `invitation to XXX expired`..

Solution

On System Manager, add the LyncAdaptation to the SIP entity belonging to the Lync or Skype for Business Edge.

The routing pattern to Avaya Multimedia Messaging is missing or incorrect

Conditions

Lync or Skype for Business point to point to Avaya Multimedia Messaging fails.

Both the internal and external communication between Lync or Skype for Business and Avaya Multimedia Messaging fail under the following circumstances:

- The Lync or Skype for Business message reaches the Avaya Multimedia Messaging client.
- The Lync or Skype for Business 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 or Skype for Business client.

- Subsequent messages from Lync or Skype for Business continue to reach Avaya Multimedia Messaging client.
- After a minute, the Avaya Multimedia Messaging client shows that the Lync or Skype for Business user left the conversation.
- The next message from the Lync or Skype for Business client creates a new Avaya Multimedia Messaging client conversation window.

Avaya Multimedia Messaging to Lync or Skype for Business fails.

Both the internal and external communication between Avaya Multimedia Messaging and Lync or Skype for Business fail under the following circumstances:

- The Lync or Skype for Business client receives in a pop-up window the invitation from Avaya Multimedia Messaging and the Lync or Skype for Business user accepts the invitation.
- The Lync or Skype for Business 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 or Skype for Business client pop-up.
- After a minute, the Avaya Multimedia Messaging client shows that the Lync or Skype for Business user left the conversation.

Lync conference to Avaya Multimedia Messaging works.

Solution

Add the routing patterns in System Manager for Avaya Multimedia Messaging. For more information about routing patterns and routing policies, see *Deploying Avaya Multimedia Messaging*.

The routing pattern to Lync or Skype for Business Edge is missing or incorrect

Condition

The external communication with Lync or Skype for Business Edge fails in the following cases:

- Lync or Skype for Business point-to-point to Avaya Multimedia Messaging: The Avaya Multimedia Messaging client receives the first message from the Lync or Skype for Business client. After a second, the Avaya Multimedia Messaging client shows that the Lync or Skype for Business user left the conversation.

  Each subsequent message from the Lync or Skype for Business client creates a new conversation with the same outcome as above.
- Avaya Multimedia Messaging to Lync or Skype for Business: A second after sending a message or adding a Lync or Skype for Business user, the Avaya Multimedia Messaging client shows that the Lync or Skype for Business user left the conversation.
- Lync or Skype for Business conference to Avaya Multimedia Messaging: After you add an Avaya Multimedia Messaging user to the Lync or Skype for Business client, the system displays an error: `Invitation to 15 _user_ expired`.

Solution

On System Manager, add the routing pattern for routing to Lync or Skype for Business Edge.

Note:

You might need to create a routing policy for Lync or Skype for Business Edge.

Route to the destination domain is missing

Condition

The internal communication between Lync or Skype for Business and Avaya Multimedia Messaging fails in the following cases:

- Lync or Skype for Business point to point to Avaya Multimedia Messaging: After an IM message is sent, the Lync or Skype for Business client displays the following alert: `We couldn't reach _IM_user_ID_ to send this message.`
- Avaya Multimedia Messaging to Lync or Skype for Business: The Lync or Skype for Business client receives the invitation from Avaya Multimedia Messaging in a pop-up window, and the Lync or Skype for Business user accepts the invitation. The Lync or Skype for Business client displays the message: `The meeting you are trying to join doesn't exist or has ended`. After one minute, the Avaya Multimedia Messaging client shows that the Lync or Skype for Business user left the conversation.
- Lync or Skype for Business conference to Avaya Multimedia Messaging: After you add an Avaya Multimedia Messaging user to the conference, the Lync or Skype for Business 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 or Skype for Business server.
2. Verify that the static route is set to the Avaya Aura® Presence Services Federation Relay.

   Run the following command on the front-end server to verify the router:

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

Avaya Multimedia Messaging front-end FQDN is not administered as a SIP federated provider

Condition

The internal communication between Lync or Skype for Business and Avaya Multimedia Messaging fails in the following cases:

- Lync or Skype for Business point to point to Avaya Multimedia Messaging: After an IM message is sent, the Lync or Skype for Business client displays the following alert: `We couldn't reach _IM_user_ID_ to send this message.`
- Avaya Multimedia Messaging to Lync or Skype for Business: The Lync or Skype for Business client receives the invitation from Avaya Multimedia Messaging in a pop-up window, and the Lync or Skype for Business user accepts the invitation. The Lync or Skype for Business client displays the message: `The meeting you are trying to join doesn't exist or has ended`. After one minute, the Avaya Multimedia Messaging client shows that the Lync or Skype for Business user left the conversation.

- Lync or Skype for Business conference to Avaya Multimedia Messaging: After you add an Avaya Multimedia Messaging user to the conference, the Lync or Skype for Business client displays the following alert: `_IM_user_ID_ cannot be found. Please check the address and check again.`

Solution

1. Open the Lync or Skype for Business 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 or Skype for Business front-end service.

Lync front-end server cannot start

Condition

The Lync or Skype for Business 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**.

Users and user profiles

User did not acknowledge message receipt

Condition

Both internal and external communication fail between Lync or Skype for Business and Avaya Multimedia Messaging when, after sending an IM, the Lync or Skype for Business client displays an alert: `This message wasn’t sent to everyone.`

Solution

No workaround is available.

Chapter 4: Resources

Documentation

The following table lists related documentation for Avaya Multimedia Messaging. All Avaya documentation is available at http://support.avaya.com.

Table 2: Avaya Equinox™ and Avaya Multimedia Messaging documentation

Title	Use this document to	Audience
Overview		
Avaya Equinox™ Overview and Specification for Android, iOS, Mac, and Windows	Understand high-level product functionality, performance specifications, security, and licensing.	Customers and sales, services, and support personnel
Planning		
Planning for and Administering Avaya Equinox™ for Android, iOS, Mac, and Windows	Perform system planning and configuration for: • Avaya Equinox™ for Android • Avaya Equinox™ for iOS • Avaya Equinox™ for Mac • Avaya Equinox™ for Windows	• System administrators • Customers and sales, services, and support personnel
Avaya Multimedia Messaging Reference Configuration	Understand technical overview information, system architecture, functional limitations, and capacity and scalability for Avaya Multimedia Messaging.	Customers and sales, services, and support personnel
Implementing		
Deploying Avaya Multimedia Messaging	Install, configure, administer, and troubleshoot Avaya Multimedia Messaging.	Implementation personnel
Administering		
Administering Avaya Multimedia Messaging	Administer and manage 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

Table 3: Other related documents

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

Finding documents on the Avaya Support website

Procedure

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

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

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.

Using the Avaya InSite Knowledge Base

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

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

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

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

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Index