Implementing and Administering Avaya Aura® Media Server

Release 10.1.x
Issue 6
April 2024

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 media which may include product information, subscription or service descriptions, 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. Please refer to your agreement with Avaya 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 the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided 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.

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. Unless otherwise stated, 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.

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE 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 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, please contact your Avaya Sales Representative.

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 Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud 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 LLC.

All non-Avaya trademarks are the property of their respective owners.

Contents

Chapter 1: Introduction

Purpose

Use this document to perform Avaya Aura® Media Server 10.x configuration, troubleshooting, and system administration tasks.

This document can be used for both appliance and non-appliance versions of Avaya Aura® Media Server 10.x. However, when you are working with the Avaya Aura® Media Server 10.x as an appliance in the VMware Virtualized Environment or as an appliance on Avaya Solutions Platform, first see *Deploying and Updating Avaya Aura® Media Server Appliance*. The appliance specific document takes precedence. Only use this document when the appliance document does not have a specific procedure for the task and when the appliance document directs you to this document.

This document is intended for people who perform Avaya Aura® Media Server 10.x configuration, troubleshooting, and system administration tasks.

Change history

Issue	Date	Summary of changes
6	April 2024	Added supported announcement table in Media file format on page 152 section and SNMP FIPS note in Adding a SNMP User on page 75 section.
5	May 2023	Added note about limit of one syslog destination for physical and virtual appliance in the Configuring SysLog settings on page 194 section.
4	April 2023	Added the section: Remove stale media server cluster and server data in System Manager on page 248
3	February 2023	Added the section: Replacing Default Staging certificates on page 30. Updated certificate management procedures.
2	July 2022	Updated SIP settings.
1	April 2022	Initial issue for Release 10.1 document

Chapter 2: New in this release

This section contains features new to Avaya Aura® Media Server 10.x which are common to both appliance and non-appliance (software only) systems.

Related links

New in Avaya Aura® Media Server 10.1.0 on page 13

New in Avaya Aura® Media Server 10.1.0

- Support for Red Hat Enterprise Linux® Server 7.x is removed.
- Support for Red Hat Enterprise Linux® Server 8.x. is added.

Related links

New in this release on page 13

Chapter 3: Management Interface

Introduction to Element Manager

Element Manager (EM) is an optional, web-based administration tool. EM facilitates the Operation, Administration, and Maintenance (OAM) of Avaya Aura® Media Server (MS).

Some adopting products provide a different OAM management system for Avaya Aura® MS. Those systems have similar functionality though the navigation and interface are different.

The procedures in the document are based on the optional EM installed by the Avaya Aura® MS installer.

EM installation

When performing the Avaya Aura® MS installation procedures, you can choose to install Avaya Aura® MS Element Manager (EM) for management of the system. If you do not have an alternate OAM management system, install EM to configure Avaya Aura® MS.

Avaya Aura® MS installer installs EM unless you or an adopting product installer, which embeds Avaya Aura® MS, specifically decline EM installation.

The installation procedures for Avaya Aura® MS cover the EM installation option in detail.

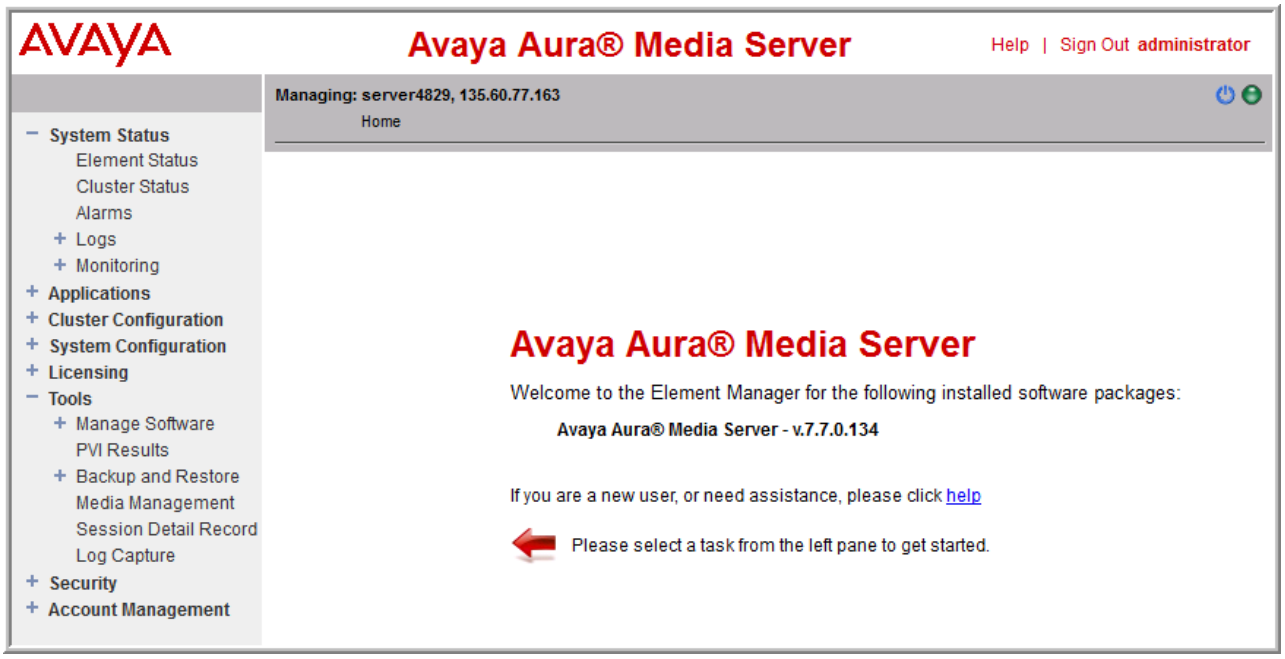
Web browser configuration

You can gain access to Avaya Aura® MS Element Manager (EM) by using a web browser. You can log in to the EM locally on the server, or remotely from another computer. The EM works with recent versions of Chrome, Firefox, and Microsoft Edge.

EM overview

The Element Manager (EM) layout includes a branding banner at the top, a task pane at the left, a content pane at the right for management activities, and a navigation bar at the top of the content pane. The upper-right corner of the EM page has **Help** and **Sign out** links and displays the user ID of the currently signed-in user.

The system displays the Home page after initial login. The content pane displays the welcome message, the version of Avaya Aura® MS installed, and a message to assist your administrator to get started.



The navigation bar is located under the branding banner. The navigation bar includes the host name, the management IP address of the component that you are managing, and the navigation history, known as breadcrumbs, reflecting the location of the current task within the task hierarchy. The navigation breadcrumbs are active links that you can use to return to previously accessed areas.

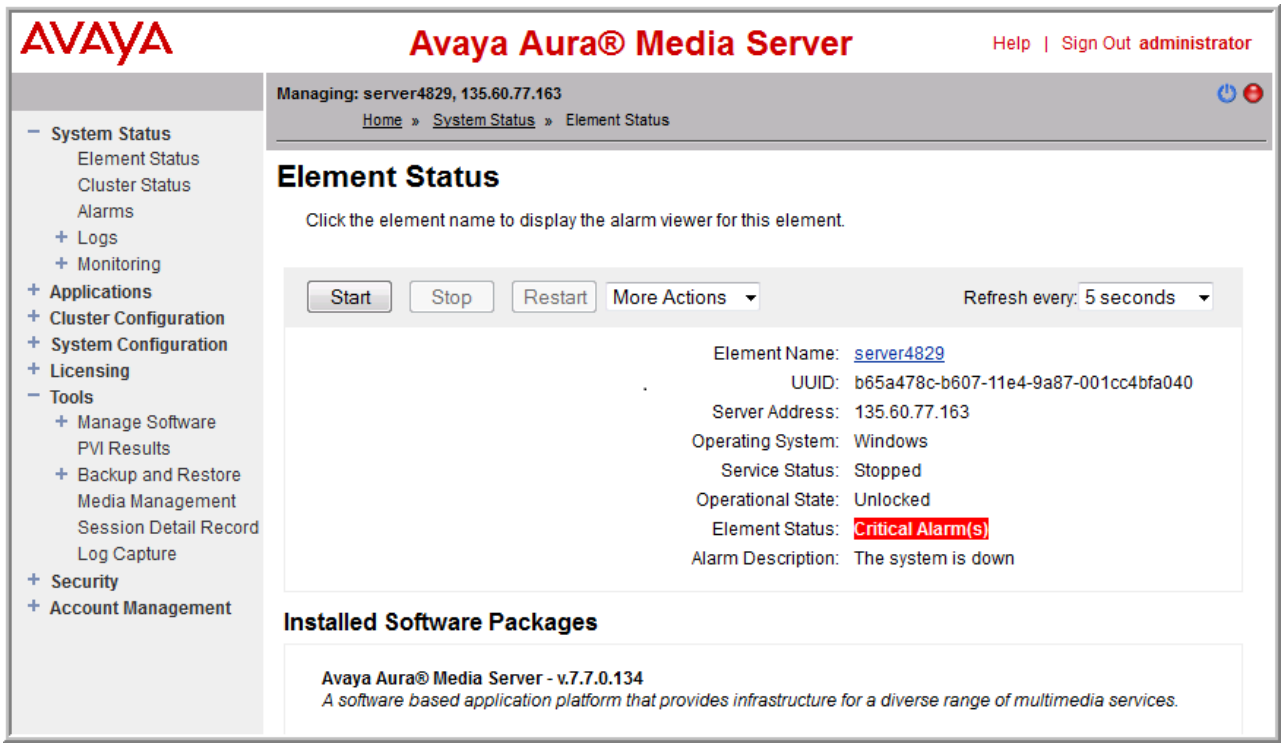
The right side of the navigation bar displays icons to alert you of the Avaya Aura® MS alarms and restart states.

EM displays a round colored icon representing the alarm state of Avaya Aura® MS. Hovering your mouse cursor over the alarm reveals the most severe active alarm. Clicking on the alarm icon displays the Alarms page with details about all the currently active alarms. EM displays the following alarm levels:

- Critical
- Major
- Minor

- Normal

When configuration items that require a restart to take effect have been saved, EM displays a restart icon next to the alarm status icon to indicate that you must perform an Avaya Aura® MS restart. EM clears the icon after the Avaya Aura® MS restarts.

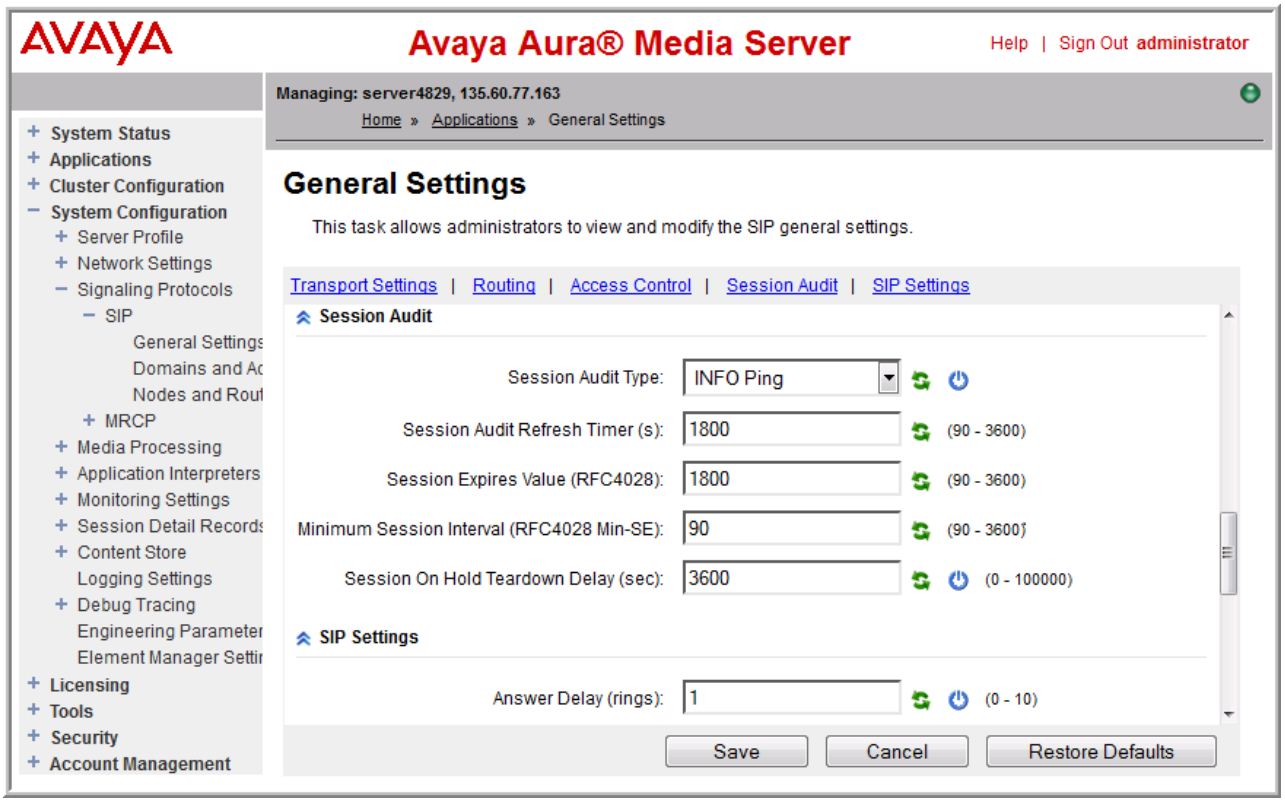


The tasks pane on the left lists all the actions that an administrator performs for Avaya Aura® MS OAM. The actions are grouped into categories as follows:

Actions	Description
System Status	Presents a view of the current and historical information pertaining to the status of the system. These tasks includes: • element status • alarm viewing • cluster status • event log viewing • monitoring The monitoring task includes: • performance monitoring • operational measurements • protocol monitoring of Avaya Aura® MS The active session monitoring includes graphical SIP message flows and SIP traces and displays details of messages for a particular session.
Applications	Lists all installed applications, whether custom or packaged. Expanding an application displays all tasks specific to the operation, administration, and maintenance of that application.
Cluster Configuration	Provides tasks for server designation, replication settings, clustering and high availability configuration, and load balancing settings.
System Configuration	Categories include, server profiles, network settings, signaling protocols, media processing, application interpreters, monitoring settings, session detail records, engineering parameters, EM settings, and SIP routing. The administrator can view and modify Avaya Aura® MS platform configuration.
Licensing	Provides an interface to configure and monitor the licensing services.
Tools	Provides utilities to view which software versions are installed. It performs a backup or restore of system and customer data, manage media, view session detail records, and collect logs.
Security	Provides an interface for Security related configuration.
Account Management	Manage administrators, roles, and permissions for Avaya Aura® MS EM users.

EM interface

The following figure illustrates the features of the Element Manager (EM) interface:



Task navigation

You can expand categories or higher-level tasks to reveal subtasks in the menu pane. Click the expansion button that appears to the left of the category or task label. If an item contains more contents, the system displays a plus sign (+) before the item. You can click the plus sign (+) to expand the item and display its contents.

Click the minus sign (-) to collapse the expanded contents.

Click an item label in the menu pane to select and launch the associated task in the content area.

Content areas with a large amount of content are divided into sections. Using the shortcut links provided at the top of the pane, you can navigate directly to the section of your interest. These links serve as an index of the content.

You can open a task in a new browser window or browser tab by using the right-click menu of the Web browser.

Scroll bars

The system displays vertical scroll bars when the system cannot display the content in a window without vertical clipping. The system displays horizontal scroll bars when the system cannot display the content in a window without horizontal clipping. You can reduce horizontal clipping by

using the vertical line separating the menu pane and the content areas to resize the menu pane horizontally.

Disabled items

Some configuration items are designed to enable or disable certain other features on the page. You cannot modify configuration items which are unavailable, until you enable the configuration items by selecting other features.

Saving configuration changes

Click **Save** in the bottom-right corner of the configuration page to save changes. No changes are made to the system configuration until you click **Save**. The system validates the input it stores the configuration in the Avaya Aura® MS database. If the system detects any errors during the validation, the system redisplays the page with an error message for each invalid entry. Correct the errors and click **Save** to save the changes. After you save the changes, the system redisplays the parent of the current page, which is often the previous page.

If you do not want to save the changes made to the configuration, click **Cancel** to discard changes. If you click **Cancel**, the system returns to the parent of the current page without saving changes to the configuration.

Undo changes

You can use the restore default icon button (), next to the fields, to restore individual configuration items to the default value that Avaya provides. You can use the **Restore Defaults** button to restore all the fields on the current page to the default values. The **Restore Defaults** button is located next to the **Save** and **Cancel** buttons. Click **Save** to apply the restored default values to the system.

Avaya Aura® MS restarts

The system designates some configuration items with a restart icon ().

These configuration items require an Avaya Aura® MS restart for any change to take effect. For these items, saving the change only saves the change in the system database. Restart Avaya Aura® MS so that the change is applied to system processing.

Data validation

Configuration items with data entry fields also include the valid data range in parentheses at the right of the data field. For example, you can see a data range such as (90-3600) or a limit such as (maximum: 128 characters). Sometimes, the parentheses contain a description like (Service IP address). In these cases, the system verifies whether the data is in the IP address format.

Help

In addition to the main help document available using the **Help** link in the upper-right corner next to the **Sign Out** link, the system also dynamically displays help text when you hover your mouse cursor over certain elements of the display. If available, the system displays the help text near the cursor.

Setting the content pane refresh frequency

About this task

An EM page that has dynamically updated content, has a user selectable refresh rate drop-down menu.

Perform the following procedure to customize the refresh rate of the content you are viewing:

Procedure

1. Navigate to **EM** > **System Status** > **Element Status** or to any task with the refresh option.
2. Click on the **Refresh every** drop-down menu and select the required refresh interval.

   The page you are viewing refreshes at the selected frequency.

Advanced settings and engineering parameters

Do not reconfigure the default values in the Advanced Settings and Engineering Parameters pages.

These defaults are set for optimal performance of Avaya Aura® MS. If you think these settings need to be changed, contact Avaya Technical Support to discuss the changes. Reconfigure these settings only under explicit direction from Avaya Technical Support.

Chapter 4: Basic management tasks

Signing in to EM

About this task

Use this procedure to gain access to Avaya Aura® MS Element Manager (EM) whenever required in a task. For example, if you see **EM** > **System Status** > **Element Status**, follow this procedure to first gain access to EM and then, click **System Status** and click **Element Status**.

Before you begin

Signing into EM applies to systems that have the optional Avaya Aura® MS EM installed. You must first install Avaya Aura® MS with EM to perform this procedure.

Procedure

1. In a web browser, type the following URL:

   `https://`*`serverAddress`*`:8443/em`, where *serverAddress* is the address of Avaya Aura® MS.

   For example, `https://10.60.86.209:8443/em`.

2. Sign into EM. The first time you sign in, the username is **admin** and password is **Admin123$**. After initial login you will be prompted to change the admin password.

Observing the current operational status by using EM

About this task

Use this procedure to observe the current operational status of Avaya Aura® MS.

Procedure

1. Navigate to **EM** > **System Status** > **Element Status**.
2. Observe the status of the element in the content pane.

   On the **Element Status** page, the system displays the following:

   - Attributes identifying this server: **Element Name**, **UUID** (a unique identifier for the element), **Server Address**, and **Operating System**.

- **Service Status**: Indicates whether the media server is started or stopped. This state is coordinated with the **Stop**, **Start**, and **Restart** buttons on the page.
- **Operational State**: This state can be set to **Unlocked**, **Locked**, or **Pending Locked**. You can select the required state using the **More Option** drop-down menu.
- **Element Status**: Reports the most severe status of the current active alarms for the element. For example, if an element has two active alarms, one with severity Critical and the other with severity Minor, then the overall status of the element is Critical. When no active alarm exists, the element state is Normal.
- **Alarm Description**: If any alarms are raised, an explanation of the most critical alarms is noted in this field.
- **Installed Software Packages**: Lists the versions of Avaya Aura® MS and any installed software packages.

Starting and stopping the media server

About this task

Use this procedure to Start, Stop, or Restart Avaya Aura® MS by using EM. The Start, Stop, and Restart actions for Avaya Aura® MS operate as follows:

Action	Description
Start	Starts all the necessary software processes to enable media server functionality. Ensure that Avaya Aura® MS is set to Stopped before using this function.
Stop	Ends all software processes that enable media server functionality and take the element out of service. Ensure that Avaya Aura® MS is set to Started before using this function.
Restart	Restarts Avaya Aura® MS, which is the same as stopping the media server and then starting the media server again. Ensure that Avaya Aura® MS is set to Started before using this function. The *Service Status* of Avaya Aura® MS must be set to `Started` before you can restart Avaya Aura® MS. Restarting Avaya Aura® MS is the same as stopping the media server and then starting the media server again.

Before you begin

Avaya recommends that you set the Operational State of Avaya Aura® MS to Pending Lock and then Lock before stopping or restarting a server with active sessions. This reduces the number of user sessions impacted by stopping the media server. For details, see Setting the operational state

Procedure

1. Navigate to **EM** > **System Status** > **Element Status**.
2. Depending upon the current and the required state, click **Start**, **Stop**, or **Restart**.
3. Click **Confirm**.

   After a few seconds, the system updates the status fields and activates or deactivates the buttons based on the new state of the media server.

Related links

Setting the operational state on page 23

Setting the operational state

About this task

You can specify the level of service availability for Avaya Aura® MS which is in the started state. The level of service availability is useful under certain conditions as follows:

Action	Description
Lock	Locks the system and ends existing sessions. The media server no longer accepts new requests, and redirects new traffic to other nodes in the cluster. You typically place the system into locked state when performing maintenance. The Operational State of Avaya Aura® MS must be set to **Unlocked** or **Pending Locked** before you can lock Avaya Aura® MS.
Unlock	Unlocks the media server and allows incoming session requests to be accepted by the system for processing. The Operational State of Avaya Aura® MS must be set to **Locked** or **Pending Locked** before you can unlock Avaya Aura® MS.

Table continues…

Action	Description
Pending Lock	The system does not accept new requests. It redirects new traffic to other nodes in the cluster. Unlike **Lock**, **Pending Lock** preserves existing sessions. You typically place the system into a **Pending Locked** state before transiting to a **Locked** state when you prepare for system maintenance. This allows sessions to naturally end over time, without being ended unexpectedly for users of the system. The system automatically changes to the **Locked** state after all the sessions have ended. The Operational State of Avaya Aura® MS must be set to **Unlocked** or **Locked** before you set the system to **Pending Lock**.
Failover	Transfers all the active sessions from this media server to the peer. The peer automatically becomes the active node. All new session requests are automatically directed to the newly active peer node. The failed node enters the Standby state and is ready for maintenance or other activities while the peer continues to provide service. You can select **Failover** when the media server is in a High Availability configuration with another node.

Procedure

1. Navigate to **EM** > **System Status** > **Element Status**.
2. Click **More Actions** and select the state from the list of applicable states.

   The list is dynamic and dependent of the current state.
3. Click **Confirm**.

   After a few seconds, the system updates the status fields and content of the **More Actions** drop-down menu-based on the new state of the media server.

Managing the High Availability state

About this task

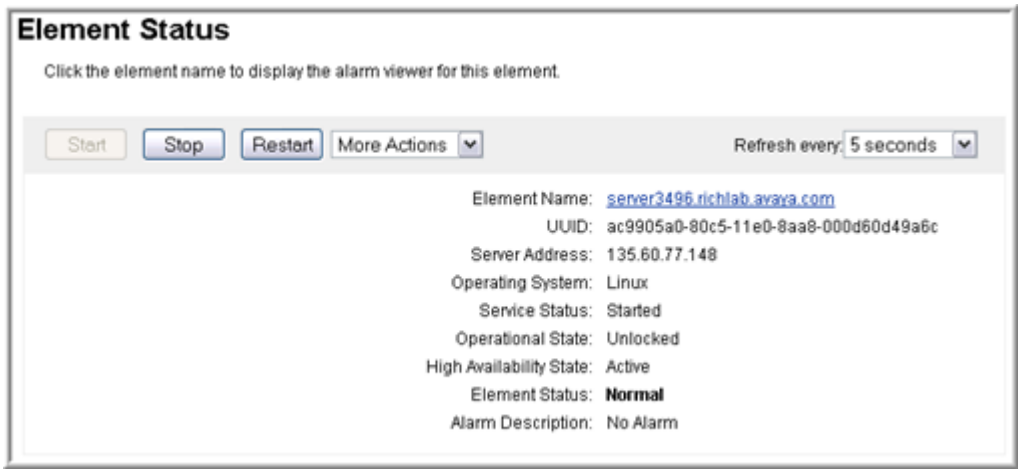
If you configured Avaya Aura® MS for High Availability, the system displays the High Availability state of the server on the **EM** > **System Status** > **Element Status** page. The **More Actions** drop-down menu contains state transition options, which are available only when High Availability is enabled. The High Availability state can be one of the following values:

Action	Description
Active	The server has a configured Service IP address and is providing service.
Standby	The server is inactive but remains synchronized with the active server.
Failed	The server has failed. The server will soon restart and transition to a Searching state.
Locked Active	The active High Availability server is Locked Active when you select **Local High Availability State Lock** on **EM** > **Cluster Configuration** > **High Availability** and the server is not shutdown.
Locked Standby	The standby High Availability server is Locked Standby when you select **Local High Availability State Lock** on **EM** > **Cluster Configuration** > **High Availability** and the server is not shutdown.
Shutdown	The server is in a management shutdown state and is not providing service.
Searching	The server tries to determine the state of the other server in the High Availability pair. The server remains in the Searching state for less than a second before transiting to the Active or the Standby state.

Procedure

1. On one of the paired High Availability servers, navigate to **EM** > **System Status** > **Element Status**.

   Servers in the High Availability mode display an additional field, **High Availability State**, on the **Element Status** page, as shown below:



2. Use the **More Actions** drop-down menu to select the required High Availability state. For example, you can choose **Failover**.

The High Availability states listed on the menu depend upon the current **High Availability State**, which is shown on the **Element Status** page.

3. Read the warning and then click **Confirm** to apply the state change.
4. On the **Element Status** page, ensure that the **High Availability State** field now displays the new state.

Viewing the software inventory

About this task

EM provides a summary of the installed Avaya Aura® MS software, applications, and patches along with the version information. The summary is called the software inventory.

Use this procedure to gain access to the software inventory:

Procedure

Navigate to **EM** > **Tools** > **Manage Software** > **Inventory**.

The system displays a list of the installed software with the version and patch level information.

Reviewing the PVI Check results

About this task

Using EM, you can review the hardware, software, and storage inspection reports generated during the Avaya Aura® MS installation.

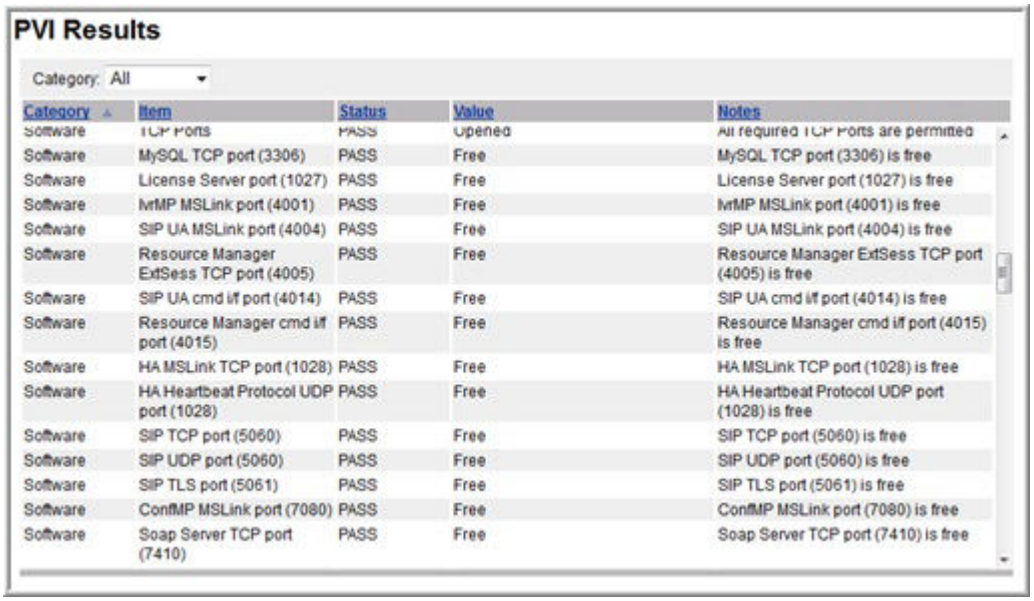
The Platform Vendor Independent Check (PVI Check) software ensures that the server and the configured operating system meet the hardware, software, and storage requirements for Avaya Aura® MS.

PVI Check is integrated into the Avaya Aura® MS installer and produces a report that is stored in the system for reference.

Procedure

1. Navigate to **EM** > **Tools** > **PVI Results**.

2. Refine the scope of the result by using the **Category** drop-down menu on the **PVI Results** page. You can sort the results by clicking on any column title.



System configuration and trace logs

The Log Capture tool provides an easy way to collect all system configurations and trace logs that Avaya technical support teams might need to debug reported system issues.

When support engineers request trace logs, ensure that the debug logging is enabled. Also ensure that you capture the logs when the problem is observed on the system. The Log Capture tool is then used to collect all the required logs from the system and download the logs to your local workstation.

Enabling Debug Tracing

About this task

Debug logging provides advanced system trace and debug logs required by support engineers to troubleshoot your system.

Use this procedure to enable debug logging as instructed by Avaya support engineers before using the log capture tool:

Procedure

1. Navigate to **EM** > **System Configuration** > **Debug Tracing** > **General Settings**.
2. Select **Enabled** from the **Debug Logging** drop-down menu.
3. If instructed by Avaya support engineers, change **Trace File History**.

Trace File History defines the number of rotating trace files that the system keeps before discarding the oldest file. By increasing this value, you can collect more data, but more disk space is consumed.

4. If instructed by Avaya support engineers, change **Trace File Size**.

   Trace File Size defines the size of the trace files. By increasing this value, you can collect more data, but more disk space is consumed.

5. Click **Save**.

Downloading log capture by using a web browser

About this task

The Log Capture tool collects advanced system traces and debug logs that are required by support engineers to troubleshoot the system.

Before you begin

Ensure that you enable debug logging so that you can capture the traces when a problem is observed on the system.

Procedure

1. Navigate to **EM** > **Tools** > **Log Capture**.
2. If instructed by Avaya support engineers, select **Include trace logs**.
3. Click **download**.

   The system gathers all the trace files together in the form of a zip file and displays a dialog box so that you can download the zip file to the local workstation.

Downloading a log capture by using the command-line mode

About this task

The Log Capture tool collects advanced system traces and debug logs that are required by support engineers to troubleshoot the system.

Before you begin

Ensure that you enable debug logging so that you can capture the traces during the interval when a problem is observed on the system.

Procedure

1. Open a Linux® shell on Avaya Aura® MS.
2. From the command-line, run the Log Capture tool by using one of the following commands as instructed by Avaya support engineers:

   - `logcapture`
   - `logcapture -t`

The system gathers all the log files together in the form of a zip file. When the `-t` option is included the zip file also includes the advanced system debugging traces.

Enabling automatic log capture on process crash

About this task

The log capture tool collects debug logs automatically when a sub process crashes on Avaya Aura® Media Server.

Before you begin

Ensure that debug logging is enabled to capture the traces during the interval when a problem is observed on the system.

Procedure

1. Navigate to **EM** > **System Configuration** > **Debug Tracing** > **General Settings**.
2. Select **Enable Logcapture on Process Crash** to enable automatic debug log collection.
3. If instructed by Avaya support engineers, change **Logcapture File History** .

   Logcapture file history defines the number of rotating Log capture files that the system keeps before discarding the oldest file. By increasing this value, you can collect more data with more disk space consumption.
4. Click **Save**.

   Note:

   The location of the debug logs is `$MASHOME/platdata/crashcapture`. You will require Root access for accessing the log file. If required, contact Avaya support to request access to the log file.

Obtaining the UUID of a media server

About this task

When you install Avaya Aura® MS, the system assigns a universally unique identification (UUID) to Avaya Aura® MS. This UUID is a required input during various cluster configuration procedures.

Perform the following procedure to gain access to the UUID:

Procedure

1. Navigate to **EM** > **Cluster Configuration** > **Server Designation**.

   In the content pane, under **Local Server**, you can see the server **Name**, **Address**, **Role**, and the **UUID** which looks similar to this: 835c8aa4-6d0b-11e0-958e-001f296491ca.
2. Highlight the UUID.

   Ensure that you get all the characters. Triple-clicking on the UUID works in most browsers.

3. To copy the highlighted UUID, select **Copy** from the **Edit** menu of your browser, or press `Control+C`, or right-click on the highlighted **UUID** and select **Copy**.
4. Click in the target field related to the cluster configuration procedure you are following.
5. To paste the UUID in the field, select **Paste** from the **Edit** menu of your browser, or press `Control+V`, or right-click on the target field and select **Paste**.

Replacing Default Staging certificates

About this task

When you install Avaya Aura® MS, the system dynamically creates the self-signed certificates for the media server for each-installation. These dynamically created certificates contain a key certificate for the media server and the certificate of a private Certificate Authority (CA) that signs the key certificate.

If the media server generated certificate is in use, Avaya Aura® MS will generate an alarm.

Important:

The media server generated certificates are not considered secure. It is mandatory to replace the media server generated certificates soon after installation.

Before you begin

Ensure you have access to an organization-approved CA for the required certificate generation.

Procedure

1. Generate a unique key certificate for the media server using one of the following options for the signing CA:

Avaya Aura® System Manager	See *Creating a new certificate signed by System Manager as the root certificate authority in the key store* or *Creating a new certificate signed by System Manager as the intermediate certificate authority in the key store*
Another CA (internal or external)	See *Creating a new certificate to be signed by other Certificate Authorities in the key store* and *Processing a Certificate Signing Request Response in the key store*

Important:

Ensure to use the same CA to sign the key certificates for the servers in the same cluster. If the signing CA is not System Manager, you also need to import the CA certificate into the trust store of each server. For more information on importing a CA certificate, see *Importing a trust certificate to the trust store*.

2. Assign the generated key certificate to all MS service profiles, see *Assigning a certificate to a service profile*.
3. Delete the default staging key certificate from the key store, see *Deleting a key certificate from the key store*.
4. Delete the default staging CA certificate from the trust store, see *Deleting Certificate Authorities from the trust store*.
5. Reboot the media server for the certificate configuration changes to take effect.

Related links

Creating a new certificate signed by System Manager as the root certificate authority in the key store on page 132
Creating a new certificate signed by System Manager as the intermediate certificate authority in the key store on page 132
Creating a new certificate to be signed by other Certificate Authorities in the key store on page 133
Processing a Certificate Signing Request Response in the key store on page 134
Importing a trust certificate to the trust store on page 136
Assigning a certificate to a service profile on page 135
Deleting a key certificate from the key store on page 136
Deleting Certificate Authorities from the trust store on page 137

Chapter 5: Configuration

Configuration overview

This chapter describes how to activate a license, define translations, set protocol preferences, configure server clusters, and set up high availability configurations.

Before you use the configuration procedures, ensure you installed Avaya Aura® MS by using either the Quick Setup procedure or the installation procedures mentioned in *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS*.

N+1 Load Sharing cluster configuration

An N+1 Load Sharing cluster is a collection of Avaya Aura® Media Servers that work closely together. The cluster can be viewed as one system that is capable of providing service at an increased capacity and with redundancy. All the nodes in a cluster must be running the same application set.

An Avaya Aura® MS N+1 Load Sharing cluster must consist of a Primary and Secondary server. You can add additional servers, known as Standard servers.

Perform the following procedures to first configure the Primary, Secondary, and optional Standard servers and then connect the servers as an N+1 Load Sharing cluster.

In the following procedures, you can enable and configure a Replication Account. You must configure and enable the Replication Account by using the same user name and password on each server in the cluster. Replication is used for communication between the servers and enables configuration changes to be automatically replicated throughout the cluster when changes are made on the Primary server.

An Avaya Aura® MS cluster must use a centralized time source for clock synchronization. For more information, see *Setting the network time source server*.

Limitations:

- The maximum number of servers in a cluster is eight.
- N+1 Load Sharing clusters are engineered to provide the processing capacity of N servers. During normal operations, all N+1 servers are processing sessions. When one server is out of service, the cluster still provides the engineered capacity provided by N servers.

- Either the Primary or Secondary server must remain in service for the cluster to remain operational. Cluster service is lost if the Primary and Secondary servers are out of service at the same time.
- N+1 Load Sharing Clusters, and 1+1 High Availability clusters are two different configuration options that cannot be combined.
- A cluster must not span geographical locations. Cluster members must be on the same local network.

Related links

Setting the network time source server on page 66

Configuring a Primary server for a cluster

About this task

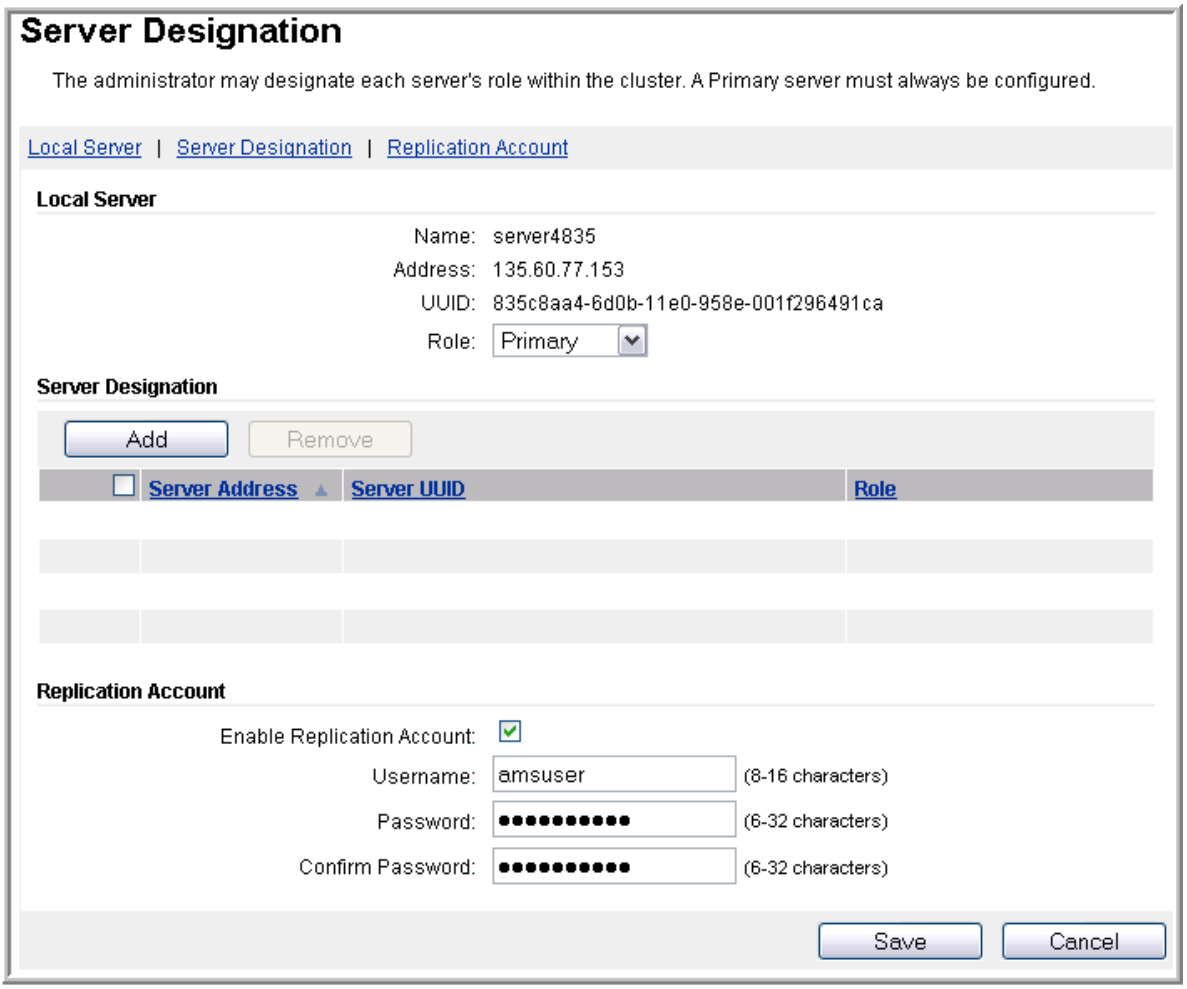
Using EM, perform the following procedure to configure Avaya Aura® MS as the Primary server in an N+1 Load Sharing cluster.

Before you begin

Ensure to replace the default staging certificates.

Procedure

1. To designate a server as primary, navigate to **EM** > **Cluster Configuration** > **Server Designation**.



2. In the **Local Server** section, ensure that **Role** is set to **Primary**.
3. Note the Primary node IP address and the UUID.

   You will need this information later to configure other nodes in the cluster.
4. In the **Replication Account** section, ensure **Enable Replication Account** is selected.
5. In the **Username**, **Password**, and **Confirm Password** fields, enter a user name and password.

   Important:

   All servers in the cluster must use the same Replication Account user name and password.
6. Click **Save**.
7. Click **Confirm**.

Related links

Replacing Default Staging certificates on page 30

Configuring a Secondary server for a cluster

About this task

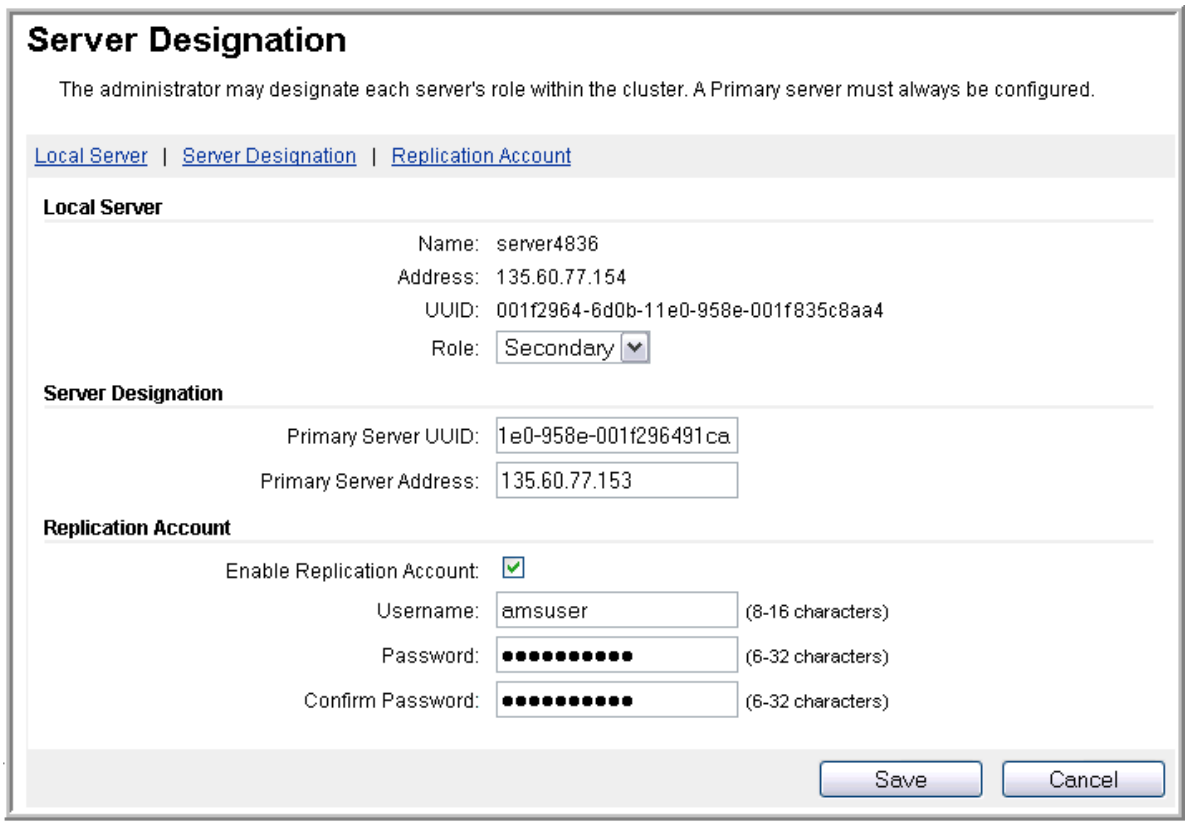
Using EM, perform the following procedure to configure Avaya Aura® MS as the Secondary server in an N+1 Load Sharing cluster:

Before you begin

- Ensure to replace the default staging certificates.
- Configure a separate Avaya Aura® MS as the Primary server with a Replication Account enabled.
- Obtain the UUID and the IP address of the Primary server.
- Obtain the user name and the password of the Replication Account of the Primary server.

Procedure

1. To designate a server as Secondary, navigate to **EM** > **Cluster Configuration** > **Server Designation**.



2. In the **Local Server** section, set **Role** to **Secondary**.

   The system updates the page with fields that are specific to the Secondary server configuration.

3. Using the EM for the Primary server, copy the UUID of the Primary server.

   For more information about copying the UUID, see *Obtaining the UUID of a media server*.

4. Using the EM for the Secondary server, paste the UUID of the Primary server in the **Primary Server UUID** field.
   a. In the **Primary Server Address** field, enter the IP address of the Primary server.
   b. In the **Replication Account** section, ensure **Enable Replication Account** is selected.
   c. In the **Username**, **Password**, and **Confirm Password** fields, enter the user name and password for the Replication Account on the Primary server.

      Important:

      All servers in the cluster must use the same Replication Account user name and password.
5. Click **Save**.
6. Click **Confirm**.
7. Restart Avaya Aura® MS for the changes to take effect. Navigate to **EM** > **System Status** > **Element Status** and click **Restart**.
8. Click **Confirm**.

Next steps

If you add a media server to a cluster enrolled in System Manager, then you must also enroll the new media server cluster node in System Manager.

Related links

Obtaining the UUID of a media server on page 29
Replacing Default Staging certificates on page 30
Configuring a Standard server for a cluster on page 36
Enrolling a media server after extending a cluster enrolled with System Manager on page 146

Configuring a Standard server for a cluster

About this task

Using EM, perform the following procedure to configure Avaya Aura® MS as a Standard server in the N+1 Load Sharing cluster.

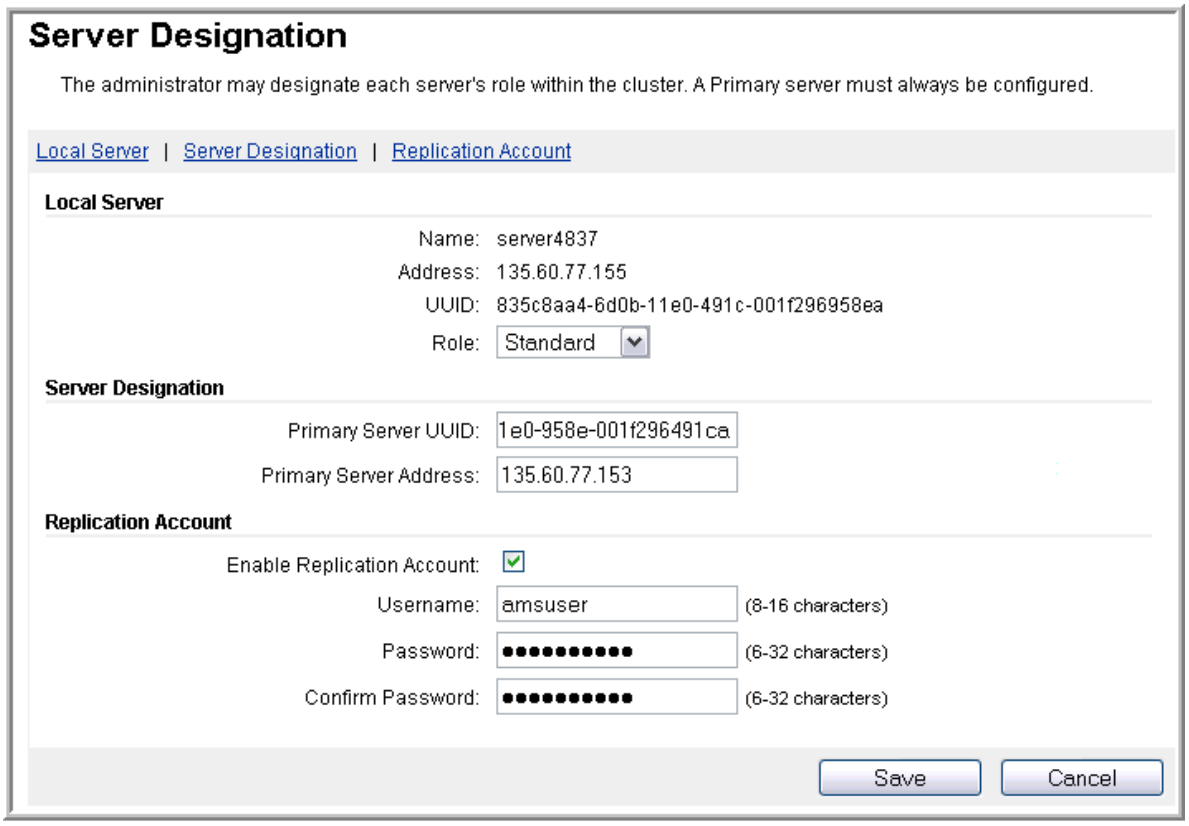
Add Standard nodes after you add Primary and Secondary nodes to the cluster.

Before you begin

- Ensure to replace the default staging certificates.
- Configure a separate Avaya Aura® MS as a Primary server and with a Replication Account enabled.
- Configure a separate Avaya Aura® MS as a Secondary server and with a Replication Account enabled.
- Obtain the UUID and the IP address of the Primary server.
- Obtain the user name and password of the Replication Account of the Primary server.

Procedure

1. To designate a server as Standard, navigate to **EM** > **Cluster Configuration** > **Server Designation**.



2. In the **Local Server** section, set the **Role** to **Standard**.

   The system updates the page with fields that are specific to the Standard server configuration.

3. Using the EM for the Primary server, copy the UUID of the Primary server.

   For more information about copying the UUID, see *Obtaining the UUID of a media server*.

4. Using the EM for the Standard server, paste the UUID of the Primary server in the **Primary Server UUID** field.

   a. In the **Primary Server Address** field, enter the IP address of the Primary server.

   b. In the **Replication Account** section, ensure **Enable Replication Account** is selected.

   c. In the **Username**, **Password**, and **Confirm Password** fields, enter the user credentials you entered for **Replication Account** on the Primary server.

Important:

All servers in the cluster must use the same Replication Account user name and password.

5. Click **Save**.
6. Click **Confirm**.
7. Restart Avaya Aura® MS for the changes to take effect. Navigate to: **EM** > **System Status** > **Element Status** and click **Restart**.
8. Click **Confirm**.
9. Repeat this procedure for each additional Standard server that you need to add to the cluster.

Next steps

If you add a media server to a cluster enrolled in System Manager, then you must also enroll the new media server cluster node in System Manager.

Related links

Obtaining the UUID of a media server on page 29
Replacing Default Staging certificates on page 30
Configuring a Secondary server for a cluster on page 35
Enrolling a media server after extending a cluster enrolled with System Manager on page 146

Configuring the replication settings for a cluster

About this task

You can enable replication for certain system settings and data.

When you enable **Configuration Replication**, the system replicates changes to all of the other servers in the cluster. This provides one central place for making configuration changes in a cluster.

Note:

When you enable **Configuration Replication**, many configuration changes can only be performed from EM of the Primary server.

Use this procedure to configure the replication preferences in an N+1 Load Sharing cluster:

Procedure

1. Log on to the Avaya Aura® MS Element Manager of the Primary media server.
2. Click **EM** > **Cluster Configuration** > **Replication Settings**.
3. Select **Configuration Replication**.
4. **(Optional)** Select any other items that you would like to replicate across all servers in the cluster.
5. Click **Save**.

6. To restart Avaya Aura® MS click **EM** > **System Status** > **Element Status** and click **Restart**.
7. Click **Confirm**.

Configuring SIP load balancing for a cluster

About this task

Load balancing is the responsibility of the application. The application must be configured to balance the session requests across all the nodes in the Avaya Aura® MS cluster. The cluster load balancing previously provided by Avaya Aura® MS is no longer available.

Replication of configuration settings in a cluster

After you configure an N+1 Load Sharing cluster and enable **Configuration Replication**, most configurable settings in EM for servers with roles other than Primary are unavailable. In a cluster, you use the Primary server EM to make changes to system settings. The system replicates the changes you make on the Primary server to all other servers in the cluster. Use EM of each server to configure items that are server specific, such as Server Designation.

Configuration replication does not replicate settings between different clusters.

During cluster upgrades, replication only occurs between media servers running the same release of software.

1+1 High Availability cluster configuration

The 1+1 High Availability cluster configuration ensures uninterrupted availability of media processing when a media server fails. Use the High Availability configuration option when you require the capacity of only a single Avaya Aura® MS.

The High Availability configuration deploys as a Primary server and a Backup server. Only one server is active at a time. The other server is waiting in synchronized hot standby to take over instantly.

Both servers must have identical configuration so that either server can take over the full media processing load if the other server fails. Ensure that the deployed servers meet the following requirements:

- Each media server in a 1+1 High Availability cluster deployed as a virtual machine (VM) must be deployed on separate but equally capable host servers with the same hardware and processor model. The VMs must be deployed using the same configuration profile so that they have the same number of vCPUs.
- Each media server in a 1+1 High Availability cluster deployed as non-appliance, software-only physical server or an Avaya physical appliance must be deployed on similar hardware with the same processor model. The servers can be from a different manufacturer, but

the two systems must have the same clock rate, number of cores, bus speed, and other performance-critical specifications.

- There is no inter-cluster communication between different 1+1 High Availability clusters. Different 1+1 High Availability clusters can use different hardware or profiles, but the specifications within a cluster must match.

To configure a 1+1 High Availability cluster, you must enable and configure a Replication Account with the same user name and password on each server. The system uses the Replication Account for communication between the servers. The Replication Account is also used for automatic replication of configuration changes to the Backup server when changes are made to the Primary server.

Perform the High Availability configuration procedures in the following sequence:

1. Configuring the Primary server for High Availability
2. Configuring the Backup server for High Availability
3. Completing 1+1 High Availability cluster configuration
4. Enabling High Availability

1+1 High Availability cluster synchronization overview

Servers in a 1+1 High Availability cluster pair communicate with each other using a heart-beat synchronization mechanism. Interruptions in the heart-beat from the active server trigger a failover to the standby server. The failure of a critical component process on the active server also triggers a failover to the standby server. The Primary and Backup servers are identical in functionality and configuration, resulting in a seamless failover.

The system synchronizes the state of all active sessions to the Backup server in real-time. State synchronization ensures the Backup server preserves the state of each active session without interruption to the user. Scenarios where the session state synchronization might not be fully synchronized, are handled by notifying the application of the failover. The failover notification provides the application the opportunity to run proper recovery steps for the given session state, for example, re-prompting the user for digit collection.

Both the Backup and the Primary servers can become active at the same time if the servers become network isolated from each other. When the servers reconnect, the servers exchange state information. The system uses the state information to select the server that becomes the active server and the server that becomes the standby server. The system selects the server that was the last server to process a new session as the active server. If the system did not process a new session then the server that was active the longest becomes active. In most cases, the server that was active for the longest period is the server that was active before the network isolation occurred.

When the High Availability state is locked, the system prevents failovers and service redundancy is unavailable. You set the High Availability state to locked only when the 1+1 High Availability cluster is recovering from a network isolation issue. The Locked state ensures that sessions are not lost from the server that processes the sessions during the network isolation recovery.

Under normal conditions, the High Availability state must not be unlocked. After the network isolation issue is resolved and both servers are actively part of the cluster, ensure that the High Availability state is not locked. Both servers must be unlocked to provide failover redundancy.

Restrictions and limitations of 1+1 High Availability clusters

1+1 High Availability clusters have the following restrictions and limitations:

- High Availability functionality is limited to specific applications. To determine if you can configure an application with High Availability, see adopting product documentation. Do not configure High Availability unless the adopting product documentation indicates it is supported.
- High availability is not supported in public cloud computing platforms such as Amazon Web Services.
- High Availability can be configured only in 1+1 configuration. N+1 Load Sharing clustering and 1+1 High Availability clustering are two different configuration options that you cannot combine.
- High Availability is available only if the servers are installed on the Linux® operating system.
- High Availability peer servers must be on the same subnet and the subnet must have Layer 2 network redundancy.
- High Availability servers must be configured with network interface bonding for increased performance and network interface redundancy.
- Splitting an 1+1 High Availability cluster across two data centers is not a recommended configuration. A stretch layer 2 LAN is required and round trip latency must be less than 50 milliseconds.
- IPv4 SIP signaling and media processing must use same IPv4 host address.
- If IPv6 is used, SIP signaling and media processing must use same IPv6 host address.
- If IPv6 is used, IPv4 and IPv6 host addresses must be on the same network interface.
- WebRTC and video media sessions are not preserved after failover.
- Core file generation on High Availability servers must be disabled. If not, end-users experience temporary voice loss or loss of service when processes unexpectedly quit. For more information on configuring core file generation, see *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS*.
- Both the Primary and Backup Avaya Aura® MS must use a common Network Time Protocol (NTP) server for clock synchronization.
- After the Backup server is active, service falls back to the Primary server only when the Backup server fails. To restore the Primary server to the active state immediately, manually set the Backup server status to **Failover**. Select **Failover** from the **More Actions** drop-down list on **EM** > **Element Status**.

Configuring the Primary server for High Availability

About this task

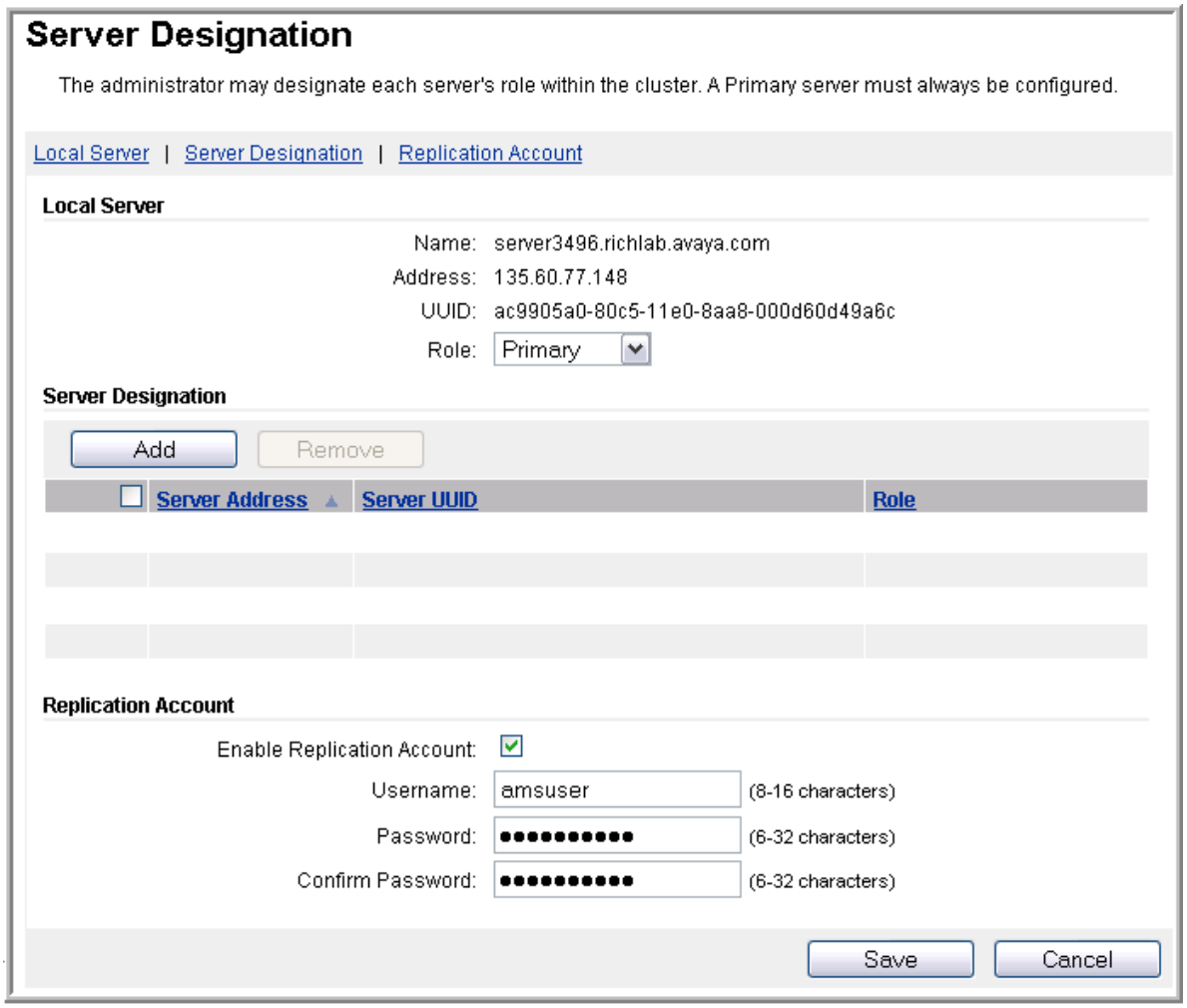
Using EM, perform the following procedure to configure the role of Avaya Aura® MS as a Primary server in a 1+1 High Availability cluster:

Before you begin

- Deploy two media servers to be configured as the Primary and Backup servers.
- Ensure to replace the default staging certificates.
- The Primary and Backup servers must have identical configuration so that either server can take over the full media processing load. Ensure that the servers in this cluster meet the 1+1 High Availability requirements listed at the beginning of this section.
- Ensure that the system is configured with a license.

Procedure

1. To designate Linux® based Avaya Aura® MS as a Primary server, navigate to **EM** > **Cluster Configuration** > **Server Designation**.
2. In the **Local Server** section, set the **Role** to **Primary**.



3. Note the Primary node IP address and the UUID since you will need this information later when configuring the Backup server.
4. In the **Replication Account** section, ensure **Enable Replication Account** is selected.
5. In the **Username**, **Password**, and **Confirm Password** fields, enter a user name and password.

   Important:

   Use the same Replication Account user name and password on both servers in the High Availability pair.
6. Click **Save**.
7. Click **Confirm**.

Next steps

Deploy and configure a Backup server for High Availability.

Related links

Replacing Default Staging certificates on page 30

Configuring the Backup server for High Availability

About this task

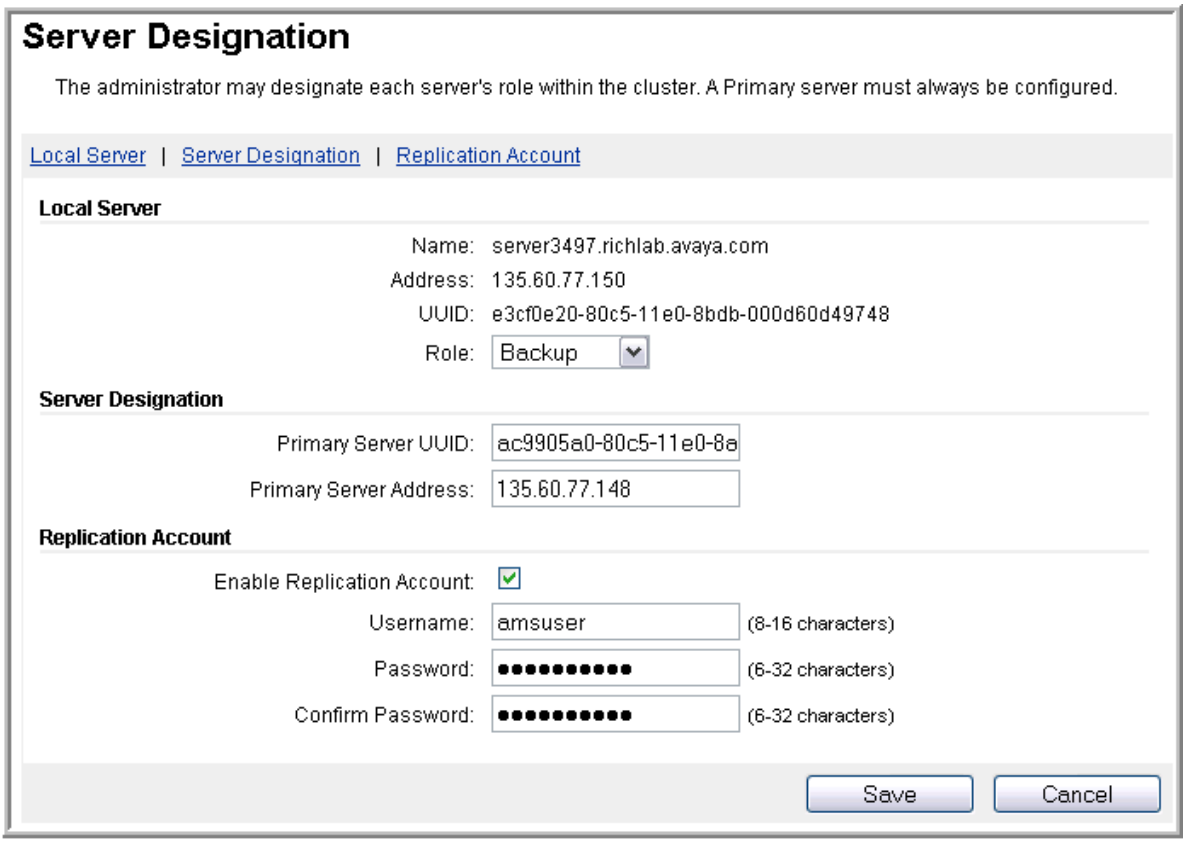
Using EM, perform the following procedure to configure Avaya Aura® MS as a Backup server in a 1+1 High Availability cluster.

Before you begin

- Ensure to replace the default staging certificates.
- Configure a separate Avaya Aura® MS as a Primary server with a Replication Account enabled.
- Obtain the UUID and the IPv4 address of the Primary server and the user name and password of the Replication Account.
- Ensure that the Primary and Backup servers are on the same subnet.
- Deploy a media server designated as the Backup server. To protect against hardware failure, High Availability media servers deployed as virtual machines (VMs) should be deployed on separate, equally capable host servers.
- The Backup server must have identical configuration to the Primary server so that it can take over the full media processing load. Ensure that the servers in this cluster meet the 1+1 High Availability requirements listed at the beginning of this section.

Procedure

1. To designate a Linux®-based Avaya Aura® MS as a Backup server, navigate to **EM** > **Cluster Configuration** > **Server Designation**.



2. In the **Local Server** section, set the **Role** to **Backup**.

   The system updates the page with fields specific to the Backup server configuration.

3. Using the EM for the Primary server, copy the UUID of the Primary server.

   For more information about copying the UUID, see *Obtaining the UUID of a media server*.

4. Using the EM for the Backup server, paste the Primary server UUID in the **Primary Server UUID** field.

   a. In the **Primary Server Address** field, enter the IPv4 address of the Primary server.

   b. In the **Replication Account** section, ensure **Enable Replication Account** is selected.

   c. In the **Username**, **Password**, and **Confirm Password** fields, enter the same credentials you entered for the Replication Account on the Primary server.

   Important:

   Use the same **Replication Account** user name and password on both servers in the High Availability cluster.

5. Click **Save**.

6. Click **Confirm**.

7. Navigate to **EM** > **System Status** > **Element Status** and click **Restart** for the changes to take effect.
8. Click **Confirm**.

Next steps

If you pair the Backup media server to a Primary server enrolled in System Manager, then you must also enroll the Backup media server in System Manager.

Related links

Obtaining the UUID of a media server on page 29
Replacing Default Staging certificates on page 30
Enrolling a media server after extending a cluster enrolled with System Manager on page 146

Completing 1+1 High Availability cluster configuration

About this task

Use this procedure to complete the High Availability server pairing:

Before you begin

Configure the Primary and Backup servers.

Procedure

1. Using the EM for the Primary server, navigate to **EM** > **Cluster Configuration** > **Server Designation**.
2. Confirm the following:
   - **Local Server Role** is set to **Primary**.
   - One server is shown in the **Server Designation** section and the server has the **Role** of **Backup**.
   - **Enable Replication Account** is selected.
3. If the Backup server is not listed in the **Server Designation** section, then do the following:
   a. Click **Add**.
   b. In the **Server Address** field, type the IPv4 address of the Backup server.
   c. In the **Server UUID** field, type the UUID of the Backup server.
   d. Select **Backup** for the Role.
   e. Click **Save**.

Next steps

Enabling High Availability on page 47.

Enabling High Availability

About this task

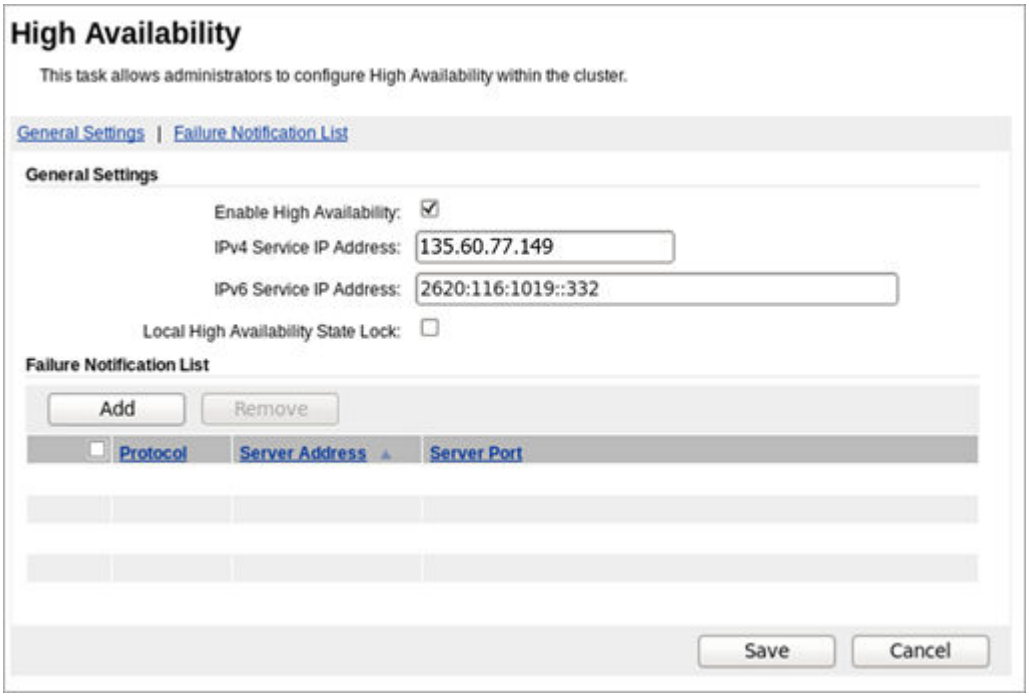
Use this procedure to configure the floating IPv4 (and optionally, IPv6) address on both the Primary and the Backup servers and to activate High Availability.

Before you begin

- Configure the Primary and the Backup servers.
- Obtain the desired floating IP addresses designated for the service provided by the media servers.
- Ensure that both the Primary and the Backup Avaya Aura® MS use a common Network Time Protocol (NTP) server for clock synchronization.

Procedure

1. Navigate to **EM** > **Cluster Configuration** > **High Availability**.
2. Select **Enable High Availability**.



3. In the **IPv4 Service IP Address** field, enter the floating service IPv4 address.
4. **(Optional)** In the **IPv6 Service IP Address** field, enter the floating service IPv6 address.
5. Clear **Local High Availability State Lock** check box, if selected.
6. **(Optional)** In the **Failure Notification List** area, click **Add** to add the address of the server in the adopting product which must be notified when a failover occurs.

   For information about the address to provide, see the documentation of the adopting product.

7. Click **Save**.
8. Click **Confirm**.

   The system restarts to activate the High Availability configuration.
9. Perform Step 1 to Step 8 using the same values, for both the Primary and the Backup Servers.

Reviewing High Availability configuration and status

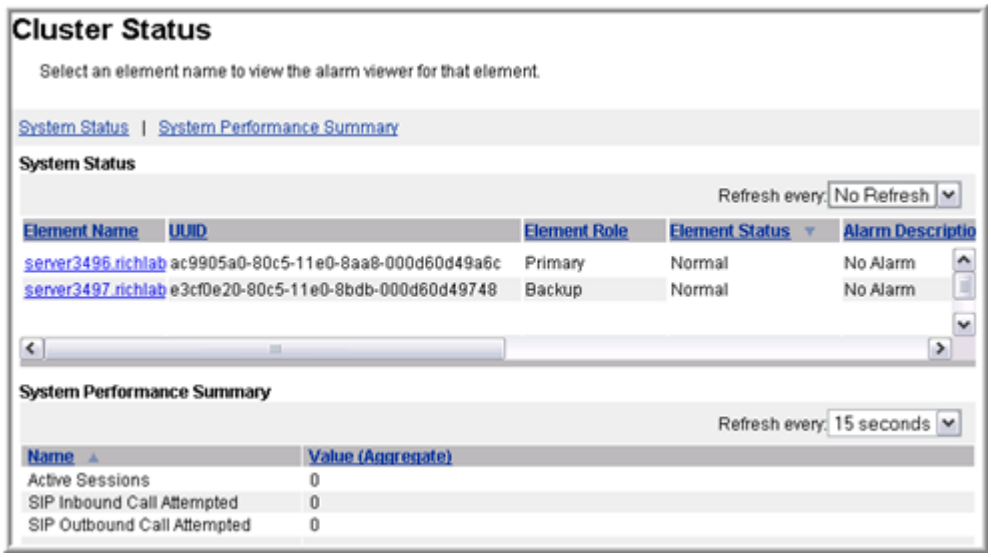
About this task

After the 1+1 High Availability cluster is formed, several EM pages display new features that reflect the new High Availability state.

Use this procedure to use the new features of High Availability and to ensure High Availability is in full service:

Procedure

1. Using the EM for the Primary server, navigate to **EM** > **System Status** > **Cluster Status**.
2. Confirm the following:
   - Only two nodes are listed.
   - One **Element Role** is listed for each of the Primary and Backup server.
   - No alarms are listed in the **Alarm Description** column.

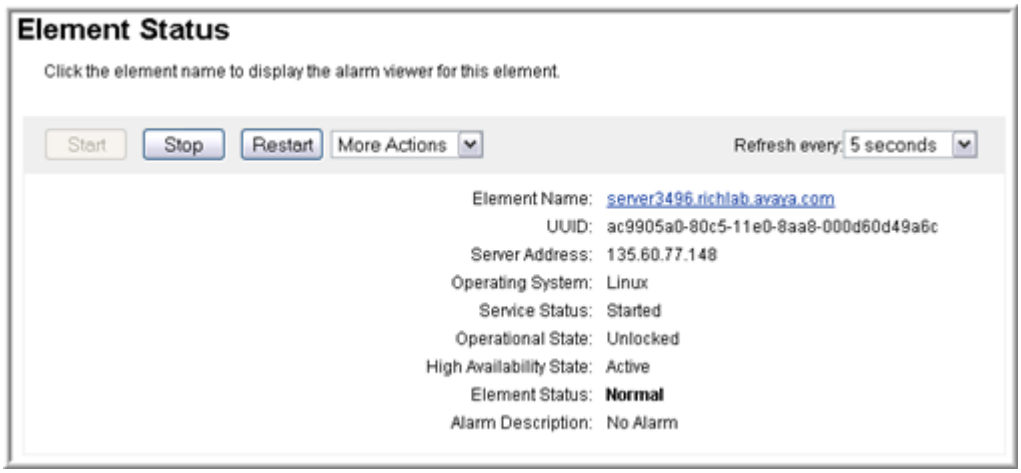


3. Navigate to **EM** > **System Status** > **Element Status**.

   The system now displays a new field, **High Availability State**, on the Element Status page.

   High Availability State must be **Active**.

   Ensure no alarms or service impacting states exist.

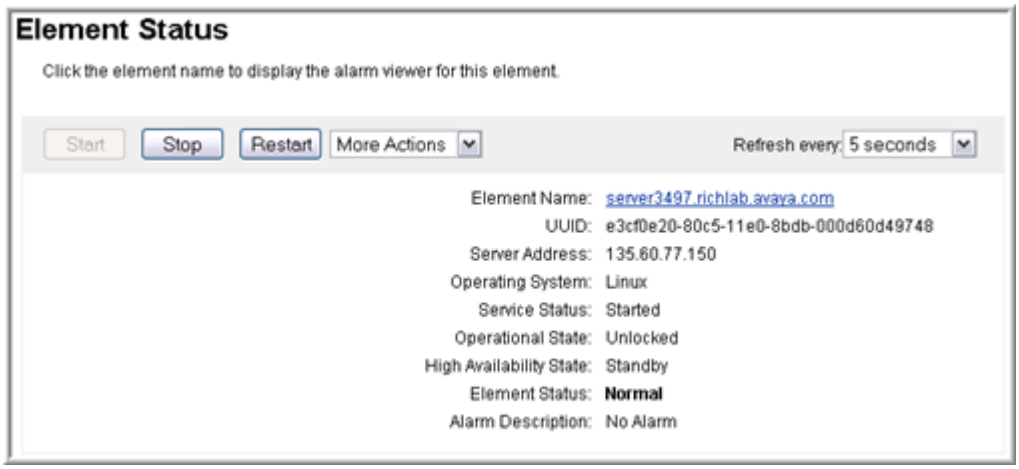


4. Using the EM for the Backup server, navigate to **EM** > **System Status** > **Element Status**.

   The system displays a new field, **High Availability State**, on the **Element Status** page.

   The **High Availability State** must be **Standby**.

   Ensure no alarms or service impacting states exist.



Locking and unlocking the High Availability state

About this task

When the High Availability state is locked the system prevents failovers and service redundancy is unavailable. You set High Availability to the locked state only when the 1+1 High Availability cluster is recovering from a network isolation issue. In the locked state, the sessions are not lost from the server processing the sessions during the network isolation recovery.

Under normal conditions the High Availability state must not be locked. After the network isolation issue is resolved and both servers are actively part of the cluster, ensure that the High Availability state is not locked. Both servers must be unlocked to provide failover redundancy.

Use this procedure to lock or unlock the High Availability state of Avaya Aura® MS.

Procedure

1. Navigate to **EM** > **Cluster Configuration** > **High Availability**.
2. Do one of the following:
   - To lock the High Availability state of the server and prevent failovers, select **Local High Availability State Lock**.
   - To unlock the High Availability state of the server and allow failovers, clear **Local High Availability State Lock**.
3. Click **Save**.
4. Click **Confirm**.

Recovering from network isolation

About this task

Media servers might become network isolated for the following reasons:

- Network switch failure or misconfiguration
- Network interface card (NIC) failure
- Network cables damaged or removed

When servers that are part of a 1+1 High Availability cluster are isolated from the network, they cannot communicate with each other. Both servers then enter the active High Availability state. However, only one of the servers is actually processing sessions.

To prevent loss of user sessions when the server is recovering from a network isolation condition, you must lock the High Availability state on the server that you determine is active and processing the sessions.

After the network isolation issue is resolved and both servers are back on the network, unlock the High Availability state in both servers to provide failover redundancy.

Use this procedure to recover High Availability servers from network isolation.

Procedure

1. Gain access to the server with the active sessions and navigate to **EM** > **Cluster Configuration** > **High Availability**.

   The server with active sessions is usually the only one you can access.
2. Lock the High Availability state of the server processing the sessions by selecting **Local High Availability State Lock**.
3. Perform the necessary hardware or network changes to recover the peer server from network isolation.
4. Unlock the High Availability state of the server processing the sessions by unselecting **Local High Availability State Lock**.
5. Click **Save**.

6. Click **Confirm**.

Related links

Viewing current active sessions on page 195
Locking and unlocking the High Availability state on page 49
Managing the High Availability state on page 24

Changing the Service IPv4 or IPv6 Addresses for a High Availability configuration

About this task

Use this procedure to update the Service IPv4 or IPv6 Addresses for a 1+1 High Availability cluster:

Before you begin

Stop both High Availability server peers before changing the Service IPv4 or IPv6 Addresses. For details, see Starting and stopping the media server on page 22.

Procedure

1. Navigate to **EM** > **Cluster Configuration** > **High Availability**.
2. Update the **IPv4 or IPv6 Service IP Address**
3. Update the **IPv6 Service IP Address**.
4. Click **Save**.
5. Click **Confirm**.
6. Repeat Step 1 to Step 5 for the peer server.
7. Start Avaya Aura® MS by navigating to **EM** > **System Status** > **Element Status**.
8. Click **Start**.
9. Click **Confirm**.
10. Check the **Operational State** by navigating to **EM** > **System Status** > **Element Status**.
11. If the **Operational State** is **Lock** or **Pending Lock**, select **Unlock** from the **More Actions** drop-down menu.
12. Click **Confirm**.
13. Repeat Step 7 to Step 12 for the peer server.

Related links

Starting and stopping the media server on page 22

Adding an IPv6 Service Address to a High Availability configuration

Adding an IPv6 Service Address to a High Availability configuration on Inactive Server

About this task

Use this procedure on the inactive server to add an IPv6 Service Address to an existing 1+1 High Availability cluster.

Procedure

1. To disable HA, navigate to **EM** > **Cluster Configuration** > **High Availability**.
2. Clear **Enable High Availability**.
3. Click **Save**.
4. Click **Confirm**.
5. If necessary, add a new IPv6 address to the server.
   a. Log in to a server console.
   b. Add the new IPv6 address using a specific procedure.
   c. Restart EM using the command:

      ```
      service avaya.em restart
      ```
6. To configure IPv6 from EM, navigate to **EM** > **System Configuration** > **Network Settings** > **IP Interface Assignment**.

   Configure the Signaling/Media IPv6 interfaces as required.
7. Click **Save**.
8. Click **Confirm**.
9. To enable HA, navigate to **EM** > **Cluster Configuration** > **High Availability** and select **Enable High Availability**.
10. Enter an **IPv6 Service Address**. Do not use a host name.
11. Click **Save**.
12. Click **Confirm**.

Adding an IPv6 Service Address to a High Availability configuration on Active Server

About this task

Use this procedure to add an IPv6 **Service Address** to an existing 1+1 High Availability cluster on active server.

Procedure

1. Navigate to **EM** > **System Status** > **Element Status**.
2. In **More Actions**, select **Failover**.
3. Click **Confirm**.

   This server is now the inactive server.
4. Now that this server is the inactive server, perform the procedure for Adding an IPv6 Service Address to a High Availability configuration on Inactive Server on page 52.

Related links

Selecting IP interface assignments on page 70

Disabling High Availability

About this task

When you no longer require the redundancy provided by a 1+1 High Availability cluster or you need to separate the servers for maintenance reasons, you can break-up the cluster resulting in two standalone servers, also known as simplex media servers.

Perform the following procedure to remove the configuration for a 1+1 High Availability cluster.

Procedure

1. Gain access to the Backup server and navigate to **EM** > **Element Status**.
2. If the Backup server is active then select **Failover** from the **More Actions** drop-down menu.

   The Primary server is now the active server. Wait until the alarms clear before continuing.
3. Gain access to the Primary server and navigate to **EM** > **Cluster Configuration** > **High Availability**.
4. Lock the High Availability state of the Primary server by selecting **Local High Availability State Lock**.
5. Disable High Availability on the Backup server by navigating to **EM** > **Cluster Configuration** > **High Availability** and clearing **Enable High Availability**.
6. Click **Save**.
7. Click **Confirm**.
8. Prevent new sessions from starting on the Primary server by navigating to **EM** > **System Status** > **Element Status** and clicking **More Actions** > **Pending Lock**.
9. Click **Confirm**.
10. Check for active sessions on the Primary server by navigating to **EM** > **System Status** > **Monitoring** > **Active Sessions**.

    Wait for the active sessions to end. The system automatically changes to the **Locked** state after all the sessions have ended.

Perform the following steps if you want to continue before the active sessions end:

a. Manually lock Avaya Aura® MS by navigating to **EM** > **System Status** > **Element Status** and clicking **More Actions** > **Lock**. Locking the media server also ends any remaining sessions.

b. Click **Confirm**.

11. Disable High Availability on the Primary server by navigating to **EM** > **Cluster Configuration** > **High Availability** and clearing **Enable High Availability**.
12. Click **Save**.
13. Click **Confirm**.
14. Gain access to the Backup server and navigate to **EM** > **Cluster Configuration** > **Server Designation**.
15. Select **Primary** for the **Role**.
16. Click **Save**.
17. Click **Confirm**.
18. Gain access to the original Primary server and navigate to **EM** > **Cluster Configuration** > **Server Designation**.
19. Remove the former Backup server from the **Server Designation** list by selecting the server and clicking **Remove**.
20. Click **Save**.
21. Click **Confirm**.
22. Unlock the original Primary server, by navigating to **EM** > **Element Status** and selecting **Unlock** from the **More Actions** drop-down menu.

    Both servers are now in service as simplex media servers.
23. **(Optional)** Both servers contain data in their Content Stores that was synchronized when the servers were configured as a High Availability cluster. You can remove the data from one or both servers by deleting the namespaces or content groups that you no longer need as follows:

    a. Navigate to **EM** > **Tools** > **Media Management**.

    b. Select the application related namespaces that you want to remove from the **Content Namespaces** list.

    c. Click **Delete…**

    d. Click **Confirm**.

Replication of configuration settings in a High Availability cluster

After configuring the 1+1 High Availability cluster, the system displays most configurable settings in EM as unavailable for the Backup server.

The 1+1 High Availability cluster requires that you make most of the changes using the Primary server EM. The system replicates the changes you make on the Primary server to the Backup server so that you only have to change the settings in one place. Items that are server specific, for example, server designation, require you to use the Backup server EM.

Configuration replication does not replicate settings between different clusters.

During cluster upgrades, replication only occurs between media servers with the same release of software.

Replication of Content Store data between clusters

Configuring replication of Content Store data between clusters

About this task

Content Store replication is a one-way data copy that only flows from the master cluster to the replica clusters. No changes are required on the master cluster to enable replication. Replica clusters connect to the master cluster using the Replication Account for authentication.

Content Store replication between clusters provides the following capabilities:

- Single point provisioning: Many clusters with common data, for example, announcement recordings, can be provisioned from a single designated master cluster. Replication ensures the data is copied from the master cluster to the replica clusters.
- Geographic-redundancy: A duplicate cluster at an alternate location can be maintained as a contingency cluster to receive traffic when the primary location becomes unavailable. The contingency cluster is a replica of the master cluster and receives all the Content Store application data in real-time so that it is ready to take over with the latest content. A contingency cluster must not receive traffic or provisioning changes when in standby.

  Perform the following procedure to enable replication of Content Store data between N+1 Load Sharing Cluster or 1+1 High Availability Clusters.

Before you begin

- Configure one Avaya Aura® MS cluster to function as the master cluster.
- Configure one Avaya Aura® MS cluster to function as the replica cluster.
- Obtain the UUID and the IP address of the Primary server.
- Obtain the username and the password of the Replication Account.

Procedure

1. Access the Element Manager (EM) for the Primary server in the replica cluster and navigate to **EM** > **Cluster Configuration** > **Replication Settings**.
2. In **Master Cluster Primary Node Address**, type the address of the Primary server of the master cluster.

Note:

A maximum of four replication clusters can point to one master cluster in a star topology. Chain topologies do not have a length limit and can be combined with star topologies.

3. Click **Save**.

   The Avaya Aura® MS system activates the replication immediately. The entire content data on the master cluster is copied to the replica cluster.

   If the system raises any critical mirror connection alarms, ensure that you have used the correct address and the Replication Account username and password are the same for all of the clusters.

   If you have not enabled **Configuration Replication** within the cluster, you must repeat Step 1 to Step 3 for each node in the replica cluster.

Disabling replication of Content Store data between clusters

About this task

Perform the following procedure to disable the replication of Content Store data between clusters:

Procedure

1. Using the EM for the Primary server in the replica cluster, navigate to **EM** > **Cluster Configuration** > **Replication Settings**.
2. Clear the **Master Cluster Primary Node Address** field.
3. Click **Save**.

   The system disables replication immediately.

   The system does not delete the content on the replica. The replica can use the local content the replica has, but will no longer receive updates from the master cluster. If required, use the EM Media Management tool to remove content data.

   If you have not enabled **Configuration Replication** within the cluster, repeat Step 1 to Step 3 for each node in the replica cluster.

Returning servers to a cluster

Special consideration must be made when returning certain media servers back to a cluster after they have been out of service for some time. There are two master Content Stores in every cluster. Servers with the role of Primary, Secondary and Backup contain master Content Stores. It is necessary to delete the content from a master Content Store that has been removed from service, before it is returned as a member of an active cluster. This prevents the re-appearance of deleted content that can still be present on the Content Store of a Primary, Secondary, or Backup server that was removed from service for some time.

You can use one of the following methods to delete content from an out-of-service Content Store before returning it to a cluster. Ensure that the server is isolated and not connected to the active cluster while performing these procedures.

- Uninstall the media server without preserving data, and then reinstall the media server. You can use a backup file to restore the Configuration Data, but do not restore the Application Content data. The newly installed media server has an empty Content Store.
- Use the Element Manager Media Management tool to remove all the application Namespaces. Restart the media server to run the deletion audit and remove the content.
- Use another provisioning interface that interfaces with the Content Store Web Services to remove all the application Namespaces. Restart the media server to run the deletion audit and remove the content.

When the server is returned to the cluster, the latest content from the peer master Content Store synchronizes automatically.

It is not required to delete the content from an out-of-service Content Store on a server with the role of Standard. Content Stores on Standard servers are not masters and will automatically delete obsolete content when they synchronize the latest content from one of the master Content Stores in the cluster.

Removing non-primary servers from a cluster

About this task

Perform the following procedure to remove a non-primary server from a cluster that has not been enrolled with System Manager. For clusters enrolled with System Manager, see Removing a non-primary server from an enrolled cluster on page 149.

Procedure

1. To remove a server from a cluster, access EM for the server to be removed. Navigate to **EM** > **Cluster Configuration** > **Server Designation**.
2. Set the **Role** to **Primary**.

   This puts the server in standalone, simplex mode.
3. Click **Save**.
4. Click **Confirm**.
5. Restart the media server for the change to take effect. Navigate to **EM** > **System Status** > **Element Status** and click **Restart**.
6. Click **Confirm**.
7. You can remove the server from the list of cluster members on the Primary server of the cluster. Access EM for the Primary server. Navigate to **EM** > **Cluster Configuration** > **Server Designation**.

8. In the **Server Designation** area, select the server to be removed and click **Remove**.
9. Click **Save**.
10. Click **Confirm**.
11. Restart the media server for the change to take effect. Navigate to **EM** > **System Status** > **Element Status** and click **Restart**.
12. Click **Confirm**.

Video Compositor Configuration

An Avaya Aura® MS can be configured as a Video Compositor which provides video transcoding and compositing services. A solution can contain one or more backend Avaya Aura® Media Servers configured to provide video compositing services. These video composite servers are configured behind one or more frontend Avaya Aura® Media Servers, which perform video processing.

Enabling Video Composite Services

About this task

Perform the following procedure to configure Video Composite services.

Before you begin

Deploy one or more Avaya Aura® Media Servers to configure as backend video composite servers. If this media server is a virtual appliance, you must increase the system capacity by resizing the VM. See *Deploying and Updating Avaya Aura® Media Server Appliance*.

Deploy one or more Avaya Aura® Media Servers to configure as frontend video processing servers.

Procedure

1. For each backend video composite server, perform the following steps:
   a. Navigate to **EM** > **System Configuration** > **Server Profile** > **Advanced Settings**.
   b. Select **Video Compositor** for the **Server Profile** setting.
   c. Click **Save**.
   d. Restart Avaya Aura® MS for the changes to take effect. Navigate to **EM** > **System Status** > **Element Status** and click **Restart**.
2. For each frontend Avaya Aura® MS using these Video Composite servers as a resource, perform the following steps:
   a. To Configure the server profile and functions, navigate to **EM** > **System Configuration** > **Server Profile** > **Advanced Settings**.
   b. Select **Default** for the **Server Profile** setting.

c. Select **Video Media Processor**.

d. Select **Video Compositor**.

e. Click **Save**.

f. To configure video composite resources, navigate to **EM** > **System Configuration** > **Media Processing** > **General Settings** > **Compositor Resource**.

g. For each video compositor server, add the hostname or IP address.

h. Click **Save**.

i. Restart Avaya Aura® MS for the changes to take effect. Navigate to **EM** > **System Status** > **Element Status** and click **Restart**.

Web Collaboration Configuration

You can configure Avaya Aura® MS to provide whiteboard and screen sharing web collaboration services. Web collaboration services are available when you enable the Web Collaboration Server Function on frontend Avaya Aura® Media Servers. The Avaya Equinox Management Conference Focus application controls access to collaboration meetings. The Conference Focus application provides the following functions in the solution:

- Routes and authenticates participant connections to a frontend Avaya Aura® MS with collaboration resources.
- Organizes participants into meetings and manages cascaded meetings.

Enabling Web Collaboration

About this task

Perform the following procedure to enable web collaboration services on frontend Avaya Aura® Media Servers.

Before you begin

Deploy the Equinox Management system and one or more Avaya Aura® Media Servers to configure as frontend video processor and web collaboration servers.

Procedure

1. Navigate to **EM** > **System Configuration** > **Server Profile** > **Server Function**.
2. Select **Web Collaboration**.
3. Click **Save**.
4. Restart the media server to activate Web Collaboration. Navigate to **EM** > **System Status** > **Element Status** and click **Restart**. Click **Confirm**.
5. To configure Web Collaboration properties, navigate to **EM** > **System Configuration** > **Web Collaboration** > **General Settings** > **Conference Focus**.

6. In the **FQDN** field, type the fully qualified domain name that users use to access the Web Collaboration service.
7. In the Web Collaboration **Port** field, type `443`.
8. To configure the list of trusted Focus servers, in the **Trusted Nodes** field, add the IP addresses of the trusted Focus servers separated by a semicolon (;). You must use the physical IP address of each server and not the virtual IP address or hostnames.
9. Click **Save**.
10. To configure Web Collaboration connection properties, navigate to **EM** > **System Configuration** > **Web Collaboration** > **Advanced Settings** > **Conference Focus**.
11. To use secure connections, select **Enable TLS**.
12. In the **API Version** field, select `1`.
13. Click **Save**.

License configuration

Licensing configuration shows how to enter your license keycodes, which enable the purchased features on your system.

You can configure Avaya Aura® MS licensing in two ways. Only one of the licensing schemes is active at a time:

License type	Description
Nodal Licensing	A Nodal License is bound to a particular Avaya Aura® MS server and is not shared across Avaya Aura® MS nodes. In this node-locked configuration, you must configure each Avaya Aura® MS node with its own license key.
WebLM Server	WebLM Servers use the Avaya WebLM Web-based licensing management system.

Choose the licensing configuration procedure based on the type of license provided.

Configuring WebLM Server licensing

About this task

In the WebLM configuration, you install licenses on the Avaya Web License Manager server.

Each Avaya Aura® MS is configured with the URL of the WebLM server that it uses to acquire licenses.

Procedure

1. Access the Element Manager (EM) for each of the servers and navigate to **EM** > **Licensing** > **General Settings**.
2. From the **Licensing** drop-down menu, select **WebLM Server**.
3. In **Server Host Name or IP Address**, type the address of the WebLM server to use.
4. In **Server Port**, type the port to use with the WebLM server. The WebLM server processes license requests from the port you configure in **Server Port**. The default port is 52233.
5. Type the **URL Suffix** used to identify the WebLM server. The default **URL Suffix** is `/WebLM/LicenseServer`.
6. Click **Save**.

   The system displays a confirmation page.
7. Click **Confirm**.
8. To apply the new license, navigate to **EM** > **System Status** > **Element Status** and click **Restart**.
9. Click **Confirm**.
10. To confirm your license configuration, verify that there are no active Licensing alarms raised on **EM** > **System Status** > **Alarms**.
11. Repeat this procedure for each media server in the cluster.

Configuring Nodal Licensing

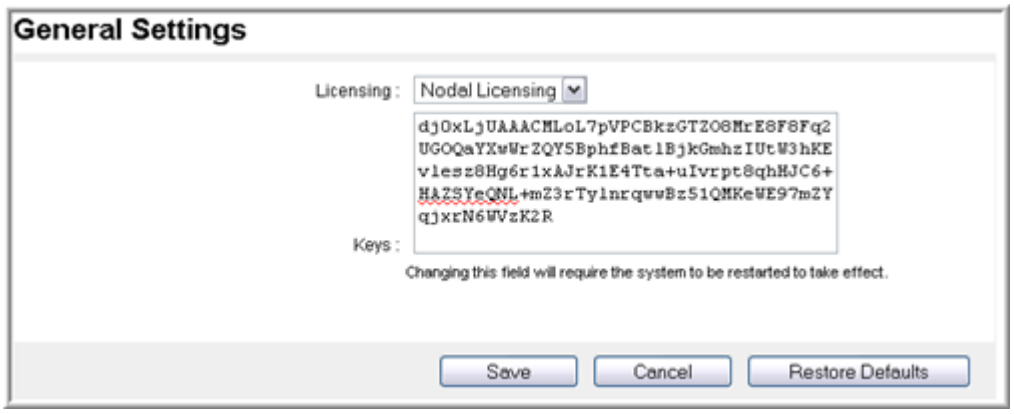
About this task

In the Nodal Licensing configuration, the system configures each Avaya Aura® MS with a node-locked key that enables features only for that server. The key is based on the unique MAC addresses of each server and does not work on any other server.

Perform the following procedure to configure a nodal license:

Procedure

1. Gain access to EM for each of the servers and click **EM** > **Licensing** > **General Settings**.
2. From the **Licensing** drop-down menu, select **Nodal Licensing**.



3. Apply the license key generated specifically for this server by copying and pasting the license key into the **Keys** field.
4. Click **Save**.

   The system displays a confirmation page.
5. Click **Confirm**.
6. Navigate to **EM** > **System Status** > **Element Status** and click **Restart** to apply the new license.
7. Click **Confirm**.
8. To confirm the license configuration, verify that there are no active licensing alarms raised on **EM** > **System Status** > **Alarms**.
9. Repeat Step 1 to Step 8 for each media server in the cluster.

Updating Nodal Licensing keys

About this task

If Avaya provides you with a new Nodal License key, then perform the following procedure to update an existing key:

Procedure

1. Gain access to the EM for each of the media servers and navigate to **EM** > **Licensing** > **General Settings**.
2. Remove the old license key by clicking **Keys** field and then pressing `Control+A` to select the old key.
3. Press the `Delete` or the `Backspace` key.
4. Copy and paste the new license keys into the **Keys** field.
5. Click **Save**.

   The system displays a confirmation page.
6. Click **Confirm**.

7. Navigate to **EM** > **System Status** > **Element Status** and click **Restart** to apply the new license.
8. Click **Confirm**.
9. To confirm your license configuration, verify that there are no active licensing alarms raised on **EM** > **System Status** > **Alarms**.
10. Repeat this procedure for each media server in the cluster.

License utilization alarm threshold configuration

The system raises utilization threshold alarms after a license reaches or exceeds the provisioned license utilization threshold percentage.

Setting nodal licensing alarm thresholds

About this task

Perform the following procedure when you have selected the **Nodal Licensing** option.

You cannot disable License utilization threshold alarms while using Nodal Licensing. However, you can configure the alarm threshold.

Procedure

1. Navigate to **EM** > **Licensing** > **General Settings**.
2. In **Nodal License Utilization Threshold**, enter the threshold percentage for the alarm.
3. Click **Save**.

Server profile configuration

Setting the capacity profile

About this task

Avaya Aura® MS automatically selects a capacity profile that matches the performance limits of the physical or virtual hardware that the system is installed on. The selected profile restricts the maximum number of sessions Avaya Aura® MS concurrently supports. You can select a capacity profile that lowers the maximum number of sessions to conserve system resources, such as CPU and memory. Restricting resources is useful when Avaya Aura® MS is deployed co-resident with other software.

Note:

The processor affinity configuration can limit the options available for the Avaya Aura® MS capacity profile configuration on EM.

Perform the following procedure to limit the server resource use and the processing capacity of Avaya Aura® MS:

Procedure

1. Navigate to **EM** > **System Configuration** > **Server Profile** > **General Settings** > **Capacity Profile**.
2. To select the required size, assign the required processing capability to Avaya Aura® MS by using the **Capacity Profile** drop-down menu.

   The system updates the **Maximum Sessions** field to indicate the highest number of sessions Avaya Aura® MS supports with the selected **Capacity Profile**.
3. Click **Save**.
4. For the changes to take effect, restart Avaya Aura® MS.

Related links

Setting the processor affinity configuration on page 65

Setting the media server function

About this task

Perform the following procedure to enable the required media processing functions for Avaya Aura® MS. Optional media processing software components provide the services for each function. The components that you enable are available for processing after you restart Avaya Aura® MS.

Procedure

1. Navigate to **EM** > **System Configuration** > **Server Profile** > **General Settings** > **Server Function**.
2. **(Optional)** To enable firewall network address translation (NAT) tunneling services to Internet Connectivity Establishment (ICE) enabled endpoints, select **Firewall NAT Tunneling Media Processor**.
3. **(Optional)** To enable video processing and routing services, select **Video Media Processor**.

   Note:

   The Video Media Processor does not currently support IPv6. SDP received by Avaya Aura® MS must contain a video media stream with IPv4 to negotiate video. ANAT is not supported for video.
4. **(Optional)** To enable VoiceXML application services, select **VoiceXML Interpreter**.
5. Click **Save**.
6. For the changes to take effect, restart Avaya Aura® MS.

Viewing the server hardware properties

About this task

Perform the following procedure to view the server CPU and memory details of the server.

Procedure

Navigate to **EM** > **System Configuration** > **Server Profile** > **Processor Affinity** > **CPU and Memory Details**.

Setting the processor affinity configuration

About this task

The processor affinity configuration provides a mechanism to restrict the CPU-intensive media processing on the media server to a subset of logical processors you designate. Certain deployments require changes to the processor affinity configuration to maximize performance.

Processor affinity configuration is only supported on Microsoft Windows® systems.

For example, a Windows®-based dual eight-core server has two CPU sockets each with a processor containing eight cores, for sixteen logical processors. Hyper-threading doubles the number of available logical processors. With hyper-threading enabled, the number of logical processors is 32. Avaya Aura® MS performance on this particular Windows® system is optimized when the media processing components are assigned to the sixteen logical processors of the processor in socket one. In this case, socket one is preferred for Avaya Aura® MS processing because packet interrupt handling is assigned to socket zero. This reduces the processing capacity available to Avaya Aura® MS in socket zero.

Note:

Reducing the number of processor cores that are available for the media processing components can impact system capacity. It also limits the options available for the Avaya Aura® MS capacity profile configuration on EM.

The following media processing components adhere to the processor affinity settings:

- Conference Media Processor
- Interactive Voice Response Media Processor
- Video Media Processor
- Firewall NAT Tunneling Media Processor

Perform the following procedure to enable or disable media processing for each logical processor on the system:

Procedure

1. Navigate to **EM** > **System Configuration** > **Server Profile** > **Processor Affinity**.
2. Configure the processors to use for media processing by selecting the required logical processors in the **Allow Execution** column.
3. Click **Save**.
4. For the changes to take effect, restart Avaya Aura® MS.

Related links

Viewing the server hardware properties on page 64
Setting the capacity profile on page 63

Network settings configuration

Setting the administrative name and description

About this task

Perform the following procedure to assign a unique name and description to each media server:

Procedure

1. Navigate to **EM** > **System Configuration** > **Network Settings** > **General Settings**.
2. To assign a unique name to the media server, enter a name of your choice in the **Element Administrative Name** field.
3. To assign a description to the media server, enter the description in the **Element Administrative Description** field.
4. Click **Save**.

Setting the network time source server

About this task

All the Avaya Aura® MS clusters must use a common network time source server so that the time across the nodes is synchronized. The system might encounter problems if the servers do not have the synchronized time.

Important:

If media servers are enrolled with System Manager, then the media servers and System Manager must use the same NTP server for time synchronization. The system time difference between the System Manager and the media servers must not exceed 10 minutes.

Perform the following procedure to configure Network Time Protocol (NTP) servers for each Avaya Aura® MS:

Procedure

1. Navigate to **EM** > **System Configuration** > **Network Settings** > **General Settings** > **General**.
2. In the **Network Time Source Server** field, enter the IP address or hostname of a up to three network time source (NTP) servers.
3. Click **Save**.

Configuring SOAP

About this task

Avaya Aura® MS uses Simple Object Access Protocol (SOAP) to provide various Web services and administrative tasks to clients.

Perform the following procedure to configure Avaya Aura® MS SOAP attributes:

Procedure

1. Navigate to **EM** > **System Configuration** > **Network Settings** > **General Settings** > **SOAP**.
2. (Optional) Set the **Server Private Key**.

   If you use this key, ensure the key matches on the client as well as the server side of the SOAP interface.
3. Select **Enable Trusted SOAP Nodes** if you want to restrict the SOAP connections to Avaya Aura® MS.
4. In the **Trusted Nodes** field, enter the addresses of the nodes that can gain access to the SOAP services offered by Avaya Aura® MS.

   Separate multiple addresses with semicolons.

   The **Trusted Nodes** field needs to be populated only if **Enable Trusted SOAP Nodes** is selected.
5. **(Optional)** Configure **Enable HTTP Digest Authentication**.

   If you choose to enable HTTP Digest Authentication, configure the following:

   - HTTP Digest Authentication Domain
   - HTTP Digest Authentication User Name
   - HTTP Digest Authentication Password
6. Select **Enable SOAP TLS Transport** to use TLS for SOAP connections to Avaya Aura® MS.

   Important:

   If you select **Enable SOAP TLS Transport**, ensure that mutual authentication is properly set up between the SOAP client and the Avaya Aura® MS SOAP service.
7. Click **Save**.
8. Restart Avaya Aura® MS for the changes to take effect. Navigate to **EM** > **System Status** > **Element Status** and click **Restart**.
9. Click **Confirm**.

Configuring connection security options

Procedure

1. Navigate to **EM** > **System Configuration** > **Network Settings** > **General Settings** > **Connection Security**.
2. For the system to verify that the subject name and the target host name match in certificates, select **Verify Host Name**.

3. To configure TLS for all external media server connections, select **Enable TCP TLS Transport**.

   This does not enable TCP TLS Transport for remote database connections.

4. To support real-time certificate revocation, enable support for Online Certificate Status Protocol (OCSP) on TLS connections. To enable this, select **Enable OCSP** and configure the following OCSP options:

   a. Configure the timeout interval for OCSP query responses in the **OCSP Response Timeout (ms)** field.

   b. To allow TLS connections even if no OCSP response is received, select **OCSP Permit if no Response**.

   c. Use synchronous OCSP queries by selecting **Enable OCSP Synchronous Mode**.

5. To allow either side of a TLS connection to change the parameters of the established secure session, select **TCP TLS Session Renegotiation Enable**.

6. To configure the number of minutes between TLS renegotiations, set **TCP TLS Session Renegotiation Timer (min)**.

7. To specify that the connections from other media servers or remote element managers must use a secure TLS connection to the media server database, select **Use TCP TLS Transport for Remote Database Connections**.

8. Click **Save**.

9. Restart Avaya Aura® MS for the changes to take effect. Navigate to **EM** > **System Status** > **Element Status** and click **Restart**.

10. Click **Confirm**.

Configuring TLS ciphers for connections

About this task

Perform the following procedure to enable and rank the required TLS ciphers for each service profile on the system. For each cipher, select the service profiles that can use the cipher. For service profile descriptions, see Security configuration on page 131. Enter a rank for each cipher to define the relative preference of the ciphers for each service profile.

Procedure

1. Navigate to **EM** > **System Configuration** > **Network Settings** > **Advanced Settings** > **TLS Ciphers**.

2. Select the service profile and cipher configurations required for the system.

3. For each cipher with service profile selections, rank the preference for using the cipher relative to other selected ciphers for the same service profile. The rank is a number between 0 and 2147483647, where 0 represents the highest preference in the rank.

Tip:

You can list the ciphers by assigned rank by clicking on the **Rank** column. You can list the ciphers by name by clicking on the **Cipher Name** column.

4. Click **Save**.
5. Click **Confirm**.

   Avaya Aura® MS restarts for the changes to take effect.

Related links

Security configuration on page 131

Configuring transmit prioritization

About this task

When Avaya Aura® MS is installed on a Linux® system, you can control the output priority of signaling and media packets relative to other traffic by configuring Transmit Prioritization settings. These settings configure the operating system to transmit delay sensitive media packets ahead of delay tolerant traffic, such as FTP, HTTP, and SSH. Proper Transmit Prioritization helps guarantee Avaya Aura® MS can provide the required bit rate, delay, jitter, and packet loss for media sessions.

Note:

If you observe the Transmit Prioritization Configuration Error alarm, then consult with Avaya support engineers before the following procedure.

Procedure

1. Navigate to **EM** > **System Configuration** > **Network Settings** > **General Settings** > **Transmit Prioritization**.
2. Select **Transmit Prioritization Enable**.
3. (Optional) Specify a class identifier in the **Root Traffic Control class ID** field. Alter this value to resolve Transmit Prioritization conflicts encountered with other software installed on the server.
4. (Optional) Specify a class identifier in the **High-priority Traffic Control class ID** field. Alter this value to resolve Transmit Prioritization conflicts encountered with other software installed on the server.
5. (Optional) Select **Enable Alarm Suppression for Transmit Prioritization Conflicts** to prevent the system from generating alarm notifications when Transmit Prioritization conflicts are encountered with other software installed on the server.

   Select **Enable Alarm Suppression for Transmit Prioritization Conflicts** only when conflicts are handled in a way other than changing the **Root Traffic Control class ID** or **High-priority Traffic Control class ID** fields.
6. Click **Save**.

Selecting IP interface assignments

About this task

Avaya Aura® MSsupports SDP containing IPv4 and IPv6 network address types using the ANAT (Alternate Network Address Types) protocol as described in RFC 4091.

The IP network address assignment functions as follows:

When Transport is set to IPv4 Only:

- The SDP offer generated by Avaya Aura® MS does not contain IPv6.
- The SDP answer from Avaya Aura® MS is always IPv4.
  - If the incoming SDP is IPv4 only, the SDP answer is IPv4 only.
  - If the incoming SDP is ANAT IPv4/IPv6, the SDP answer is ANAT with IPv4 selected.
- Preferences for remote and local offers are not used when IPv4 only is selected as the transport.

When Transport is set to Dual IPv4/IPv6:

- Avaya Aura® MS generates an SDP offer containing both IPv4 and IPv6 using ANAT. The ordering of IPv4/IPv6 is determined by using the **Preferences for Local Offers** as follows:
  - If **Preferences for Local Offers** is set to **IPv4 Preferred**, then the SDP contains ANAT with both IPv4/IPv6 and with IPv4 preferred in the ANAT group.
  - If **Preferences for Local Offers** is set to **IPv6 Preferred**, then the SDP contains ANAT with both IPv4/IPv6 and with IPv6 preferred in the ANAT group.
- Avaya Aura® MS generates SDP answer using the **Preferences for Remote Offers** as follows:
  - If **Preferences for Remote Offers** is set to the default of **Use Remote Preference**, then the selection of IPv4 or IPv6 is based on the received SDP preference:
    - For incoming IPv4 only SDP, IPv4 only SDP is used.
    - For incoming IPv6 only SDP, IPv6 only SDP is used.
    - For incoming ANAT SDP with IPv4 preferred over IPv6, IPv4 is used in the ANAT response.
    - For incoming ANAT SDP with IPv6 preferred over IPv4, IPv6 is used in the ANAT response.
  - If **Preferences for Remote Offers** is set to **IPv4 Preferred**, the system overwrites the remote preference and sets IPv4 is in the offer.
    - For incoming IPv4 only SDP, IPv4 only SDP is used.
    - For incoming IPv6 only SDP, IPv6 only SDP is used, since this was the only transport offered.
    - For incoming ANAT SDP with IPv4 preferred over IPv6, IPv4 is used in the ANAT response.
    - For incoming ANAT SDP with IPv6 preferred over IPv4, IPv4 is used in the ANAT response.

- If **Preferences for Remote Offers** is set to **IPv6 Preferred**, the system overwrites the remote preference and sets IPv6 is in the offer.
  - For incoming IPv4 only SDP, IPv4 only SDP is used.
  - For incoming IPv6 only SDP, IPv6 only SDP is used.
  - For incoming ANAT SDP with IPv4 preferred over IPv6, IPv6 is used in the ANAT response.
  - For incoming ANAT SDP with IPv6 preferred over IPv4, IPv6 is used in the ANAT response.

Perform the following procedure to configure the IP interfaces for Avaya Aura® MS:

Before you begin

IPv4 is enabled by default. If your system requires IPv6, you must ensure it is enabled before proceeding with Avaya Aura® MS interface assignments. If IPv6 is not enabled, then EM only displays IPv4 options. For information about enabling IPv6 for Linux®, see the OS documentation.

Procedure

1. Navigate to **EM** > **System Configuration** > **Network Settings** > **IP Interface Assignments**.
2. Under **IPv4 Interfaces**, select the desired IPv4 address for each interface: **Signaling**, **Media**, **Cluster** and **OAM**.
3. Under **IPv6 Interfaces**, select IPv6 address for **Signaling** and **Media Cluster** interfaces, if desired.
4. If 1+1 High Availability configuration is desired:
   a. IPv4 Signaling and Media Cluster addresses must match.
   b. If IPv6 is configured:
      - IPv6 Signaling and Media Cluster addresses must match.
      - IPv4 and IPv6 addresses must be on the same network interface.
5. If IPv6 is enabled for your system, then configure the following:
   a. In the **IP Configuration** section, select the **Transport mode** as either **Dual IPv4/IPv6** or **IPv4 Only**.
   b. In the **IP Configuration** section, select **Preferences for Remote Offers**.
   c. In the **IP Configuration** section, select **Preferences for Local Offers**.
6. Click **Save**.

Configuring name resolution

About this task

You can use EM to view and update IP address and hostname mappings for the server. The server preserves this data in the local hosts file. The hosts file is preserved in Avaya Aura® MS backups.

Important:

Avaya also provides appliance versions of Avaya Aura® MS. Do not use this document when you are working with Avaya Aura® MS as a physical or virtual appliance. For appliance installations, see *Deploying and Updating Avaya Aura® Media Server Appliance*.

Note:

The Name Resolution page in EM does not display the localhost IP and local hostname data.

Procedure

1. Navigate to **EM** > **System Configuration** > **Network Settings** > **Name Resolution**.
2. To add a new name resolution mapping to the existing list click **Add**.
3. Add the **IP Address** and the **Hostname** for a new mapping or alter the values of an existing mapping.
4. To remove a mapping, click in the checkbox next to the IP address and click **Remove**.
5. Click **Save**.

Changing media port ranges

About this task

Avaya Aura® MS requires a range of dedicated ports for RTP, SRTP, RTCP, and SRTCP, media connections.

You can configure a contiguous port range for Avaya Aura® MS media ports in the basic configuration mode. You can use the advanced configuration mode to configure several ranges for Avaya Aura® MS media ports. Configuring multiple smaller ranges of ports is useful to avoid overlapping with ports that other software on the server requires.

Perform the following procedure to configure the media port range available for Avaya Aura® MS sessions.

Before you begin

When High Availability is enabled, the Backup server must be stopped before configuring the media port range. Make the configuration change on the Primary server after the Primary server High Availability state displays active. Restart the Primary server to apply the change. This restart results in a loss of service. After the Primary High Availability state displays active, restart the Backup server.

Procedure

1. Navigate to **EM** > **System Configuration** > **Network Settings** > **Advanced Settings** > **Media Port Ranges**.
2. Choose the **Configuration Mode**:
   - To configure a contiguous media port range, select **Basic**.
   - To configure multiple media port ranges, select **Advanced**.

3. Choose one of the following:
   - If you have selected the Basic configuration mode, enter the beginning of the port range in the **Start Port** field. Enter the end of the port range in the **End Port** field.
   - If you have selected the Advanced configuration mode, click **add** to create a new range. Enter the beginning of the port range in the **Start Port** field. Enter the end of the port range in the **End Port** field.
4. Click **Save**.
5. To restart Avaya Aura® MS and to apply the port changes, click **Confirm**.

Changing media server component port assignments

About this task

To offer media services, the software components of Avaya Aura® MS require network ports.

Perform the following procedure to change the port a component uses to avoid conflicts with other software port requirements on the server.

Procedure

1. Navigate to **EM** > **System Configuration** > **Network Settings** > **Advanced Settings** > **Port Assignments**.
2. Enter a new port in the **Value** field.
3. Click **Save**.
4. Click **Confirm**.
5. Restart Avaya Aura® MS for the changes to take effect. Navigate to **EM** > **System Status** > **Element Status** and click **Restart**.
6. Click **Confirm**.

Changing the EM server ports

About this task

Use the following procedure to reassign the ports that Avaya Aura® MS EM uses.

Important:

Avaya also provides appliance versions of Avaya Aura® MS. Do not use this procedure when you are working with Avaya Aura® MS as a physical or virtual appliance. For appliance installations, see *Deploying and Updating Avaya Aura® Media Server Appliance*.

Procedure

1. To change the default ports that Avaya Aura® MS EM uses, edit the HTTP and HTTPS connector port values in the following Linux® file:

   `installpath/ma/apache-tomcat/conf/server.xml`

Important:

The `redirectPort` value for the HTTP connector must match the `Connector port` of the HTTPS connector.

2. Restart the server.

SNMP Configuration

Avaya Aura® MS contains a bilingual SNMP agent that supports SNMPv1, SNMPv2c, and SNMPv3. The media server SNMP agent also acts as a proxy to the Operating System SNMP agent and supports the following RFC's:

RFC	Title
2741	Agent Extensibility (AgentX) Protocol Version 1 Note for TCP and Linux ports.
2742	Definitions of Managed Objects for Extensible SNMP Agents.
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP).
3413	Simple Network Management Protocol Applications.
3414	User Based Security Model (USM) for SNMPv3.
3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).
3416	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP).
3417	Transport Mappings for the Simple Network Management Protocol (SNMP). **Note:** UDP transport only.
3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP).
3584	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework.
3826	The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model.
3877	Alarm Management Information Base (MIB).
7630	HMAC-SHA-2 Authentication Protocols in the User-based Security Model (USM) for SNMPv3.

The Avaya Aura® Media Server 10.x MIB can be downloaded from support.avaya.com or PLDS using download publication ID MSR000000041. This download is a zip file that contains the AVMediaServer-MIB and the AVAYAGEN-MIB. The AVAYAGEN-MIB must be imported into the Network Management Station (NMS) before importing AVMediaServer-MIB

The following configuration is required before an NMS can issue SNMP requests to the media server:

- Define SNMP Users
- Enable the SNMP Agent and specify the SNMP Users that may issue SNMP requests to this device

This procedure is described in detail in the section called Configuring SNMP Agent.

The following configuration is required before an NMS can receive SNMP traps from the media server:

- Define SNMP Users
- Define SNMP Trap Destinations
- Define SNMP Routes
- Enable SNMP trap notifications for Alarms and/or Event logs.

This procedure is described in detail in section called Enabling SNMP Traps.

Note:

Avaya Aura® Media Server will send traps using Coordinated Universal Time (UTC) rather than local system time.

Important:

You can only update SNMP configuration on the Primary server. Configuration changes applied to the primary server will be replicated to all servers within the cluster.

SNMP Users

An SNMP user defines a user that may issue an SNMP request to the media server or the user associated with an SNMP trap generated by the media server. The SNMP user configuration defines the SNMP protocol version and security preferences for the user.

Adding a SNMP User

About this task

Perform the following procedure to add an SNMP user that is associated with an SNMP request or trap. The properties of the user are dependent on SNMP protocol version selected.

Refer to the following definitions of the SNMPv1/v2c User Properties for descriptions of each property:

Definitions for SNMPv1/v2c Users Properties	
Property	**Description**
Security name	SNMP community string. The security name must be unique and has a maximum length of 32 characters.
Description	A brief description of the user. The maximum length is 512 characters.
Version	Must select v1/v2c.
Access rights	Specifies if the users access rights, which may be read-only or read-write access.

Refer to the following definitions of the SNMPv3 User Properties for descriptions of each property:

Definitions for SNMPv3 Users Properties	
Property	**Description**
Security name	Security name assigned to this user. The security name must be unique and has a maximum length of 32 characters.
Description	A brief description of the user. The maximum length is 512 characters.
Version	Must select v3.
Access rights	Specifies if the users access rights, which may be read-only or read-write access.
Authentication Mode	Specifies the authentication mode (None, SHA or MD5) for this user. If the authentication mode is specified then the authentication password must be specified. **Note:** MD5 authentication is not supported when enabling FIPS.
Authentication Password	Specifies the authentication password if the mode is set to SHA or MD5. The maximum length is 128 characters.
Privacy Mode	Specifies the privacy mode (None, DES, AES 192, or AES 256 for this user. If a privacy mode is specified then the privacy password must be specified.
Privacy Password	Specifies the privacy password if the mode is set to DES, AES 192, or AES 256. The maximum length is 128 characters.

Before you begin

Ensure that you have a Network Management Station configured and user configuration is known so that the configuration on the media server is the same.

Procedure

1. On the Primary server navigate to **EM** > **System Configuration** > **Network Settings** > **SNMP** > **Users**.
2. Click **Add**.
3. Enter the name that is used to identify the user in the **Security Name** field.

4. Enter the description of the user in the **Description** field.
5. Select the protocol version associated with the user in the **Version** field.
6. Select the access rights of the user in the **Access Rights** field.
7. Configure authentication and privacy mode if v3 is selected for the **Version** field.
    a. (Optional) Select the authentication mode from the **Authentication Mode** field. If you choose to enable authentication mode, then enter the password for the authentication mode in the **Authentication Password** field. Re-enter the password in the **Confirm Password** field.
    b. (Optional) Select the privacy mode from the **Privacy Mode** field. If you choose to enable privacy mode, then enter the password for the privacy mode in the **Privacy Password** field. Re-enter the password in the **Confirm Password** field.
8. Click **Save**.

Next steps

You must restart all the media servers in the cluster to apply the changes. If you have other SNMP configuration changes required, then proceed with those changes before restarting the servers.

Editing a SNMP User

About this task

Perform the following procedure to edit an SNMP user.

Procedure

1. On the Primary server navigate to **EM** > **System Configuration** > **Network Settings** > **SNMP** > **Users**.
2. Select the user that you want to edit.
3. Click **Edit**.
4. On the Edit Users page edit the fields you want to modify.
5. Click **Save** on the Edit Users page.

Next steps

You must restart all the media servers in the cluster to apply the changes. If you have other SNMP configuration changes required, then proceed with those changes before restarting the servers.

Related links

Editing a SNMP Trap Destination on page 79
Editing a SNMP Trap Route on page 81
Deleting a SNMP Trap Route on page 81

Deleting a SNMP User

About this task

Perform the following procedure to delete an SNMP user.

Before you begin

Ensure there is no SNMP trap routes defined with the SNMP users that you want to delete.

Procedure

1. On the Primary server navigate to **EM** > **System Configuration** > **Network Settings** > **SNMP** > **Users**.
2. Select the users that you want to delete.
3. Click **Delete**.

Next steps

You must restart all the media servers in the cluster to apply the changes. If you have other SNMP configuration changes required, then proceed with those changes before restarting the servers.

SNMP Trap Destinations

An SNMP trap destination defines an entity that can receive a SNMP trap from the media server. The SNMP trap destination configuration describes the hostname or IPv4 address and port of the entity.

Adding a SNMP Trap Destination

About this task

Perform the following procedure to add an SNMP trap destination.

Refer to the following definitions of the new SNMP trap destination for descriptions of each property:

Definitions for SNMP Trap Destination Properties	
Destination Address	The hostname or the IPv4 address of the SNMP trap destination. The hostname needs to be resolvable by the media server and the maximum length is 64 characters.
Destination Port	The port that the media server will send the SNMP trap to and the default is 162. The range is 0 to 65535 and must match what is configured on the NMS.

Before you begin

Ensure that you have a Network Management Station configured and user configuration is known so that the configuration on the media server is the same.

Procedure

1. On the Primary server navigate to **EM** > **System Configuration** > **Network Settings** > **SNMP** > **Destinations**.
2. Click **Add**.
3. Enter the address of the NMS in the **Destination Address** field.
4. Enter the NMS port in the **Destination Port** field.

5. Click **Save**.

Next steps

Add a SNMP trap route

You must restart all the media servers in the cluster to apply the changes. If you have other SNMP configuration changes required, then proceed with those changes before restarting the servers.

Editing a SNMP Trap Destination

About this task

Perform the following procedure to edit an SNMP trap destination.

Procedure

1. On the Primary server navigate to **EM** > **System Configuration** > **Network Settings** > **SNMP** > **Destinations** > **Trap Destinations**.
2. Select the destination that you want to edit.
3. Click **Edit**.
4. On the Edit Trap Destination page, edit the fields you want to modify.
5. Click **Save**.

Next steps

You must restart all the media servers in the cluster to apply the changes. If you have other SNMP configuration changes required, then proceed with those changes before restarting the servers.

Related links

Editing a SNMP User on page 77
Editing a SNMP Trap Route on page 81
Deleting a SNMP Trap Route on page 81

Deleting a SNMP Trap Destination

About this task

Perform the following procedure to delete an SNMP trap destination.

Before you begin

Ensure there is no SNMP trap routes defined with the SNMP destination that you want to delete.

Procedure

1. On the Primary server navigate to **EM** > **System Configuration** > **Network Settings** > **SNMP** > **Users**.
2. On the Trap Destinations page, select the check box next to the destination that you want to delete.
3. Click **Delete**.

Next steps

You must restart all the media servers in the cluster to apply the changes. If you have other SNMP configuration changes required, then proceed with those changes prior to restarting the servers.

SNMP Trap Routes

An SNMP trap route defines the entity that the media server will send a trap and trap security attributes.

Adding a SNMP Trap Route

About this task

Refer to the following definitions for descriptions of each SNMP trap route property:

Definitions for SNMP Trap Route Properties	
Destination Address	A SNMP trap destination that was configured on the media server. The destination will be displayed as IPv4Adress:Port.
Trap Unlocked	Indicates if the trap route is locked or unlocked (default). If this is checked then the media server will send traps to this route. If this is unchecked then the media server will not send traps to this route.
Version	Version of the SNMP trap, which may be V1/V2c or V3.
User	SNMP user that defines the security attributes of the trap that is being sent.
Description	A brief description of the trap route and the maximum length is 512 characters.

Before you begin

Configure the SNMP users and trap destinations required to define this trap route.

Procedure

1. On the Primary server navigate to **EM** > **System Configuration** > **Network Settings** > **SNMP** > **Destinations**.
2. Click **Add**.
3. Select the destination of the SNMP trap in **Destination Address** field.
4. Select or clear the **Trap Unlocked** field.
5. Select the SNMP version in the **Version** field.
6. Select the SNMP user in the **User** field.
7. Enter the route description in the **Description** field.
8. Click **Save**.

Next steps

Enabling SNMP traps on page 82

You must restart all the media servers in the cluster to apply the changes. If you have other SNMP configuration changes required, then proceed with those changes before restarting the servers.

Editing a SNMP Trap Route

About this task

Perform the following procedure to edit an SNMP trap route.

Procedure

1. On the Primary server navigate to **EM** > **System Configuration** > **Network Settings** > **SNMP** > **Destinations** > **Trap Routes**.
2. Select the route that you want to edit.
3. Click **Edit**.
4. On the Edit Trap Route page edit the fields you want to modify.
5. Click **Save**.

Next steps

You must restart all the media servers in the cluster to apply the changes. If you have other SNMP configuration changes required, then proceed with those changes before restarting the servers.

Related links

Editing a SNMP Trap Destination on page 79
Editing a SNMP User on page 77
Deleting a SNMP Trap Route on page 81

Deleting a SNMP Trap Route

About this task

Perform the following procedure to delete an SNMP trap route.

Procedure

1. On the Primary server navigate to **EM** > **System Configuration** > **Network Settings** > **SNMP** > **Destinations** > **Trap Routes**.
2. Select the destination that you want to delete.
3. Click **Delete**.

Next steps

You must restart all the media servers in the cluster to apply the changes. If you have other SNMP configuration changes required, then proceed with those changes before restarting the servers.

Related links

Editing a SNMP Trap Destination on page 79
Editing a SNMP User on page 77
Editing a SNMP Trap Route on page 81

Enabling SNMP traps

About this task

Perform the following procedure to configure the media server to send SNMP traps to all configured SNMP trap routes.

Avaya Aura® MS uses the Simple Network Management Protocol (SNMP) protocol to provide logs and events which may need administrative attention to a central management system.

Avaya Aura® MS reports the SNMP traps to the management system when a corresponding event triggers. For example, Avaya Aura® MS reports an SNMP trap when an alarm is raised.

Before you begin

Define one or more SNMP users, one or more SNMP trap destinations, and one or more SNMP trap routes.

Procedure

1. On the Primary server navigate to **EM** > **System Configuration** > **Network Settings** > **SNMP** > **Destinations**.
2. **(Optional)** Select **SNMP Alarm Delivery Traps** to enable sending a SNMP trap whenever an alarm is raised or cleared.
3. **(Optional)** Select **SNMP Event Log Delivery Traps** to enable sending a SNMP trap whenever an event log is generated.

Related links

Adding a SNMP User on page 75
Adding a SNMP Trap Destination on page 78
Adding a SNMP Trap Route on page 80

Disabling SNMP traps

About this task

Perform the following procedure to configure the media server to not send SNMP traps to all configured SNMP trap routes.

Procedure

1. On the Primary server navigate to **EM** > **System Configuration** > **Network Settings** > **SNMP** > **Destinations**.
2. Uncheck the **SNMP Alarm Delivery Traps** field to disable sending a SNMP trap whenever an alarm is raised or cleared.
3. Uncheck the **SNMP Event Log Delivery Traps** field to disable sending a SNMP trap whenever an event log is generated.

Configuring SNMP Agent

About this task

The management system can raise a query for SNMP specific information. The SNMP Agent on Avaya Aura® MS receives these queries and sends a response back to the management system with the requested information.

All SNMP requests must be sent to the Avaya Aura® MS SNMP Agent. This SNMP agent processes all the media server specific SNMP requests. The Avaya Aura® MS SNMP Agent acts as a proxy for other SNMP requests. These requests are forwarded to the native SNMP agent of the operating system.

Perform the following procedure to configure Avaya Aura® MS SNMP Agent.

Before you begin

Add a SNMPv3 user if you wish to enable SNMPv3 in the agent

Add a SNMPv1/v2c user if you wish to enable SNMP v1/2c in the agent.

To add a SNMP user, see Adding a SNMP User on page 75.

Procedure

1. On the Primary server navigate to **EM** > **System Configuration** > **Network Settings** > **SNMP** > **Destinations**.
2. In the General Settings section:
   a. Select the **Agent Enabled** field to enable the media server SNMP agent. To disable the media server SNMP agent, clear the **Agent Enabled** field.
   b. Enter the system location in the **System Location** field.
   c. Enter the system contact in the **System Contact** field.
   d. Enter the system name in the **System Name** field.
3. (Optional) In the Version 3 section
   a. Select the **Enabled** field to enable SNMPv3 support in the media server SNMP agent. Clear this field to disable SNMPv3 support.
   b. (Optional) If SNMPv3 is enabled then you must select a user from the **User** field. This is the SNMP user that the media server SNMP agent will accept SNMPv3 requests from.
4. (Optional) In the Version 1/2c section
   a. Select the **Enabled** field to enable SNMPv1 and SNMPv2c support in the media server SNMP agent. Clear this field to disable SNMPv1 and SNMPv2c support.
   b. (Optional) If SNMPv3 is enabled then you must select a user from the **User** field. This is the SNMP user that the media server SNMP agent will accept SNMPv1 and SNMPv2c requests from.

Related links

Adding a SNMP User on page 75

Adding a SNMP Trap Destination on page 78
Adding a SNMP Trap Route on page 80

Configuring the Avaya Aura® MS SNMP agent when Net SNMP is installed after Avaya Aura® MS is installed

About this task

If you install Net-SNMP after the media server is installed, then you must manually reconfigure the system for proper SNMP processing. This procedure reconfigures the native SNMP of the operating system so that the Avaya Aura® MS can process SNMP requests. When configured, all SNMP requests are sent to the Avaya Aura® MS SNMP Agent. This SNMP agent processes all the media server specific SNMP requests. Avaya Aura® MS SNMP Agent acts as a proxy for other SNMP requests. These requests are forwarded to the native SNMP agent of the operating system.

Important:

Avaya also provides appliance versions of Avaya Aura® Media Server. Do not use this procedure when you are working with the Avaya Aura® Media Server as an appliance in the VMware® virtualized environment or as an appliance on Avaya Solutions Platform.

Procedure

Using a Linux® shell, enter the following command to reconfigure the SNMP agent:

```
snmpconf.sh -install
```

Next steps

Configure the Avaya Aura® MS SNMP agent.

Computer name and IP address modification

Perform the following procedures if you need to change the IP address or host name of an installed Avaya Aura® MS.

Note:

When the IP address or host name of a server changes, you might need to replace the TLS certificates on the system. For information about configuring TLS certificates, see Security configuration.

Related links

Security configuration on page 131

Changing the computer name on Linux®

About this task

Perform the following procedure if you need to change the host name of a Linux® based Avaya Aura® MS:

Important:

Avaya also provides appliance versions of Avaya Aura® MS. Do not use this procedure when you are working with Avaya Aura® MS as a physical or virtual appliance. For appliance installations, see *Deploying and Updating Avaya Aura® Media Server Appliance*.

Before you begin

Stop Avaya Aura® MS before changing the computer name.

Procedure

1. Edit the file `/etc/hosts`.
2. Update the host name wherever the host name appears in the file.
3. Save the file.
4. Edit the file `/etc/sysconfig/network`.
5. Update the host name wherever the host name appears in the file.
6. Save the file.
7. Using a Linux® shell, enter the following command to apply the host name change to the system:

   `hostname` *`newhostname`*

   Where *`newhostname`* is the new name for the server.
8. Restart the server to apply change system-wide.

Related links

Starting and stopping the media server on page 22

Changing the IP address on Linux®

About this task

To change the IP address of a Linux® based Avaya Aura® MS, perform the following procedure:

Important:

Avaya also provides appliance versions of Avaya Aura® MS. Do not use this document when you are working with Avaya Aura® MS as a physical or virtual appliance. For appliance installations, see *Deploying and Updating Avaya Aura® Media Server Appliance*.

Before you begin

Do not use this procedure to change the Service IP address of a High Availability configuration.

Do not use this procedure to change the IP address of an Avaya Aura® MS appliance.

Stop Avaya Aura® MS before changing the IP address.

Procedure

1. Using the local Linux® console shell, edit the file `/etc/hosts`.

   Update the IP Address wherever it appears in the file.

   Save the file.

2. Using the local Linux® console shell, enter the following command to the list of network interfaces:

   ```
   ifconfig
   ```

   Edit the required interface configuration file, for example

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

   Update the IP address wherever it appears in the file.

   Save the file.

3. Using the local Linux® console shell, enter the following commands to apply the IP Address change to the system:

   ```
   /etc/init.d/network stop
   ```

   ```
   /etc/init.d/network start
   ```

4. Login to EM using the new IP address in the URL for the EM login.
5. Navigate to **EM** > **System Configuration** > **Network Settings** > **IP Interface Assignment**.
6. IP Interface Assignment fields show errors, as a result of the IP address change. Select valid IP addresses from the drop-down menus for each field showing **Invalid**.
7. Click **Save**.
8. Click **Confirm**.
9. Restart the server to apply the change system-wide.
10. If this server is a member of a cluster or High Availability pair, then navigate to **EM** > **Cluster Configuration** > **Server Designation** on each server. Ensure that the IP address you just changed is updated on each server. For more information, see Cluster configuration.

    To change the High Availability Service IP address, see Changing the Service IP Address for a High Availability configuration.

11. If this is a Primary server of a master cluster, then replication clusters that point to the master cluster must be updated with the new address of this server. On the Primary node in each replication cluster, navigate to **EM** > **Cluster configuration** > **Replication Settings** > **Master Cluster Primary Node Address**.

Related links

Starting and stopping the media server on page 22
N+1 Load Sharing cluster configuration on page 32
Changing the Service IPv4 or IPv6 Addresses for a High Availability configuration on page 51

SIP configuration

Session Initiation Protocol (SIP) is a signaling protocol that is used to create, modify, and end media streams containing text messaging, voice, and video.

SIP provides a standard means to establish sessions, negotiate capabilities, invoke applications, and exchange data with Avaya Aura® MS. The SIP protocol is an application layer protocol designed to be independent of the underlying transport layer. Avaya Aura® MS supports SIP on Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Transport Layer Security (TLS).

Configuring SIP general settings

About this task

Perform the following procedure to change the SIP settings for your system:

Important:

Change only those settings that are required for the system. The default settings are sufficient for most systems.

Refer to the following definitions for descriptions of each SIP setting:

Definitions for SIP settings	
Setting	**Description**
Enable SIP UDP Transport	Select to allow the system to accept and request SIP over UDP.
Enable SIP TCP Transport	Select if you want the system to accept and request SIP over TCP.
Enable SIP TLS Transport	Select to allow the system to accept and request SIP over TLS.
Enable SIP TLS Mutual Authentication	Select to enable the mutual authentication option for SIP TLS.
Enable SIP TLS Host Name Verification	Select to enable certificate hostname verification.
Enforce SIP TLS in Secured Media Mode	Select to disable the non-TLS transport in secured media mode.
Always Approve SIP TLS Certificate	Select if you want the system to accept remote certificate over SIP TLS. The default is disabled.

Table continues…

Definitions for SIP settings	
Setting	**Description**
Always Use SIP Default outbound Proxy	Select this option to enable the system to route SIP requests that do not match the domain proxy configuration, through the default outbound proxy. This routing happens even if an IP address is specified in the host portion of the destination URI.
Enforce SIP Route Configuration	Select if outgoing route configuration is required. By default, the system raises an alarm if route configuration is missing. If outgoing route configuration is not required, clear the check box.
Trusted Node Access Only	Select to prevent traffic from nodes that are not trusted. If a default proxy is configured, the call is redirected with a 305 Use Proxy message. Otherwise, the call attempt is rejected with a 403 Forbidden message.
Always Process Requests for Media Server SIP Reports	Always process OPTIONS methods that request the media server information report or performance report, even if the system is locked or overloaded.
SIP Response Code When System/Application Locked	The SIP Response Code needed to restore service when the application is locked, out-of-service, or exceeds engineering limits. The default value is 503. The range is 400 to 699.
Session Audit Type	Select the preferred Long Call Method to use: Disable Audit, INFO Ping, re-INVITE, or UPDATE.
Session Audit Refresh Timer	The time period in seconds for sending a refresh request. The default is 1800 seconds. The range is 90 to 3600 seconds.
Session Expires Value (RFC4028)	The number of seconds before a call times out if the call is not successfully refreshed. The default is 1800 seconds. The range is 90 to 3600 seconds.
Minimum Session Interval (RFC4028 Min-SE)	The minimum value for the session interval that the application can accept. RFC4028 recommends a Min-SE value of 90 seconds. The default is 90 seconds. The range is 90 to 3600 seconds.
Session On Hold Teardown Delay (sec)	The number of seconds a session can remain on hold before the system ends the session. A value of 0 indicates the system will not end a session on hold. The default is 3600 seconds. The range is 0 to 100,000 seconds.
Answer Delay (rings)	The number of rings before an incoming SIP call is answered. You can configure the duration of a ring using the Ring Interval engineering parameter. A value of 0 indicates an immediate answer. The default value is 1 ring. The range is 0 to 10 rings.

Table continues…

Definitions for SIP settings	
Setting	**Description**
Hide SIP User-Agent Header	Select to prevent the User-Agent header from being included in SIP messaging.
SIP Hold Before Refer	The call is placed on Hold prior to REFER.
Enable SIP UPDATE method	Select to allow session participants to modify the characteristics of the multimedia session through re-INVITE messages or UPDATE messages. Re-INVITE and UPDATE messages initiate session changes, such as hold and retrieve, codec changes, and adding or dropping media.
Enforce SIPS for security enforced calls	Select to require sips: in the URI to negotiate to use SRTP for media transport. Clear to allow SRTP with both sip: and sips: URIs.
Use SIPS for best effort calls	Select to use sips: in the URI for outgoing best-effort offers originated from the Avaya Aura® MS. Clear to use sip: in the URI for outgoing best-effort offers.
Require SIPS for Best Effort Calls	Select to include capability negotiation (crypto) offers when sips: is used. Do not include capability negotiation (crypto) offers when sip: is used. Clear to include capability negotiation (crypto) for both sip: and sips: URIs.
Use Contact Address For SIP REFER With Replaces	Select to replace the Refer-To address with the contact address for merged calls using REFER with replaces.
Enable GSID Handling	Select to support SIP Global Session Identifier (GSLID) processing.
Use GSID as GSLID	Select to use the SIP Global Session Identifier (GSLID) as the Global Session Logging Identifier (GSLID) is Avaya Aura® MS logging and tracing.

Perform the following procedure to change the SIP settings for the system:

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **SIP** > **General Settings**.
2. Modify the settings listed in the categories **Transport Settings**, **Routing** , **Access Control**, **Session Audit**, and **SIP Settings**.
3. Click **Save**.

Note:

For some of the changes to take effect, restart Avaya Aura® MS.

Adding SIP domains

About this task

A network provisioned SIP domain must be added only if:

- Avaya Aura® MS needs to send SIP Register to the network
- Avaya Aura® MS is connected to more than one SIP domain that is controlled by different proxies. Calls can also originate from Avaya Aura® MS.

Avaya Aura® MS has an internal default domain called the wildcard domain represented by an asterisk (*). The system uses the default wildcard domain if no matching domain is found.

For most cases, SIP domain configuration is not required because Avaya Aura® MS is connected to one or more proxies or call servers that are capable of routing calls to various domains. In such cases, the default wildcard domain is sufficient.

Perform the following procedure to add a SIP domain for your system if the wildcard domain is not sufficient:

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **SIP** > **Domains and Accounts**.
2. In the **Domains** section, click **Add...** to add a SIP domain.
3. In the Add SIP Domain page, enter the name of the SIP domain in the **Name** field.
4. Click **Save**.

Adding SIP accounts

About this task

Configure SIP accounts only if you require the use of a registrar server. You use SIP accounts to register your applications in the SIP network. Avaya Aura® MS registers all accounts with the registrar servers. You do not require SIP account configuration if Avaya Aura® MS is provisioned in your network as a trusted entity.

Perform the following procedure to add a SIP account for your system:

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **SIP** > **Domains and Accounts**.
2. In the **Accounts** area, click **Add** to add a SIP account.
3. On the **Add SIP Account** page, enter the name of the SIP account in the **Name** field.
4. Enter the password for the SIP account in the **Password** field.
5. Re-enter the password in the **Confirm Password** field.
6. Select the SIP domain to associate with the account from the **Domain** list.
7. Select the cluster node to associate with the account from the **Cluster Node** list.

8. Click **Save**.

Configuring SIP trusted nodes

About this task

Avaya Aura® MS only processes SIP traffic from trusted nodes, for example, proxies. Avaya Aura® MS rejects requests from nodes that are not trusted. All proxy servers and registrar servers that interact with Avaya Aura® MS must be trusted nodes.

Perform the following procedure to configure trusted nodes for each proxy server and registrar server:

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **SIP** > **Nodes and Routes**.
2. In the Trusted Nodes section, click **Add** to add a new SIP trusted node.
3. On the Add SIP Trusted Node page, enter the address of the SIP node in the **Host or Server Address** field.
4. Click **Save**.

Configuring SIP routes

About this task

Configure SIP routes for all proxy servers and registrar servers. SIP routes define all proxy and registrar servers with which the Avaya Aura® MS node communicates.

You can configure up to 32 routes for each domain.

The system selects the routes based on the matching domain. If no domain is configured, the system uses the default wild card domain represented by an asterisk (*).

The system uses the **Priority** and **Weight** of a route for outbound call load balancing. If multiple routes are configured for a domain, the calls are attempted on the highest priority routes. If the remote server is not responsive or is out of service, the attempted calls can failover to lower priority routes. For routes which have the same priority, the system distributes the load based on the route weight.

Refer to the following parameter definitions for the descriptions of each SIP route setting:

Definitions for SIP route settings	
Setting	**Description**
Enabled	Select to enable or disable a SIP route. Typically, routes are enabled. However, a route can be disabled to remove the route temporarily without reconfiguring the system.

Table continues…

Definitions for SIP route settings	
Setting	**Description**
Domain	The name of the domain to which you are adding the route. The SIP route is associated with the domain.
IM Proxy	If there are multiple proxy routes in the domain, route IMs to the route which is enabled.
Priority	The priority value for the route. The default value is 0. The range is from 0 to 65535 with the lowest value having the highest priority. The highest priority routes, which have lower values, are selected first.
Proxy	Select to assign a proxy server role to the route. A SIP proxy server accepts Avaya Aura® MS requests and uses the SIP registrar server to obtain recipient addressing information.
Registrar	Select to assign a registrar server role to the route. A SIP registrar server is a database that contains the location of all user agents within a domain.
Remote Port	The remote port from which the route accepts SIP requests. The default port is 5060.
Transport	Select the appropriate SIP transport (UDP, TCP, or TLS). When you select the transport type of TLS, ensure that a certificate is configured for the SIP-TLS service profile.
Trusted Node	The trusted nodes associated with the route.
Weight	Weight is used to select routes within the same priority level. The default value is 10. The range is 0 to 65535.

Before you begin

You must have configured a SIP trusted node before adding any SIP routes.

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **SIP** > **Nodes and Routes**.
2. In the **Routes** area, click **Add...** to add a new SIP route.
3. On the **Add SIP Route** page, in the **General** section, select **Enabled** to enable the route.
4. From the **Domain** list, select the desired domain.
5. From the **Trusted Node** list, select the trusted node to associate with the route.
6. From the **Transport** list, select the transport protocol that the route uses.

Important:

If a transport type of TLS is selected, ensure that a certificate is configured for the SIP TLS service profile.

7. In the **Remote Port** field, enter the port number of the remote port.
8. In the **Priority** field, set the priority of the route by entering a value.
9. In the **Weight** field, set the weight of the route by entering a value.
10. In the **Roles** area, select whether the route is associated with the **Proxy** server, the **Registrar** server, or both by selecting **Proxy** and **Registrar**.
11. Select **IM Proxy** to route instant messages only to the route that is enabled if there are multiple proxy routes in the domain.
12. Click **Save**.
13. Restart Avaya Aura® MS for the changes to take effect. Navigate to **EM** > **System Status** > **Element Status** and click **Restart**.
14. Click **Confirm**.

Configuring SIP route properties

About this task

Refer to the following parameter definitions for descriptions of each property of the SIP route:

Definitions for SIP route properties		
Property	**Description**	
SIP Route Type	The type of route that indicates if product specific processing is required. The options include:	
	Standard SIP	This route is fully compliant and requires no special handling. You can select this option for most deployments. This is the default value.
	CS1K GW	Direct Communication Server 1000 mode.
	CS1K SRS	Communication Server 1000 configured with SIP Redirect Server (SRS).
	CS1K SPS Home	Communication Server 1000 configured with a SIP Proxy Server (SPS).
	CS1K SPS Home Redirect	Communication Server 1000 configured with SIP Proxy Server (SPS).

Table continues…

Definitions for SIP route properties		
Property	**Description**	
	CS1K SPS Redirect	Communication Server 1000 configured with SIP Proxy Server (SPS).
SIP Server Poll Timer	Interval, in milliseconds, that the route is polled for status. The mechanism used to determine the status is based on the SIP Server Keepalive configuration setting. The default value is 30,000 milliseconds. The range is 30,000 to 600,000 milliseconds.	
Server Keep Alive	The mechanism used by Avaya Aura® MS to determine the status of the route. The options include:	
	Disabled	Route status monitoring is disabled.
	Keep Alive Using OPTIONS	Route status is monitored using the SIP OPTIONS message. The route status updates based on the OPTIONS response. The OPTIONS response includes 200 (Active), 503 (Inactive), 504/No Response (Inactive or Down), and Other (Online - applies to MCS).

Before you begin

You must have configured a SIP route.

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **SIP** > **Nodes and Routes**.
2. In **Routes** area, select the check box next to **Route** field that you want to edit.
3. Click **Edit**.
4. On the **Edit SIP Route** page, scroll down to the **Properties** section to make any required changes.
5. From the **Server Keepalive** list, select to enable route status monitoring.
6. From the **SIP Route Type** list, select the type of route.
7. In the **SIP Server Poll Timer** field, enter the polling interval for route status, in milliseconds.
8. Click **Save**.

Editing a SIP domain or a SIP account

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **SIP** > **Domains and Accounts**.
2. On the **SIP Domains and Accounts** page, select the check box next to the domain or account that you want to edit.
3. Click **Edit**.
4. Edit the properties of the domain or account.
5. Click **Save**.

Changing the SIP account password

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **SIP** > **Domains and Accounts**.
2. On the SIP Domains and Accounts page, select the check box next to the account for which you want to change the password.
3. Click **Edit**.
4. On the Edit SIP Account page, click **Change Password**.
5. In the **Password** field, enter the new password.
6. In the **Confirm Password** field, re-enter the new password.
7. Click **Continue**.
8. Click **Save**.

Deleting a SIP domain or a SIP account

Before you begin

If a SIP domain has associated accounts, you must delete the SIP accounts before you delete the domain.

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **SIP** > **Domains and Accounts**.
2. On the **SIP Domains and Accounts** page, select the domain or account that you want to delete.
3. Click **Delete**.

Editing a SIP trusted node or a SIP route

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **SIP** > **Nodes and Routes**.
2. On the **SIP Nodes and Routes** page, select the trusted node or route that you want to edit.
3. Click **Edit**.
4. Edit the properties of the trusted node or route.
5. Click **Save**.

Deleting a SIP trusted node or a SIP route

Before you begin

If a SIP trusted node has routes associated with the node, you must delete the routes before you delete the node.

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **SIP** > **Nodes and Routes**.
2. On the **SIP Nodes and Routes** page, select the trusted node or route that you want to delete.
3. Click **Delete**.

MRCP configuration

Avaya Aura® MS uses MRCP servers to support speech recognition and to stream Text-To-Speech (TTS) as Avaya Aura® MS is synthesized in real-time.

To configure MRCP, define one or more MRCP servers and identify the resources on each server. Additionally, define one or more MRCP pools and add the MRCP servers for each pool.

In addition to the built-in Nuance and Loquendo support within Avaya Aura® MS, you can add custom MRCP vendors to allow for additional speech resources.

Configuring an MRCP general settings

About this task

Refer to the following definitions for descriptions of each property of the MRCP General Settings:

Definitions for MRCP general properties	
Property	**Description**
Maximum MRCP Channels	The maximum number of MRCP channels or sessions for each node that can be allocated by the server. Avaya Aura® MS uses this value to determine the maximum MRCP channels available on an MRCP server. This value is also used to initialize the MRCP stack. The Maximum MRCP Channels field is not a keycoded value. The default value is 512. The range is 0 to 2000.
Retry Limit	The number of retry attempts when a resource allocation fails. The system attempts to connect to the server with the smallest load first. It is followed by the server with the second smallest load, and then the server with the third smallest load. The default is 2 retry attempts. The range is 0 to 2.
MRCP Resource Ping Interval	The number of seconds between successive test allocations of configured MRCP resources. This value is used by Avaya Aura® MS to monitor the status of the MRCP servers. A value of 0 disables test allocations. The default value is 300 seconds. The range is 0 to 31536000 seconds.
Recognition Timeout	The maximum duration, in milliseconds, that a recognition session is active before Avaya Aura® MS terminates the session and generates a resource fault. The default value is 600000 milliseconds. The range is 0 to 31536000 milliseconds.
MRCP Transaction Timeout	The maximum duration, in milliseconds, that an MRCP transaction can last before being terminated and a resource fault generated. The default value is 10000 milliseconds. The range is 0 to 31536000 milliseconds.
MRCPv2 Control Channel Security	Override options for the security settings for the MRCPv2 control channel. Under normal conditions use the **Default** option.
MRCPv2 Media Security	Override options for the security settings for the MRCPv2 media channel. Under normal conditions use the **Default** option.

Perform the following procedure to change MRCP General Settings:

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **MRCP** > **General Settings**.
2. In the **Maximum MRCP Channels** field, enter a value for the maximum number of MRCP channels that can be allocated.

3. In the **Retry Limit** field, enter the number of allocation retries before an allocation attempt fails.
4. In the **MRCP Resource Ping Interval** field, enter the number of seconds between successive test allocations of configured MRCP resources.

   A value of 0 disables test allocations.
5. In the **Recognition Timeout** field, enter the maximum duration (in milliseconds), that a recognition session is active before Avaya Aura® MS ends it. A resource fault is generated when the system ends the session.
6. In the **MRCP Transaction Timeout** field, enter the maximum duration (in milliseconds) that an MRCP transaction can last before being ended. A resource fault is generated when the system ends the transaction.
7. **(Optional)** Override the security settings for the MRCPv2 control channel by selecting **Enforced** or **Disabled** in the **MRCPv2 Control Channel Security** drop-down menu. Under normal conditions use the **Default** option.
8. **(Optional)** Override the security settings for the MRCPv2 media channel by selecting **Enforced** or **Disabled** in the **MRCPv2 Media Security** drop-down menu. Under normal conditions use the **Default** option.
9. Click **Save**.
10. Restart Avaya Aura® MS for the changes to take effect.

Adding an MRCP server

About this task

Add an MRCP server to provide speech capabilities to the network of Avaya Aura® MS nodes. MRCP servers can be grouped into pools and shared across one or more Avaya Aura® MS systems in the network.

Refer to the following definitions of the new MRCP Server Properties for descriptions of each property:

Definitions for MRCP server properties	
Property	**Description**
Server Name	The name used to identify this MRCP server. The maximum length is 128 characters.
Server description	A brief description of the server. The maximum length is 512 characters.
Server address	The IP address of the MRCP server. The maximum length is 64 characters.
Port	The port from which the server receives requests. The default port is based on the settings of the selected vendor. The range is 0 to 65535.
MRCP Version	The MRCP protocol version Avaya Aura® MS should use.

Table continues…

Definitions for MRCP server properties	
Property	**Description**
Transport Protocol	The transport protocol Avaya Aura® MS should use with MRCP.
Vendor	Select the appropriate MRCP vendor identifier such as Nuance, Loquendo or those added on the Custom MRCP vendors page. The default is Nuance.
Codec	Select the appropriate audio codec (PCMU, PCMA or L16). The default value is based on the settings of the selected vendor.
State	The operational state: • Unlocked: The server is online and available for allocation. This is the default. • Locked: The server is offline and unavailable for allocation.
Add to Default Pool	Select the check box to add the server to the default pool. This check box is only available when adding an MRCP Server. If no default pool exists, the system creates one pool based on the server configuration. The default pool uses the following names: speechrecog-mrcp.default or speechsynth-mrcp.default. However, if there are no default pools and the pool names (speechrecog-mrcp.default or speechsynth-mrcp.default) already exist, the operation fails. The Add to Default Pool operation can also fail, if the server and default pool attributes do not match.

Important:

An MRCP server cannot have more than two MRCP resources (LVR and TTS). The **Add** button is disabled after both the MRCP resources exist for a server.

If you use the host name for the server address in the following procedure, you must enable DNS on the network.

Perform the following procedure to an MRCP server to provide speech capabilities to the network of Avaya Aura® MS nodes:

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **MRCP** > **Servers**.
2. On the **Servers** page, click **Add…**
3. Enter the name that is used to identify the MRCP server in the **Server Name** field.
4. Enter a description of the MRCP server in the **Server description** field.
5. Enter the host name or server address of the MRCP server, in the **Server address** field.

   Important:

   You must enable the DNS on the network if the host name is used.
6. Enter the port number of the MRCP server in the **Port** field.
7. Select the required version of MRCP from the **MRCP Version** drop-down menu.

8. Select the required transport protocol from the **Transport Protocol** drop-down menu.
9. From the **Vendor** list, select the vendor.
10. From the **Codec** list, select the audio codec type.
11. From the **State** list, select the appropriate initial operational state, either **Locked** or **Unlocked**.

    The default value is **Unlocked**.
12. If you want to add the server to the default pool, select **Add to Default Pool**.
13. Click **Save**.

Adding MRCP server resources

About this task

Each MRCP server can have a TTS resource, LVR resource, or both associated with the server.

Refer to the following definitions for descriptions of each property of the MRCP server resource:

Definitions for MRCP server resource properties	
Property	**Description**
Server Name	The name of the MRCP server.
Vendor name	The name of the current vendor such as Nuance, Loquendo or those added on the Custom MRCP vendors page.
Type	Select the appropriate resource capabilities (LVR or TTS) supported by MRCP. The default value is based on the settings of the selected vendor.
URL Suffix	The URL suffix used to identify the resource. This feature is enabled only when the Type is LVR or TTS. For Nuance: • LVR —media/speechrecognizer. This is the default. • TTS — media/speechsynthesizer For Loquendo: • LVR — media/recognizer • TTS — media/synthesizer The default value is based on the settings of the selected vendor.
Weight	The weighted value of the server. This value is used for distributing server resources within the pool. The default value is 1. The range is 0 to 65535.

Table continues…

Definitions for MRCP server resource properties	
Property	**Description**
Maximum Sessions	The maximum number of sessions to be allocated by one IVR media processor (IVRMP) from the defined resource. The default value is 1 session. The range is from 0 to 65535.
Languages	The language options available on the MRCP server. The default value is based on the settings of the selected vendor.

Note:

An MRCP server cannot have more than two MRCP resources (LVR and TTS). The **Add…** button is disabled after both resources exist for a server.

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **MRCP** > **Servers**.
2. On the **Servers** page, select the check box next to the MRCP server to which you want to add server resources.
3. Click **Edit…**
4. On the **Edit MRCP Server** page, in **Server Resources**, click **Add…**
5. In the **Server Name** and **Vendor** field, verify the server and vendor names.
6. From the **Type** list, select the resource capabilities supported by MRCP.
7. In the **URL Suffix** field, enter the suffix to identify the resource.

   The URL suffix must match the configuration on the speech server.
8. In the **Weight** field, enter the server weight used to distribute server resources within a pool.
9. In the **Maximum Sessions** field, enter the maximum number of sessions for this server.
10. Add the required languages in one of two ways:
    - In the **Select a Language** section, select the required language from the **Languages** drop-down menu. Click **Add** to add the selected language to the list of supported languages.
    - Click **Add New**. In the text field that the system displays, type the required language.
11. Click **Continue**.
12. On the **Edit MRCP Server** page, click **Save**.

Adding an MRCP pool

About this task

Each Avaya Aura® MS can define one or more MRCP pools from which speech resources are allocated. Each pool contains one or more servers. MRCP servers within a pool must have the same attributes. Servers can be added or removed from the pool.

Important:

All servers in the same pool must be from the same vendor and resource type,TTS or LVR.

Important:

The servers must share at least one common language. Ensure that all servers in the pool support the language set you specify.

Refer to the following definitions for descriptions of each property of the MRCP Pool:

Definitions for MRCP pool properties	
Property	**Description**
Available	Select to make the pool available for servers.
Default pool	Select to make this pool the default pool for speech capability on the network of Avaya Aura® MS nodes.
Language	The speech capability of the network of Avaya Aura® MS nodes. Select a language from the available languages. The servers must share at least one common language. When you specify languages supported by a pool, the language set must be supported by all servers in the pool. The language list displayed is based on the MRCP server configuration, more specifically, the vendor ID and the resource type). If no servers are assigned to the pool, the language field is populated with all the languages that are common among the servers being assigned.
Pool description	A brief description of the pool. The description can be up to 512 characters.
Pool name	The name used to identify this pool. The name can be up to 128 characters. An MRCP server can be assigned to many different pools.
Pool type	The type of pool (LVR or TTS).
Pool weight	A weighted value used to determine how pool resources are prioritized. The default value of 1. The range is 0 to 65535.
Vendor name	The name of the current vendor, Nuance, Loquendo or those added on Custom MRCP vendors.

Perform the following procedure to add an MRCP pool:

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **MRCP** > **Pools**.
2. On the **Pools** page, click **Add…**
3. In the **Pool name** field, enter a name to identify the pool.
4. In the **Pool description** field, enter a description of the pool.
5. From the **Pool type** list, select the MRCP server type.
6. From the **Vendor name** list, select the vendor.
7. In the **Pool weight** field, enter the required weight of the pool.
8. From the **Language** list, select a language.
9. Select **Default pool** to set the pool as the default pool.
10. To make the pool available, select **Available**.
11. Click **Save**.

Adding a server to an MRCP pool

About this task

You can assign an MRCP server to multiple pools.

Perform the following procedure to add an MRCP server to an existing MRCP server pool:

Before you begin

Define an MRCP server pool.

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **MRCP** > **Pools**.
2. On the **Pools** page, select the check box next to the pool receiving the servers.
3. Click **Edit**
4. In the **Assign servers** section, select a server from the **Available** list.
5. Click **Add** to move the server to the **Assign to this pool** list.

   Important:

   The status of the MRCP servers assigned to the pool is displayed in the **Assign to this pool** list, next to the server address.
6. Click **Save**.

Adding custom MRCP vendors

About this task

Perform the following procedure to add custom MRCP vendors for additional speech resources:

Important:

You can only add, edit, or delete custom MRCP vendors on a Primary server.

Procedure

1. Gain access to the EM for the Primary server and navigate to **EM** > **System Configuration** > **Signaling Protocols** > **MRCP** > **Custom Vendors**.
2. On the Custom Vendors page, click **Add**
3. In the **Vendor Name** field, enter the name of the new vendor.
4. Select the desired **Default Codec** from the list.
5. In the **Default Port** field, enter the default port number associated with the MRCP resource.
6. In the **Associated Caps** heading, click **Add**

   Important:

   Only one LVR and one TTS capability can be created for each vendor.
7. On the **Add Cap** page, select the resource type from the **Cap** (capability) list.
8. In the **Default Suffix** field, enter the suffix that identifies the resource type.
9. In **Languages**, select the required languages from the **Available Languages** list.
10. Click **Add** or **Add All** to move the supported language(s) to the **Selected Languages** list.
11. Click **Save** on the **Add Cap** page.
12. Click **Save** on the Add Custom MRCP Vendors page.

Editing custom MRCP vendors

About this task

Perform the following procedure to edit custom MRCP vendors:

Important:

You can only add, edit, and delete Custom MRCP vendors on a Primary server.

Procedure

1. Gain access to the EM for the Primary server and navigate to **EM** > **System Configuration** > **Signaling Protocols** > **MRCP** > **Custom Vendors**.
2. On the **Custom Vendors** page, select the check box next to the MRCP vendor resource that you want to edit.

   Important:

   Click on the alias of the vendor to view the cap settings. The settings are shown at the bottom of the page.

3. Click **Edit**.
4. On the **Edit Custom Vendors** page, edit the **Default Codec** and **Default Port**.
5. In the **Associated Caps** section, select the check box next to the cap that you want to edit.
6. Click **Edit**.
7. On the **Edit Cap** page, edit the **Cap**, **Default Suffix**, and **Selected Languages**.
8. Click **Save** on the **Edit Cap** page.
9. Click **Save** on the **Edit Custom MRCP Vendor** page.

Deleting custom MRCP vendors

About this task

Perform the following procedure to delete custom MRCP vendors:

Important:

You can only add, edit, and delete Custom MRCP vendors on a Primary server.

Procedure

1. Gain access to the EM for the Primary server and navigate to **EM** > **System Configuration** > **Signaling Protocols** > **MRCP** > **Custom Vendors**.
2. On the **Custom Vendors** page, select the check box next to the MRCP vendor resource that you want to delete.

   Important:

   If you delete a custom MRCP vendor, it deletes all MRCP servers containing the selected vendor.
3. Click **Delete**.
4. Click **Confirm** to acknowledge the deletion of the MRCP vendor resource.

Editing an MRCP server or server resources

About this task

Perform the following procedure to edit an MRCP server or server resources.

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **MRCP** > **Servers**.

   Important:

   To view the resources assigned to an MRCP server in the lower pane, click the corresponding server in the **Server Name** column.
2. On the **Servers** page, select the check box next to the MRCP server that you want to edit.

3. Click **Edit…**
4. Edit the **General** MRCP server properties.
5. To edit a server resource, select the check box next to the server resource to be edited and click **Edit…**
6. Click **Save**.

Deleting an MRCP server

About this task

Perform the following procedure to remove an MRCP server:

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **MRCP** > **Servers**.
2. On the **Servers** page, select the check box next to the MRCP server.
3. Click **Delete**.
4. Click **Confirm** to acknowledge the deletion of the MRCP server.

Deleting MRCP server resources

About this task

Perform the following procedure to remove the server resources for an MRCP server.

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **MRCP** > **Servers**.
2. On the Servers page, select MRCP server to modify.
3. Click **Edit**.
4. Under **Server Resources** on the **Edit MRCP Server** page, select the server resources you want to delete.
5. Click **Delete**.
6. On the Edit MRCP Server page, click **Save**.

Editing an MRCP pool

About this task

Perform the following procedure to edit an MRCP pool:

Important:

Changing the Pool Type or Vendor Name removes all assigned MRCP servers. The system displays servers which have attributes matching the pool's current configuration in the **Available** list.

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **MRCP** > **Pools**.

   Tip:

   The system displays the status of the MRCP servers assigned to each pool in parenthesis in the **Server names** column.

2. On the Pools page, select the MRCP pool or the server resource that you want to edit.
3. Click **Edit**.
4. Edit the **MRCP pool** fields.

   Tip:

   The system displays the status of the MRCP servers assigned to the pool in the **Assign to this pool** list.

5. Click **Save**.

Changing status of MRCP pools

About this task

Perform the following procedure to change the availability status of single or multiple MRCP pools:

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **MRCP** > **Pools**.
2. On the Pools page, select the check box next to one or more MRCP pools.
3. From the **More Actions** list, select the availability status for the selected pools.
4. Click **Confirm** to acknowledge the status change.

Deleting an MRCP pool

About this task

Perform the following procedure to delete an MRCP pool:

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **MRCP** > **Pools**.
2. On the Pools page, select the check box next to the MRCP pool or the server resource that you want to edit.
3. Click **Delete**.
4. Click **Confirm** to acknowledge the deletion of the MRCP pool.

Removing MRCP servers from a pool

About this task

Perform the following procedure to remove an MRCP server from an MRCP pool:

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **MRCP** > **Pools**.
2. On the Pools page, select the check box next to the MRCP pool that contains the server that you want to remove.
3. Click **Edit**.
4. In the **Assign servers** section, select the server you want to remove from the **Assign to this pool** list.
5. Click **Remove** to move the server back to the **Available** list.
6. Click **Save**.

REST configuration

Avaya Aura® MS supports Representational State Transfer (REST) for building scalable web services. Avaya Aura® MS Web User Agent component publishes a RESTful control interface that applications can use instead of SIP for media service access.

Enabling secure REST requests

About this task

Use the following procedure to configure secure TLS transport and authentication for REST services:

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **REST** > **General Settings**.
2. To enable TLS for REST services, select the **Enable TLS Transport** check box.
3. **(Optional)** To enable two-way authentication for an extra level of security, select the **Enable TLS Mutual Authentication** check box.
4. **(Optional)** To use plaintext usernames and passwords, select **Basic Authentication**. Alternatively, to include an authentication realm and encrypt the credentials before sending them over the network, select **Digest Authentication**.
    a. Enter the required username and password credentials in the **Authentication Username** and **Authentication Password** fields.

b. If you selected **Digest Authentication**, then enter the name of the required authentication realm in the **Authentication Realm** field.

5. Click **Save**.

Note:

Changes to the transport settings require a media server restart to take effect.

Disabling secure REST requests

About this task

Use the following procedure to disable the TLS transport and authentication for REST services:

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **REST** > **General Settings**.
2. To disable TLS for REST services, clear **Enable TLS Transport**.
3. **(Optional)** To use unencrypted authentication, clear **Digest Authentication**.
4. Click **Save**.

Note:

Changes to the transport settings require a media server restart to take effect.

Media processing configuration

Avaya Aura® MS supports text, audio, and video for most multimedia processing features. The system can stream fully synchronized real-time audio and video using a variety of codecs and formats.

Configuring QoS monitoring settings

About this task

Avaya Aura® MS uses the QualityRating to indicate audio quality for a session.

The QualityRating (range 0-100) is updated periodically for each active session. The rating is based on the negotiated codec in use and factors in the quality of the packet stream as it is transported over the network. Each codec has an individual maximum quality value. Wideband codecs have a higher maximum QualityRating value than narrowband codecs.

See Quality of Service (QOS) Troubleshooting on page 252 for further information on sources of QOS issues.

QualityRating Values	
Codec	**Maximum QualityRating**
G711	93
G722	100
G722.1	100
G726–32	86
G729	82
OPUS	100

Refer to the following definitions for descriptions of each QoS monitoring property:

Definitions for QoS monitoring properties	
Property	**Description**
QOS Monitoring	Select to enable Quality of Service monitoring.
QOS Critical Event Log Interval (sec)	The minimum time period between logs of critical QOS events, measured in seconds. Default value is 60 seconds.
Session SDR Report Interval (sec)	The minimum time between SDR statistics containing QOS information, measured in seconds. Default value is 60 seconds.
QualityRating Threshold for QOS Critical State	The QualityRating value (range 0-100) at which to set session to QOS critical state. Default value is 70.
QualityRating Threshold for QOS Warning State	The QualityRating value (range 0-100) at which to set session to QOS warning state. Default value is 80.
Number of Sessions in QOS Critical State before raising Alarm	Number of sessions in QOS critical state before critical alarm is raised. Range is 0-1000. Default value is 1.
Number of Sessions in QOS Warning State before raising Alarm	Number of Sessions in QOS Warning State before raising Alarm. Range is 0-1000. Default value is 5.

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **General Settings** > **QoS Monitoring**.
2. Change the properties using the Definitions for QoS Monitoring Properties table as an aid.
3. Click **Save**.

Note:

Some of the changes require a restart to take effect.

Related links

Quality of Service (QoS) Troubleshooting on page 252

Configuring QoS streaming settings

About this task

Avaya Aura® MS provides prioritized transport for media packets by implementing Differentiated Services Control Point (DSCP) marking as described in RFC2474, RFC3260, and RFC4594. You can configure DSCP settings separately for audio and video streams. Audio packets must receive an Expedited Forwarding (EF) marking to ensure minimum latency in the network. Video packets must receive an Assured Forwarding (AF) marking to provide network transit suitable for real-time video while still giving priority to audio packets.

Refer to the following definitions for descriptions of each QoS streaming property:

Definitions for QoS streaming properties	
Property	**Description**
Audio DSCP	DSCP marking value for audio. The default value is 46 (Expedited Forwarding). The range is 0 to 63.
Video DSCP	DSCP marking value for video. The default value is 34(Assured Forwarding). The range is 0 to 63.

Perform the following procedure to configure QoS streaming:

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **General Settings** > **QoS Streaming**.
2. Alter the properties using the Definitions for QoS Streaming Properties table as an aid.
3. Click **Save**.

Configuring silence suppression

About this task

Silence suppression eliminates background noise transmission over the network when a user is not speaking. Instead of transmitting actual background audio noise in the audio stream, comfort noise indications are transmitted (see RFC3389). This reduces the network bandwidth used by the user session.

Refer to the following definitions for descriptions of each QoS silence suppression property:

Definitions for silence suppression properties	
Property	**Description**
Silence Suppression CN Level	The silence suppression comfort noise (CN) level in dB as defined by RFC3389. The default is minus (–) 127 dB. The range is minus (–) 127 dB to 0 dB.
Silence Suppression Interval (ms)	The number of milliseconds between successive 3389 RTP SS packets. The default is Disabled. The range is 0 to 2147483647 milliseconds.

Table continues…

Definitions for silence suppression properties	
Property	**Description**
Silence Suppression Threshold (ms)	The number of milliseconds before transmitted RTP silence is suppressed with 3389 SS packets. The default is 20 milliseconds. The range is 0 to 2147483647 milliseconds.

Perform the following procedure to configure the silence suppression options:

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **Advanced Settings** > **Silence Suppression**.
2. Alter the properties using the Definitions for Silence Suppression Properties table as an aid.
3. Click **Save**.

Note:

For some of the changes to take effect, you must restart Avaya Aura® MS.

Enabling dual unicast monitoring

About this task

Avaya Aura® MS supports Prognosis from Avaya DevConnect Technology Partner, Integrated Research. Prognosis performance management software monitors voice quality, availability, and performance in real-time so that you can identify and resolve issues.

Perform this task to enable Prognosis unicast monitoring of the RTCP packets generated by Avaya Aura® MS.

Note:

In addition to the Source Description (SDES) packet, Avaya Aura® MS supports Prognosis Application Packet Subtype 4 partially. There is no support for the other Application Packet Subtypes. The following fields of Application Packet Subtype 4 are not supported.

Unsupported App Packet Subtype 4 Fields	Description
MID_RSVP_RECEIVER_STATUS	RSVP status
MID_JITTER_BUFFER_OVERRUNS	Jitter buffer overruns
MID_ECHO_TAIL_LENGTH	Echo tail length
MID_RTP_TTL	Time To Live
MID_RTP_DSCP	Received DSCP
MID_RTP_8021D	802.1 D
MID_ECHO_CANCELLATION	Acoustic Echo Cancellation
MID_ADDR6_PORT	Remote IPv6 Address and RTCP Port
MID_RTP_FLOW_LABEL	IPv6 Received Flow Label

Before you begin

Ensure that the Prognosis monitoring system is available and configured to communicate with Avaya Aura® MS.

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **General Settings** > **Dual Unicast Monitoring**.
2. To enable dual unicast monitoring, select **Dual Unicast Monitoring**.
3. Enter the address of the destination monitoring server in the **Monitoring Server IP** field.
4. Enter the port to use for the destination monitoring server in the **Monitoring Server Port** field.
5. Click **Save**.
6. Restart Avaya Aura® MS for the changes to take effect.

Enabling and configuring audio codec settings

About this task

Perform the following procedure to enable the audio codecs you want to support on the media server.

Note:

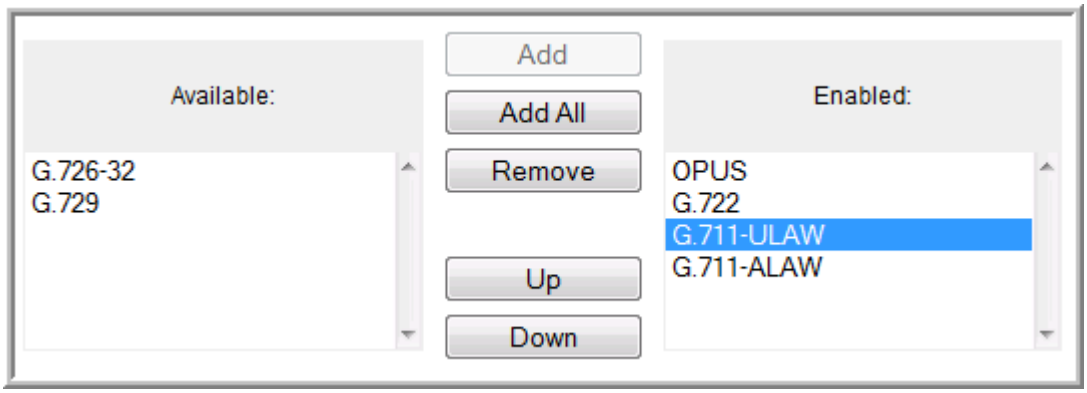
Controlling applications typically override AAMS configuration using templates and template control modifiers. Codec configuration changes and preferences must be configured first on the controlling application and not on Avaya Aura® MS. See documentation for the controlling application to determine if any Avaya Aura® MS changes are required.

Perform the following procedure to enable the audio codecs you want to support on the media server:

The order of the codecs in the **Enabled** list defines the preference of media server for codec selection in sessions originating from the media server. For incoming sessions, the first codec in the codec offering list of the incoming session, which is enabled on the media server, is accepted.

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **Audio Codecs**.



2. In the **Codec Selection** section, select one or more audio codecs from the **Available** list.
3. Click **Add** to move the codecs to the **Enabled** list.
4. To change the priority rank of a codec within the **Enabled** list, select a codec and use the **Up** or **Down** buttons to move the codec within the list.
5. If the Opus Codec is enabled, then in the **Codec Setting** section select the required Opus quality level using the **Profile** drop-down menu. Use the following profile option definitions as an aid:
   - **Constrained Narrowband @ 12Kbps:** This profile has an 8 kHz sampling rate and should be used for sessions on severely bandwidth-constrained links.
   - **Narrowband @ 16Kbps**: This profile has an 8 kHz sampling rate and can be used for sessions with bandwidth-constrained links.
   - **Wideband @ 18Kbps**: This profile has a 16 kHz sampling rate and provides high quality audio and video.
6. In the **Codec Selection** section, select **Silence Suppression** and other options for each codec as required.
7. In the **Audio Packet Time** section, select the **Default PTime** to use as the offered PTime for outgoing sessions. Avaya recommends a value of 20 ms for the best performance.
8. Click **Save**.

Removing an audio codec

About this task

Perform the following procedure to disable an audio codec you no longer want to support on Avaya Aura® MS.

Note:

Controlling applications typically override AAMS configuration using templates and template control modifiers. Codec configuration changes and preferences must be configured first on the controlling application and not on Avaya Aura® MS. See documentation for the controlling application to determine if any Avaya Aura® MS changes are required.

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **Audio Codecs**.
2. On the **Audio Codecs** page, select the audio codec from the **Enabled** list.
3. Click **Remove** to move the codec to the **Available** list.
4. Click **Save**.

Enabling the video media processor

About this task

The video media processor component (VidMP) is disabled by default on Avaya Aura® MS. Enable the video media processor when you require video relay and switching capabilities.

Procedure

1. Navigate to **EM** > **System Configuration** > **Server Profile** > **General Settings** > **Server Function**.
2. Select **Video Media Processor**.
3. Click **Save**.

Enabling and configuring video codec settings

About this task

Note:

Codec configuration changes and preferences must be configured on the controlling application and not Avaya Aura® MS.

Removing a video codec

About this task

Note:

Codec configuration changes and preferences must be configured on the controlling application and not Avaya Aura® MS.

Enabling and configuring digit relay settings

About this task

Note:

Controlling applications typically override AAMS configuration using templates and template control modifiers. Digit relay configuration changes and preferences must be configured first on the controlling application and not on Avaya Aura® MS. See documentation for the controlling application to determine if any Avaya Aura® MS changes are required.

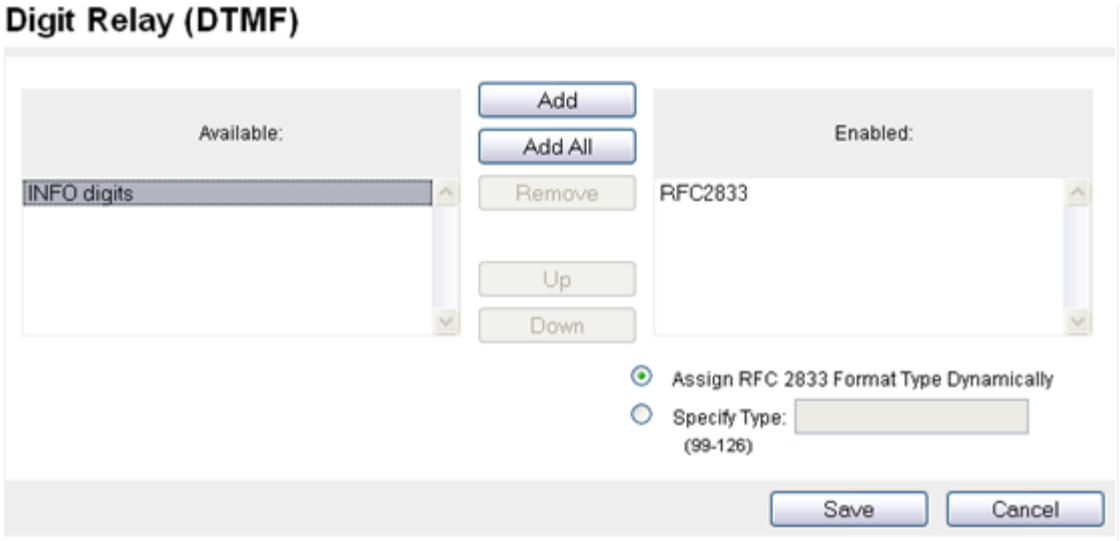
Avaya Aura® MS uses digit relay settings and the order of the enabled relay methods when negotiating digit relay with a client endpoint. These settings apply for inbound or outbound sessions.

Avaya Aura® MS also supports in-band DTMF. The system defaults to this option if no other option is configured or negotiated by Avaya Aura® MS. The preferred method of digit transmission is RFC 2833.

Perform the following procedure to enable and configure the digit relay support on Avaya Aura® MS.

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **Digit Relay (DTMF)**.



2. On the Digit Relay (DTMF) page, select one or more methods from the **Available** list.
3. Click **Add** to move the methods to the **Enabled** list.
4. To change the priority rank of a method within the **Enabled** list, select a method and use the **Up** or **Down** buttons to move it within the list.
5. Choose the required payload type option:
   - If a dynamic payload type is required, select **Assign RFC 2833 Format Type Dynamically**.
   - If a fixed payload type is required, select **Specify Type**. In the **Specify Type** field, enter the value to use in the payload type field of the RTP header when transmitting RFC2833 encoded digits.
6. Click **Save**.

Removing a digit relay method

About this task

Note:

Controlling applications typically override AAMS configuration using templates and template control modifiers. Digit relay configuration changes and preferences must be configured first on the controlling application and not on Avaya Aura® MS. See documentation for the controlling application to determine if any Avaya Aura® MS changes are required.

Perform the following procedure to disable digit relay method you no longer want to support on Avaya Aura® MS:

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **Digit Relay (DTMF)**.
2. On the Digit Relay (DTMF) page, select the method to disable from the **Enabled** list.
3. Click **Remove** to move the method to the **Available** list.
4. Click **Save**.

WebRTC configuration

Setting up a media stream with WebRTC media endpoints often requires use of the RFC 5245 Internet Connectivity Establishment (ICE) protocol for network address translation (NAT) and firewall traversal. The ICE protocol uses Session Traversal for NAT (STUN) and its extension protocol, Traversal Using Relay NAT (TURN), to support media services in a variety of network environments with NAT and firewall configurations.

You can configure multiple STUN and TURN server instances for redundancy or to scale service capacity. Avaya Aura® MS supports statistical load balancing using the priority and weight you configure for each server instance.

The audio support is enabled by default. To enable video support, see Enabling the video media processor on page 115. The Video WebRTC media session supports network congestion and loss countermeasures. Forward Error Correction and Retransmission are negotiated only if that is supported by the browser. In cases where the Media Server acts as a gateway for other devices, the source video rate will be controlled when the target client is experiencing any packet loss.

Important:

WebRTC sessions are not supported in a 1+1 HA cluster.

Enabling ICE

About this task

Configuring ICE requires that you first enable the **Firewall NAT Tunneling Media Processor**.

Perform the following procedure to enable ICE, and display the ICE configuration items in the EM task list:

Procedure

1. Navigate to **EM** > **System Configuration** > **Server Profile** > **General Settings** > **Server Function**.
2. Select **Firewall NAT Tunneling Media Processor**.
3. Click **Save**.

Configuring ICE general settings

About this task

Perform the following procedure to force media through TURN servers:

Before you begin

You must enable Firewall NAT Tunneling Media Processor before you can configure ICE.

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **ICE** > **General Settings**.
2. Select **Force Media Through a Configured TURN Server**.
3. Click **Save**.

Configuring STUN and TURN servers

Before you begin

You must enable the Firewall NAT Tunneling Media Processor before you can configure STUN and TURN servers.

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **ICE** > **STUN/TURN Servers** > **Servers**.
2. Click **Add...**
3. Enter a unique name for the server in the **Name** field.
4. Enter a description for the server in the **Description** field.
5. Select the type of server from the **Type** drop-down menu.
6. Select the required transport protocol from the **Transport Protocol** drop-down menu.
7. Enter the server IP address in the **Address** field.
8. Enter the server port in the **Port** field.

   The default port is 3478.
9. Specify the priority of this server compared to other servers in the pool in the **Priority** field. A lower number represents a higher priority.
10. Specify the weight of this server compared to other servers in the pool in the **Weight** field.

11. Select one of the following **Account** options:
    - If an account is not required for the server, select **Disabled**.
    - To use an existing STUN/TURN account with this server, select the required alias and user ID from the **Use an existing account** drop-down menu.
    - To create a new STUN/TURN account for this server, select **Create a new account** and configure the **Alias**, **User ID** and **Password** fields.
12. Click **Save**.

Locking or Unlocking STUN and TURN servers

About this task

Locking a STUN or TURN server disables the server preventing it from providing service.

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **ICE** > **STUN/TURN Servers** > **Servers**.
2. Select the servers you want to lock or unlock.
3. Select **Lock** or **Unlock** from the **More Actions** drop-down menu.

Deleting STUN and TURN servers

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **ICE** > **STUN/TURN Servers** > **Servers**.
2. Select the servers you want to remove.
3. Click **Delete**.

Adding or modifying STUN and TURN accounts

Before you begin

You must enable the Firewall NAT Tunneling Media Processor before you configure STUN and TURN accounts.

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **ICE** > **STUN/TURN Servers** > **Accounts**.
2. Click **Add...** to add a new account or select an existing account to modify and click **Edit…**
3. For new accounts, enter an **Alias**.
4. Enter the **User ID** and **Password** for the account.
5. Click **Save**.

Deleting STUN and TURN accounts

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **ICE** > **STUN/TURN Servers** > **Accounts**.
2. Select the accounts you want to remove.
3. Click **Delete**.

Media security configuration

Perform the following procedure to configure the media security policy to use for Session Description Protocol (SDP) negotiation.

You can secure media streams with cryptographic protection based on RFC 3711—The Secure Real-time Transport Protocol (SRTP). SRTP is a Real-time Transport Protocol (RTP) (RFC 3550) profile with symmetrical data encryption. SRTP provides the following security services:

encryption, message integrity, and replay protection.

Secure Real-time Transport Control Protocol (SRTCP) provides same security services to RTCP as SRTP does to RTP. SRTP message authentication protects the RTCP fields that keep track of membership, provide feedback to RTP sends, or maintain packet sequence counters.

Selecting a media security policy

About this task

Note:

Controlling applications typically override AAMS configuration using templates and template control modifiers. Media security configuration changes and preferences must be configured first on the controlling application and not on Avaya Aura® MS. See documentation for the controlling application to determine if any Avaya Aura® MS changes are required.

Perform the following procedure to enable and configure the desired media security policy.

Use the Definitions for Security Policy Options table as an aid for the procedure.

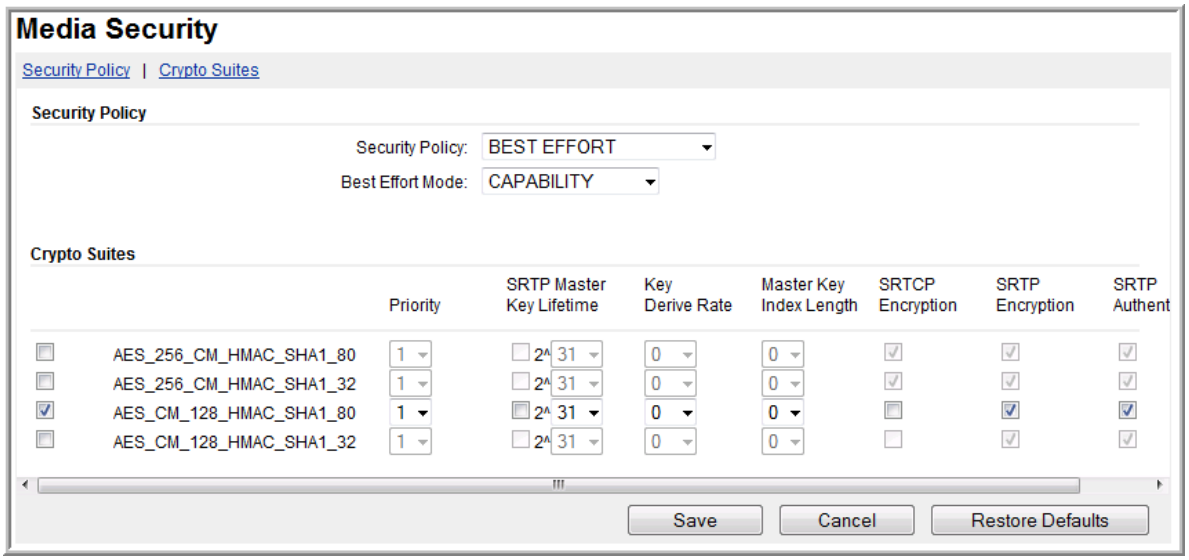
Definitions for security policy options		
Property	**Description**	
Security Policy	The media security policy to use for SDP negotiation. The options include:	
	Best Effort	Both Audio Video Profile (AVP) and Secure AVP (SAVP) sessions are offered and accepted, with preference given to negotiating to SAVP. This is the default.

Table continues…

Definitions for security policy options		
Property	**Description**	
	Security Disabled	Only AVP is offered or negotiated.
	Security Enforced	Only SAVP is offered or negotiated.
Best Effort Mode	The options include:	
	Capability	The SDP is formatted according to the Capability Negotiation format, using tcap/acap/pcap open parameters to negotiate AVP versus SAVP. This is the default.
	Dual M-Line	The existing default SDP specification, containing both AVP and SAVP media stream offerings for each media type. This is the default.
	CAPNEG Draft	The SDP is formatted according to a draft version of the Capability Negotiation standard. It does not use the Attribute Capability Attribute (acap=) to convey the crypto information.

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **Media Security**.



2. On the Media Security page, in the **Security Policy** area, use the **Security Policy** list to select the required method.

3. In the **Best Effort Mode** list, select the required mode.
4. Click **Save**.

Configuring crypto suites

About this task

Note:

Controlling applications typically override AAMS configuration using templates and template control modifiers. Media security configuration changes and preferences must be configured first on the controlling application and not on Avaya Aura® MS. See documentation for the controlling application to determine if any Avaya Aura® MS changes are required.

Configure cryptographic suites to provide message privacy.

Use the Definitions for crypto suite options table as an aid for the following procedure.

Definitions for crypto suite options	
Property	**Description**
AES_256_CM_HMAC_SHA1_80	The SRTP Advanced Encryption Standard (AES) 256 bit Counter Mode (CM) cipher is used with Hash Message Authentication Code -Secure Hash Algorithm (HMACSHA1) message authentication having an 80-bit authentication.
AES_256_CM_HMAC_SHA1_32	The SRTP AES-256 Counter Mode cipher is used with HMAC-SHA1 message authentication having a 32-bit authentication tag
AES_CM_128_HMAC_SHA1_80	The SRTP AES-128 Counter Mode cipher is used with HMAC-SHA1 message authentication having a 80-bit authentication.
AES_CM_128_HMAC_SHA1_32	The SRTP AES-128 Counter Mode cipher is used with HMAC-SHA1 message authentication having a 32- bit authentication.
Priority	The preference ranking for Crypto Suites. The default is a priority of 1. A priority of 1 is the highest priority and 9 the lowest.
SRTP Master Key Lifetime	The exponent of the number of packets between key renegotiations. The default is 2^31 for Secure RTCP (SRTCP). The range is 1 to 31.
Key Derive Rate	A value that sets the rate at which new keys are derived. The default is 0. The range is 0 to 24.
Master Key Index Length	The number of bytes in the Master Key Index, which is transmitted with each packet, to identify which master key to use for decoding. The default is 0. The range is 0 to 4.

RFC4568 specifies the following session parameters for modifying the default behavior for SRTP and SRTCP streams:

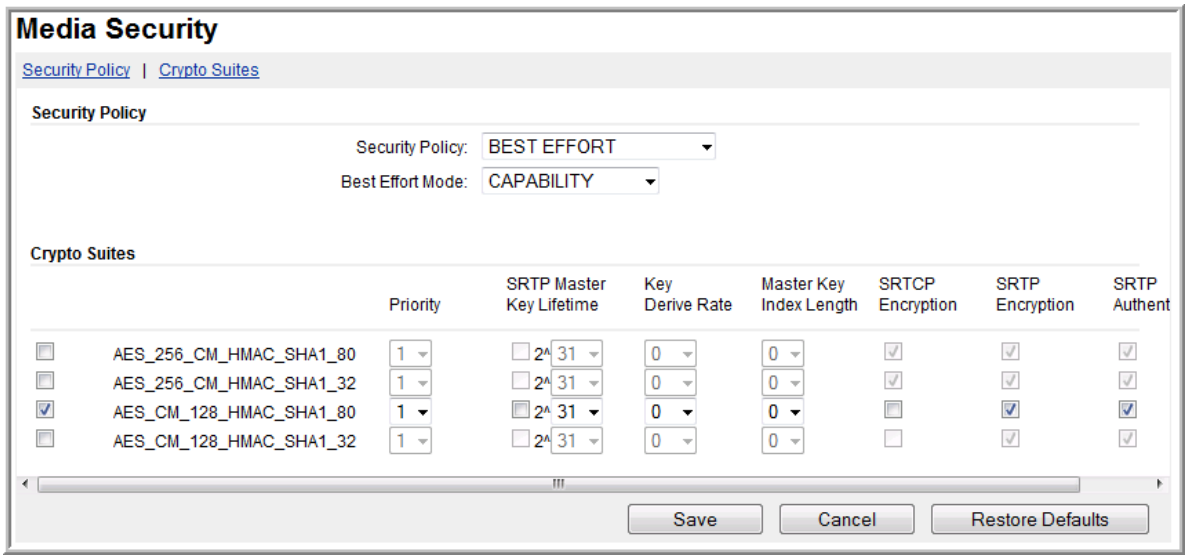
- UNENCRYPTED_SRTCP
- UNENCRYPTED_SRTP
- UNAUTHENTICATED_SRTP

When one or more of the negotiated session parameters are received in an incoming offer, Avaya Aura® MS uses the offered parameter by including the same session parameter in the answer. Avaya Aura® MS uses the configured default behavior if the received offer does not include one or more of the negotiated session parameters.

Definitions for negotiated parameters	
Property	**Description**
Enable SRTCP Encryption	Select to specify that SRTCP encryption is preferred. Clear to include the UNENCRYPTED_SRTCP session parameter in outgoing offers.
Enable SRTP Encryption	Select to specify that SRTP encryption is preferred. Clear to include the UNENCRYPTED_SRTP session parameter in outgoing offers.
Enable SRTP Authentication	Select to specify that SRTP authentication is preferred. Clear to include the UNAUTHENTICATED_SRTP session parameter in outgoing offers.

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **Media Security**.



2. On the Media Security page, in the **Crypto Suites** section, select the check boxes next to the crypto suites you want to configure.

3. For each selected crypto suite, in the **Priority** column, select a priority number.
4. In the **SRTP Master Key Lifetime** column, select the optional **SRTP master key lifetime** to include it in outgoing offers. Then, select a value for **SRTP master key lifetime**.
5. In the **Key Derive Rate** column, select a key derivation rate.
6. In the **Master Key Index Length** column, select a value for the master key index length.
7. Select or clear the **SRTCP Encryption**, **SRTP Encryption**, and **SRTP Authentication** columns as required
8. Click **Save**.

Music streaming configuration

Avaya Aura® MS supports continuous streaming of pre-transcoded audio. The media server supports the following types of music providers for streaming audio:

- Real Simple Syndication (RSS) provider
- HTTP/MP3 provider
- HTTP Live Streaming (HLS) provider

The media server supports up to 64 music streams across all the supported providers. Each provider implements a streaming protocol or playlist scheme for music playback. Provisioning a stream on the media server requires that you configure a provider with details about the source of the music. Configuration examples include providing URLs to RSS or HLS streaming radio servers on the internet.

Applications access provisioned music streams in the same way that they access an announcement for playback. Applications use the case-insensitive Stream Key that you configure for the stream to identify the required music.

Avaya Aura® MS Element Manager has a page for monitoring the status of music streaming providers. EM displays statistics for each stream which include bandwidth and the codec being used. When song metadata is available, EM displays details about the current song being played, including the song title and artist name.

Real Simple Syndication (RSS) provider

An RSS provider can be used to centrally manage music streams that have music files hosted on a remote web server. The media server downloads an RSS document specified by a URL. The media server downloads each file specified in the RSS document to a local cache.

The media server uses the RSS title element in the document as the title for the files in the cache. The files are played in alphabetical order.

The RSS provider on the media server supports audio files in WAV and MP3 formats. Avaya recommends that audio to be played by Avaya Aura® MS be encoded in G.711 or 16 bit, 8 kHz, single channel, PCM files. Codecs other than PCM or using higher sampling rates for higher

quality recordings can be used, however, with reduced system performance. Multiple channels, like stereo, are not supported.

The Time To Live (TTL) element in an RSS document specifies how many minutes an RSS channel can be cached on the media server before refreshing from the source. The minimum TTL value is 1 minute.

The GUID element in an RSS document uniquely identifies an RSS item. If an RSS item title, enclosure type, URL, or the associated file changes, then the GUID must be updated. If a GUID changes, then the media server refreshes the specified content.

The media server uses cached files to provide continuous streaming service when the RSS URL becomes unreachable. If you update or delete the RSS URL, then the files in the cache are deleted.

The RSS document must be formatted correctly. The maximum RSS document size is 256 KB. The following is an example of an RSS document with correct formatting:

```
<?xml version="1.0" encoding="UTF-8"?>
<rss version="2.0">
  <channel>
    <title>Relaxing Music</title>
    <description>Example RSS Music Playlist</description>
    <language>en-us</language>
    <ttl>15</ttl>
    <item>
      <title>Corporate Edge - A Clear Vision</title>
      <enclosure url="http://musicserver/Music/DavenportMusic-0.wav" type="audio/wav"/>
      <guid>35942909-51f1-11e5-b4f5-00ffb0699410</guid>
      </item>
    <item>
      <title>Corporate Edge - First Impressions</title>
      <enclosure url="http://musicserver/Music/DavenportMusic-1.wav" type="audio/wav"/>
      <guid>3edcc894-51f1-11e5-b4f5-00ffb0699410</guid>
      </item>
    <item>
      <title>Kaleidoscope - Shades of Blue</title>
      <enclosure url="http://musicserver/Music/DavenportMusic-2.wav" type="audio/wav"/>
      <guid>47779c66-51f1-11e5-b4f5-00ffb0699410</guid>
      </item>
     <item>
      <title>Keynotes - Colors</title>
      <enclosure url="http://musicserver/Music/DavenportMusic-3.wav" type="audio/wav"/>
      <guid>ea3dd092-51f1-11e5-b4f5-00ffb0699410</guid>
     </item>
     <item>
      <title>Kalimba</title>
      <enclosure url="http://musicserver/Music/Kalimba.mp3" type="audio/mpeg"/>
      <guid>3e789aa0-cb7b-11e5-b904-18a9051819e8</guid>
     </item>
   </channel>
</rss>
```

HTTP/MP3 provider

The HTTP/MP3 provider supports SHOUTCast ICY streams and HTTP/MP3.

Most streaming radio stations on the internet stream over HTTP/MP3. Many of the stations use the SHOUTCast ICY protocol. Typically, a SHOUTCast stream provides a playlist in a `.pls`

or `.m3u` file. The `.pls` file is known as a Winamp playlist. Winamp playlist files have HTTP URL entries that reference audio streams.

In some cases the URLs inside the playlist can use nonstandard HTTP ports. You must configure the HTTP proxy on the media server when the HTTP/MP3 server returns documents containing URLs on HTTP ports that are not permitted through the firewall.

The HTTP/MP3 provider on the media server supports all bitrates as well as stereo and mono MP3 streams. When the specified radio station supports metadata, the media server accepts the song title and artist information as it is received in real-time. EM displays the current song title and artist on the monitoring page.

Avaya Aura® MS only supports MP3 SHOUTCast streams. AAC is not supported.

Avaya Aura® MS HTTP/MP3 provider automatically records 15 minutes of content. The recorded content provides a backup when the streaming server is unreachable. A common SHOUTCast radio station aggregator is Tunein Radio.

HTTP Live Streaming (HLS) provider

The HTTP Live Streaming (HLS) provider implements the client side of the Apple® HLS protocol. The HLS provider on the media server supports M3U8 files and nested M3U8 playlist files. The media server only supports AAC-LC and MP3 encoded streams with no encryption.

When `#EXTINF` headers are provided, the media server extracts the title and artist information. If an `#EXT-X-ENDLIST` header is provided, the media server enables a playback loop. The HLS provider supports live and variant playlists. The media server automatically loops non-live playlists.

In some cases the URLs inside the playlist can use nonstandard HTTP ports. You must configure the HTTP proxy on the media server when the HLS server returns documents containing URLs on HTTP ports that are not permitted through the firewall.

Avaya Aura® MS HLS provider automatically records 15 minutes of content. The recorded content provides a backup when the streaming server is unreachable.

Music stream transcoding

Each music stream is transcoded one time by Avaya Aura® MS. The transcoded stream is shared across all sessions using the same codec. The media server uses the G.722 codec to encode the audio. If additional codecs are required, for example, G.729 or OPUS NB, then additional transcode operations occur on demand.

The media server provides high levels of efficiency for RSS providers by caching transcoded versions of the files received from the stream. After a file is transcoded, little CPU is required to stream the music from the media server.

Streaming providers, like HTTP/MP3 and HLS, require additional CPU resources because the media server transcodes them in real-time.

Configuring an HTTP proxy for external music source access

About this task

Some external streaming servers stream music on nonstandard HTTP ports. When nonstandard ports are used, enterprise firewalls can block outgoing HTTP connections. Perform the following procedure to configure the address and port of an internal proxy server to allow access to external streaming servers. This proxy configuration applies to streaming that uses RSS, HLS, and ICY protocols over HTTP.

Procedure

1. Navigate to **EM** > **System Configurtaion** > **Media Processing** > **Music** > **General Settings**.
2. In the **HTTP Proxy Host** field, enter the FQDN or IP address of the internal proxy server that provides access to the required external music servers.
3. In the **HTTP Proxy Port** field, enter the required port number for the internal proxy server.
4. Click **Save**.

Adding a streaming music source

About this task

Perform the following procedure to add a streaming music source that uses RSS, HLS, or ICY protocols over HTTP.

Before you begin

The music source you configure must meet the following requirement for each provider:

RSS requirements:

- The audio must be encoded in MPEG-1 Audio Layer 3 (MP3), MPEG-2 Audio Layer 3 (MP3) or WAV.
- The maximum RSS document size is 256 KB.

HTTP/MP3 SHOUTCast and ICY requirements:

- Mono and stereo are supported.
- The audio must be encoded in MPEG-1 Audio Layer 3 (MP3) or MPEG-2 Audio Layer 3 (MP3).
- Supported MPEG-1 sample rates: 32000, 44100, and 48000 Hz.
- Supported MPEG-2 sample rates: 22050, 24000, and 16000 Hz.
- Supported bit rates: 32, 64, 96, 128, 160, 192, 256 and 320 kbps.
- The AAC codec is not supported.
- Content type for playlists must be `audio/x-scpls or audio/x-mpegurl.`
- Content type for audio must specify `audio/mpeg, audio/x-mpeg or application/octet-stream`.

- The server can respond with ICY 200 OK or standard HTTP 200 OK responses.
- The ICY MetaData update mechanism is supported. Use of this update mechanism is optional.
- VLC and Icecast streaming sources are supported as long as the codec and content type used are also supported.
- HTTP Proxy is supported. Use of an HTTP proxy is required when the HTTP/MP3 server returns documents containing URLs on non-standard HTTP ports that are not permitted through the firewall.

HLS requirements:

- The audio must be encoded in MPEG-1 Audio Layer 3 (MP3), MPEG-2 Audio Layer 3 (MP3) or AAC-LC.
- Mono and stereo are supported. Stereo sources are mixed into mono.
- AAC sampling rates are supported in the 8 kHz to 96 kHz range.
- Supported MPEG-1 sample rates: 32000, 44100, and 48000 Hz.
- Supported MPEG-2 sample rates: 22050, 24000, and 16000 Hz.
- Supported bit rates: 32, 64, 96, 128, 160, 192, 256 and 320 kbps.
- M3U8 master playlist and nested media playlist files are supported. Playlist and media URLs can be made relative to the master playlist document.
- HTTP Proxy is supported. Use of an HTTP proxy is required when the HLS server returns documents containing URLs on non-standard HTTP ports that are not permitted through the firewall
- Content types should be `application/vnd.apple.mpegurl` or `audio/mpegurl` and document extensions must be `.m3u8` or `.m3u`
- HLS M3U8/M3U meta-data is supported:
  `#extinf:<duration>, <author - title>`
- The use of encryption is not supported.
- Servers which require authentication are not supported.
- Video is not supported.

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **Music** > **Stream Provisioning**.
2. Click **Add...**
3. In the **Stream Type** field, click the music source type.
4. In the **Name field**, enter a name for the new music source.

   The system uses this name as the stream key.
5. To form a stream key in the form `name@domain` in the **Domain** field, enter a domain name.
6. In the **Primary URL** field, enter the address of the required music source.

7. To provide an alternate music source, in the **Backup URL** field, enter the address of another music source.

   The system automatically switches to the backup music source when the primary source is unavailable.

8. To add the music source in the locked state so that system does not use the new music source, select the **Locked** check box.

9. Click **Save**.

   The system displays the Stream Provisioning page. The color of the **Stream Key** indicates the connection status of the music source.

   Note:

   The Stream Provisioning page does not automatically update the status. Manually refresh the web page to update the status or see Monitoring music streams on page 216.

Next steps

Monitoring music streams on page 216.

Editing a streaming music source

About this task

Perform the following procedure to update the properties of a streaming music source.

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processsing** > **Music** > **Stream Provisioning**.
2. To indicate the music source to edit, select the corresponding check box.
3. Click **Edit...**
4. In the **Stream Type** field, click the music source type.
5. To change the stream key name, in the **Name** field, enter a name for the new music source.
6. **(Optional)** To change the domain part of the stream key, in the **Domain field**, enter a new domain name.
7. To change the primary music source, in the **Primary URL** field, enter the new address.
8. **(Optional)** To change the alternate music source, in the **Backup URL** field, enter the new address.
9. To change the availability of this music source, select or clear the **Locked** check box.
10. Click **Save**.
11. The system displays the **Stream Provisioning** page. The color of the **Stream Key** indicates the connection status of the music source.

Note:

The **Stream Provisioning** page does not automatically update the status. Manually refresh the web page to update the status or see Monitoring music streams on page 216.

Next steps

Monitoring music streams on page 216.

Deleting a streaming music source

About this task

Perform the following procedure to remove a configured music stream from Avaya Aura® MS.

Note:

A music source can be made temporarily unavailable by locking it.

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **Music** > **Stream Provisioning**.
2. To indicate which music sources to delete, select one or more corresponding check boxes.
3. To delete the selected music sources, click **Delete**.

Related links

Locking and unlocking a streaming music source on page 130

Locking and unlocking a streaming music source

Music streams do not have to be deleted to prevent them from being used. You can prevent applications from using a music stream by locking the music stream. Unlocking a locked music stream makes the music stream available for application use.

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **Music** > **Stream Provisioning**.
2. To indicate which music sources to lock or unlock, select one or more corresponding check boxes.
3. To change the state of the streaming music source, click the **More Actions...** drop-down menu and click **Lock** or **Unlock**.

Security configuration

Avaya Aura® MS includes default certificates that are useful for demonstration purposes. To ensure production systems are not compromised, you must replace the default certificates with unique, trusted certificates. Options for certificate replacement are:

- Certificates signed by a trusted party Certificate Authority (CA).
- Certificates signed and created by you using an authoritative certificate, including root certificates generated by Avaya Aura® System Manager.

Use the following table as an aid for the security configuration procedures in this section:

Definitions for default service profiles	
Service profile name	Interface secured
Application	Connections with applications, such as VXML or an application server.
Clustering	Avaya Aura® MS internode connections in clusters.
EM	Element Manager (EM) connections for administrator web browser access.
OAM	Web services, such as those accessed using SOAP with Avaya Aura® MS, and remote database access.
Signaling	SIP and MRCPv2 connections with Avaya Aura® MS.

Configuring the System Manager settings

Procedure

1. Navigate to **EM** > **Security** > **System Manager** > **Advanced Settings**.
2. Enter the address of System Manager in the **Fully qualified domain name (FQDN) of System Manager server** field.
3. Enter the port used by System Manager in the **System Manager server port** field.
4. Enter the user name to be used for System Manager role-based registration and navigation in the **System Manager registration username** field.
5. Enter the password to be used for System Manager role-based registration and navigation in the **System Manager registration password** field.
6. Click **Save**.

Creating a new certificate signed by System Manager as the root certificate authority in the key store

About this task

Perform the following procedure when System Manager serves as the root certificate authority.

Before you begin

Ensure that you have access to the enrollment password for System Manager Trust Management. For more information on enrollment password and its expiry, see *Administering Avaya Aura® System Manager*.

Configure the System Manager server address as a Fully Qualified Domain Name (FQDN) before using it as a Certificate Authority. For more information on System Manager settings for the media server, see *Configuring the System Manager Settings*.

Procedure

1. Navigate to **EM** > **Security** > **Certificate Management** > **Key Store**.
2. In the **Key Certificates** section, click **Create New...**
3. Set the **Signing authority** field to **System Manager**.
4. 4. Enter System Manager enrollment password for **System Manager Trust Management Enrollment Password** and **System Manager Trust Management Enrollment Confirm Password**.
5. Set the remaining fields as required for your system.
6. Click **Save**.

Next steps

Assign the new certificate to all service profiles. See Assigning a certificate to a service profile on page 135

Creating a new certificate signed by System Manager as the intermediate certificate authority in the key store

About this task

Perform the following procedure when System Manager serves as the intermediate certificate authority.

Procedure

1. Use EM to create a certificate signing request. See Creating a new certificate to be signed by other Certificate Authorities in the key store on page 133.
2. Have System Manager to sign the certificate signing request. See *Administering Avaya Aura® System Manager* for how to use System Manager to sign a certificate signing request.

3. Upload the signed certificate signing request to EM. See Processing a Certificate Signing Request Response in the key store on page 134.
4. Retrieves the certificates of System Manager intermediate certificate authority and the root certificate authority. See *Administering Avaya Aura® System Manager* for how to retrieve System Manager certificate authority certificates.
5. Import the certificates of root and intermediate certificate authorities to the media server trust store. See Importing a trust certificate to the trust store on page 136.

Next steps

Assign the new certificate to all service profiles. See Assigning a certificate to a service profile on page 135

Creating a new certificate to be signed by other Certificate Authorities in the key store

Procedure

1. Navigate to **EM** > **Security** > **Certificate Management** > **Key Store**.
2. In the **Key Certificates** section, click **Create New...**
3. Set the **Signing authority** field to **Other Certificate Authorities**.
4. Set the remaining fields as required for your system.
5. Click **Save**.

   The system displays a **File Save** dialog window box and prompts you to save the file.
6. Select a location for the file and then save the file.

Next steps

The certificate signing request (CSR) must be signed by a trusted Certificate Authority (CA) before use. See Processing a Certificate Signing Request Response in the key store on page 134 to complete the creation of the new certificate.

Creating a new self-signed certificate in the key store

Procedure

1. Navigate to **EM** > **Security** > **Certificate Management** > **Key Store**.
2. In the **Key Certificates** section, click **Create New...**
3. Set the **Signing authority** field to **Self-Signed**.
4. Set the remaining fields as required for your system.
5. Click **Save**.

Next steps

Assign the new certificate to a service profile. See Assigning a certificate to a service profile on page 135.

Processing a Certificate Signing Request Response in the key store

About this task

Perform the following procedure only for a certificate that is in pending state.

Note:

The Certificate Signing Request (CSR) response needs to be in PEM format.

Procedure

1. Navigate to **EM** > **Security** > **Certificate Management** > **Key Store**.
2. Select the required certificate in the **Key Certificates** section.
3. Click **Process Certificate Signing Request...**
4. Click **Browse…** and select the file of the Certificate Signing Request response.
5. Click **Process Signed Certificate**.

Next steps

Assign the new certificate to a service profile. See Assigning a certificate to a service profile on page 135.

Importing a key certificate to the key store

Procedure

1. Navigate to **EM** > **Security** > **Certificate Management** > **Key Store**.
2. In the **Key Certificates** section, **Click Import…**
3. Enter the password or private key for the import in the **Password for certificate import** field.

   The password is the same as the one used during the export.
4. Click **Browse...** and select the key certificate file to import.

   The key certificate file must be in PKCS12 or PEM format and each included certificate must have a private key.
5. To import the certificate, click **Save**.

Next steps

Assign the new certificate to a service profile. See Assigning a certificate to a service profile on page 135.

Exporting a key certificate in PEM format from the key store

About this task

Perform the following procedure to export a key certificate in PEM format that contains only the public certificate. Certificates exported using the PEM format cannot be reimported to Avaya Aura® MS because they do not contain the certificate private key.

Procedure

1. Navigate to **EM** > **Security** > **Certificate Management** > **Key Store**.
2. Select the required certificate in the **Key Certificates** section.
3. Click **Export...**
4. Select **Export in PEM Format** for the **Type** field.
5. Click **Export**.

   The system displays a File Save dialog window and prompts you to save the file.
6. Select a folder location and save the file.

Exporting a key certificate with a key from the key store

About this task

Perform the following procedure to export a key certificate in PKCS12 format that contains both the public certificate and the private key. Certificates exported using the PKCS12 format can be reimported to Avaya Aura® MS because they contain a private key.

Procedure

1. Navigate to **EM** > **Security** > **Certificate Management** > **Key Store**.
2. Select the required certificate in the **Key Certificates** section.
3. Click **Export…**
4. Select **Export with Key** for the **Type** field.
5. Enter a key in the **Password for certificate export** field.
6. Click **Export**.

   The system displays the File Save dialog window and prompts you to save the file.
7. Select a folder location and save the file.

Assigning a certificate to a service profile

Procedure

1. Navigate to **EM** > **Security** > **Certificate Management** > **Key Store**.
2. In the Service Profiles section, Click **Assign…**.
3. Set the **Certificate** field for each profile by using the drop-down list of certificates.

4. Click **Save**.
5. To apply the change, you must reboot the server.

Deleting a key certificate from the key store

Procedure

1. Navigate to **EM** > **Security** > **Certificate Management** > **Key Store**.
2. Select a key certificate from the list.

   Note:

   You cannot delete a key certificate assigned to a service profile.
3. Click **Delete**.
4. Click **Confirm**.

Importing a trust certificate to the trust store

Procedure

1. Navigate to **EM** > **Security** > **Certificate Management** > **Trust Store**.
2. Click **Import...** on the **Trust Store** page.
3. Click **Browse…** and select a file.

   Note:

   The trust certificate must be in PEM format.
4. Click **Upload**.

   The system displays the certificates.
5. Verify the certificate information.
6. Enter a name in the **Trust friendly name** field for each certificate.
7. Click **Save**.
8. To apply the change, you must reboot the server.

Importing a Trust Certification Revocation List

Procedure

1. Navigate to **EM** > **Security** > **Certificate Management** > **Trust Store**.
2. Select a **Certificate Authority** from the list.
3. Click **Import CRL...** on the **Trust Store** page.
4. Click **Browse…** and select a file to set the **Trust certification revocation list import file** field.

5. Click **Save**.
6. To apply the change, you must reboot the server.

Downloading Certification Revocation List

Before you begin

- Ensure that the CRL distribution point is available in the trust certificate.
- If the CRL distribution point uses HTTPS, ensure that the mutual authentication is set up between Avaya Aura® MS and the server hosting the CRL.
- The CRL you want to download must be in DER format.

Procedure

1. Navigate to **EM** > **Security** > **Certificate Management** > **Trust Store**.
2. Select a **Certificate Authority** from the list.
3. Click **Download CRL...** on the **Trust Store** page.

   The system displays a File Save dialog window and prompts you to save the file.
4. Select a location for the file and then save the file.

Deleting Certificate Authorities from the trust store

Procedure

1. Navigate to **EM** > **Security** > **Certificate Management** > **Trust Store**.
2. Select the **Certificate Authority** certificates from the list.
3. Click **Delete** on the **Trust Store** page.
4. Click **Confirm**.
5. To apply the change, you must reboot the server.

Content Store configuration

Configuring Content Store location

The Content Store component of Avaya Aura® MS stores media and other files for hosted applications on a disk. Avaya Aura® MS also uses the disk for SDR storage, persistent database store, and file manipulation that is unrelated to Content Store file management. As a result of the many requirements Avaya Aura® MS has for the system disk, disk performance can be an issue for some applications.

The default installation places content storage in a directory within the main Avaya Aura® MS installation path. To improve the capacity and performance of the system, configure a dedicated

disk for Content Store. Content Store uses this dedicated disk for applications that have large media file storage requirements.

Note:

Changing the Content Store location is a commissioning task for new systems. If you change the Content Store location later, files remain in the original location. You can remove these files manually. After the new location is configured, files stored in Content Store prior to changing the Content Store location are not included. Restore the files from a backup file if you want to include them in the new location.

About this task

Perform the following procedure to configure a dedicated disk for use by Content Store for applications that have large media file storage requirements:

Before you begin

When you use this procedure, the system removes the current content saved in Content Store and creates a new, empty Content Store. Ensure you back up the application data before you reconfigure the storage location.

You can restore the data from a backup file after the configuration is complete if you need to preserve the data. The system restores data to the configured Content Store location.

Procedure

1. Navigate to **EM** > **System Configuration** > **Content Store** > **General Settings**.
2. In the **File system location for content storage** field, enter the full pathname, starting from the file system root, to specify the disk that the system should use for Content Store.

   For example, enter `/mediafiles`.

   Restore the default value or clear the **File system location for content storage** field to use the default location within the installation path.
3. Click **Save**.
4. Click **Confirm**.
5. Perform the following steps to restart Avaya Aura® MS for the changes to take effect.
   a. Navigate to **EM** > **System Status** > **Element Status** and click **Restart**.
   b. Click **Confirm**.

EM preferences configuration

Configuring time zone preferences

About this task

Perform the following procedure to configure EM to display all times and dates using either the time zone of the local server or the Greenwich Mean Time (GMT) time zone:

Avaya Aura® MS defaults to using the local time.

Procedure

1. Navigate to **EM** > **System Configuration** > **Element Manager Settings** > **General Settings**.
2. To configure EM to use Greenwich Mean Time for displayed times, ensure that **Display times using GMT** is selected.
3. Click **Save**.

Setting Login security warning text

About this task

Perform the following procedure to add custom security warnings which are displayed when a user logs into EM:

Procedure

1. Navigate to **EM** > **Security** > **General Settings**.
2. Enter the security warning text in the **Security warning message on login** field.
3. Click **Save**.

Chapter 6: System Manager enrollment

Avaya Aura® System Manager enrollment overview

Some Avaya solutions which adopt Avaya Aura® MS use Avaya Aura® System Manager to provide an integrated point of management. This chapter shows you how to use Avaya Aura® MS Element Manager (EM) to enroll media servers in System Manager.

Note:

See adopting product documentation to determine if System Manager enrollment applies to your installation.

Important:

The media servers and System Manager must use the same NTP server for time synchronization. The system time difference between the System Manager and the media servers must not exceed 10 minutes.

You must perform the following procedures so that applications can access Avaya Aura® MS:

1. Pre-Enrollment steps on the System Manager.
2. Enrollment with System Manager from the Avaya Aura® MS.
3. Location and Application assignment on the System Manager.
4. Pre-Discovery steps on the System Manager.

See System Manager and adopting product documentation for detailed procedures.

Media server enrollment in System Manager assigns a System Manager-signed certificate to the media server OAM and EM service profiles. The enrollment process also assigns System Manager as the media server authentication and authorization source. These assignments enable Avaya Aura® MS to use single sign-on (SSO) and role-based access control (RBAC) services which are managed by System Manager. After enrollment administrators access the media server EM using System Manager administrative accounts which have permission to use EM.

When a media server is dis-enrolled from System Manager, the system assigns the authentication and authorization source to Avaya Aura® MS based authentication.

When you enroll a media server in System Manager, the system restarts the SOAP and EM services to apply the changes. When you dis-enroll a media server from System Manager, the system restarts the EM service to apply the changes. Users must close their current EM browser window or tab and can sign in again after the EM restart completes.

Pre-Enrollment steps on the System Manager

About this task

Perform the following procedure to prepare a System Manager account with the proper role and security credentials for Avaya Aura® MS. This account is used by Avaya Aura® MS to enroll with System Manager. Enrollment is not possible without this account. Perform this procedure only one time, before you enroll the first Avaya Aura® MS. This task is performed on the System Manager.

Before you begin

Ensure that you can access System Manager and the task **Users** > **Administrators** > **Security** > **Roles**.

Note:

- Save the administrative account and password. These are required to enroll Avaya Aura® MS with System Manager.
- System Manager 7.1.0 or higher limits the number of simultaneous sessions. The default number of sessions is 5. If you have multiple Avaya Aura® media servers enrolled with System Managerthat use the same System Manager administrative account and you exceed this limit you may experience issues.

Procedure

1. Sign in to System Manager.
2. Navigate to **Users** > **Administrators** > **Security** > **Roles**.
3. To add permission to an existing role on the **Roles** page, highlight the **Desired Role** and click **Edit** to navigate to the **Role Details** page.
4. Perform the following steps to create a new role:
   a. Select the role System Administrator.
   b. Click **New**.
   c. On the **Add New Role** page, set the role **Name** and **Description**.
   d. Click **Commit**. Click **Continue**.
5. On the Role Details page, click **Add Mapping…**.
6. On the Select Element and/or Network Service to Map to Role page, select **Avaya Aura Media Server** as **Element or Resource Type** and **All** as **Element or Resource Instance**. Click **Next**.
7. Click **Commit**.
8. On the Role Details page, click **Add Mapping...**.
9. Select **Elements** as the **Element or Resource Type** and **All** as the **Element or Resource Instance**.
10. Click **Next**.
11. On the Permission Mapping page, enable **add**, **change**, **delete** and **view** for **Role Resource Type Actions**.

12. Click **Commit**.
13. To complete the creation of the new or existing role, on the Role Details page, click **Commit**.
14. To assign the role to a new or existing System Manager account, navigate to **Users** > **Administrators** > **User Services** > **Administrative Users** .
15. For an existing Administrator go to Step 21 on page 142.
16. To create a new Administrator, navigate on Administrative Users page, click **Add…**
17. On **Add New Administrative User** Step 1 page, fill the required field. When done, click **Commit** and **Continue**.
18. On **Add New Administrative User** Step 2 page, select and assign the role that has the related permissions (the AAMS element and elements) such as **Avaya Aura Media Server Administrator**. Click **Commit**.
19. After creating the new administrative user, sign out of SMGR.
20. Sign into System Manager Web UI again using the new administrative user and change the password at the first login.
21. On the Administrative Users page, click the link of the System Manager administrative account to edit.
22. On the User Details page, click **Select Roles**.
23. On the User Roles page, select and assign the role that has the related permissions for Avaya Aura® MSelement and elements. For example, use the role **Avaya Aura Media Server Administrator**.
24. Click **Commit**.
25. On the User Details page, click **Commit**.

Enrolling a cluster in System Manager

About this task

Perform the following procedure to enroll an existing media server cluster in System Manager.

Before you begin

- Ensure that a media server cluster is already configured.
- Ensure that you have the following Avaya Aura® System Manager information available:
  - Fully Qualified Domain Name (FQDN) of the System Manager server.
  - System Manager HTTPS server port. The default port is 443.
  - System Manager administrative account username and password. The specified user account must be assigned with a role or roles that have the permissions of the element types **Avaya Aura Media Server**, **Session Manager and Routing**, and **elements**. For the permissions from **Session Manager and Routing**, only the permission for **Web**

Services > **Routing** is required. An example role that has the required permissions is **System Administrator**.

- Enrollment password for System Manager Trust Management.

- Ensure that there is network access between the media server and System Manager.
- Ensure that the FQDN of each media server in the cluster can be resolved by DNS or the local hosts file.
- Ensure that the FQDN of System Manager can be resolved by DNS or the local hosts file.
- Ensure that the FQDN of each media server has the same parent domain as the System Manager FQDN used for Single Sign-On.
- Ensure that the difference in system time between the System Manager server and each Media Server is within 10 minutes. The Media Server and System Manager must use the same NTP server for time.

Procedure

1. For the Primary node of the media server cluster, navigate to **EM** > **Security** > **System Manager** > **Enrollment**.

   EM displays a page describing the enrollment process.

2. Click **Begin Enrollment**.

   EM displays step one of the enrollment process.

3. In the **Cluster** section, type the **Administrative name** and **Administrative description** for the media server cluster.

   Administrative name is a name of your choice that helps you easily identify this cluster. This value must be unique among all media servers enrolled with System Manager. After enrollment, this value can only be updated using System Manager.

   Administrative description is a definition of your choice that helps you easily describe this cluster. After enrollment, this value can only be updated using System Manager.

4. In the **Servers** section, type the **Element Administrative Name** and **Element Administrative Description** for each server.

   Element Administrative Name is a name of your choice that helps you easily identify this server. This value must be unique among all media servers enrolled with System Manager. This value cannot be updated after enrollment.

   Element Administrative Description is a definition of your choice that helps you easily describe this server. This value cannot be updated after enrollment.

5. Click **Next**.

   EM displays step two of the enrollment process.

6. In the **Server Configuration** section, provide the FQDN and port for System Manager. The default System Manager port is 443.

Note:

If primary System Manager is not available for the enrollment, stop the enrollment. After primary System Manager becomes available, start the enrollment process again.

7. In the **Administrative Account** section, provide the System Manager administrative account credentials required to register the Media Server.
8. Click **Next**.

   EM displays step three of the enrollment process.

   Note:

   If EM cannot validate System Manager server certificates with the Media Server trust store, then EM displays the certificates received from System Manager. Click **Acknowledge** to proceed with the enrollment or **Decline** to end the enrollment process.
9. If you have replaced the media server generated self-signed certificates with the certificates signed by the same CA on each server in the cluster, select **Use existing certificates already imported** and click **Next**.

   Otherwise, select one of the following options appropriate for your system:

   - If the current certificate setup in the cluster is correct on each Media Server and all the following are true for your system, then select **Use existing certificates already imported** and click **Next**:
     - The key identity certificate for the Media Server is in the Media Server key store.
     - The trust certificate to verify the System Manager key identity certificate is in the Media Server trust store. If the certificate chain is used, the trust certificates of root certificate authority and all intermediate certificate authorities must be in the Media Server trust store.
     - The key identity certificate for the Media Server is at least assigned to the OAM and EM service profiles.
   - Select **Create a new System Manager-signed certificate** when System Manager is the signing authority for certificates in the Media Server setup as the root certificate authority and a System Manager-signed certificate is not in the key store of the Media Server. Click **Next** to configure the certificate fields as follows:
     - Select the strength of the certificate key. Avaya recommends using strong security by selecting a Key bit length of 2048 or higher, and a Signature algorithm of SHA256 or higher.
     - Type the name of the organization using the certificate in the **Organization** and **Organization Unit** fields.
     - Type an ISO-3166 country code for the **Country field**.
     - Type the full name of the state or province in the **State/Province field**.
     - Type the location name in the **City/Locality** field.

- If the subject alternative name with the server IP address is required for the certificate, select **Include Subject Alternative Name with IP address** and enter the IP address.
- If the subject alternative name with the server FQDN is required for the certificate, select **Include Subject Alternative Name with FQDN** and enter the FQDN.
- In the Trust Management section, provide the System Manager trust management enrollment password. This is the enrollment password that the media server must use to acquire a System Manager-signed certificate from System Manager Trust Management.

  See *Administering Avaya Aura® System Manager* or the *Avaya Aura® System Manager Online Help* for additional details about this password and when it expires.

Note:

If System Manager is the signing authority and serves as an intermediate certificate authority, do not select **Create a new System Manager-signed certificate** in the enrollment process. See Creating a new certificate signed by System Manager as the root certificate authority in the key store on page 132 to set up the certificates then select **Use existing certificates already imported**.

10. Click **Next**.

    EM displays the final step of the enrollment process.

11. Verify the System Manager enrollment information. Click **Previous** if any information needs to be changed.
12. Click **Enroll**.

    EM displays a progress spinner during the enrollment process. After the enrollment completes, the system restarts the Media Server SOAP service and EM.

13. Close the EM browser window or tab.

    Wait for the EM restart to complete.

14. To verify the Media Server enrollment process, log in to each Element manager in the cluster using System Manager credentials

    After enrolling with System Manager, you can use System Manager credentials to access EM.

Next steps

The enrollment process automatically assigns the System Manager-signed certificate to the media server OAM and EM service profiles. If the System Manager-signed certificate needs to be applied to other Media Server service profiles see *Assigning a certificate to a service profile*.

If required by the adopting solution, access System Manager to configure the location and application for the newly enrolled media server. See *Location and application assignment on System Manager*.

Disenrolling a cluster from System Manager

About this task

Perform the following procedure to disenroll and remove a media server cluster from System Manager.

When a media server is disenrolled and removed from System Manager, the system assigns the media server authentication and authorization source to Avaya Aura® MS based authentication.

Before you begin

Ensure that the media server cluster that you want to disenroll is currently enrolled in System Manager.

Procedure

1. For the Primary node of the media server cluster, navigate to **EM** > **Security** > **System Manager** > **Enrollment**.

   EM displays a page describing the disenrollment process.

2. Click **Disenroll**.

   EM displays a progress spinner during the disenrollment process. After the disenrollment completes, the system restarts EM.

3. Close the EM browser window or tab.

   You can sign in again after the EM restart completes.

Enrolling a media server after extending a cluster enrolled with System Manager

About this task

When you add media servers to a cluster that is enrolled in System Manager, then you must also enroll the new media server cluster nodes in System Manager.

Perform the following procedure to enroll a media server in System Manager after you have added the media server to a cluster which is already enrolled in System Manager.

Before you begin

- Ensure that the media server is configured as part of an enrolled cluster, but it is not enrolled in System Manager.
- Ensure that you have the password for System Manager Trust Management.
- Ensure that there is network access between the media server and System Manager.
- Ensure that the FQDN of the media server can be resolved by DNS or the local hosts file.
- Ensure that the FQDN of the media server has the same parent domain as the System Manager FQDN used for Single Sign-On.

- Ensure that the difference in system time between the System Manager server and the media server is within 10 minutes. The media server and System Manager must use the same NTP server for time.

Procedure

1. Navigate to **EM** > **System Manager** > **Enrollment**.
2. Click **Begin Enrollment**.

   EM displays step one of the enrollment process.
3. Type a name of your choice that helps you easily identify this server in the **Element Administrative Name** field. This value must be unique among all media servers enrolled with System Manager. This value cannot be updated after enrollment.
4. Type a definition of your choice that describes this server in the **Element Administrative Description** field. This value cannot be updated after enrollment.
5. Click **Next**.

   EM displays step two of the enrollment process.
6. In the **Server Configuration** section, provide the FQDN and port for System Manager. The Secondary System Manager configuration fields are optional. The default System Manager port is 443.
7. In the **Administrative Account** section, provide the System Manager administrative account credentials required to register the Media Server.
8. Click **Next**.

   EM displays step three of the enrollment process.

   Note:

   If EM cannot validate System Manager server certificates with the Media Server trust store, then EM displays the certificates received from System Manager. Click **Acknowledge** to proceed with the enrollment or **Decline** to end the enrollment process.
9. Select one of the following options appropriate for your system:
   - If the current certificate setup in the cluster is correct on each Media Server and all the following are true for your system, then select **Use existing certificates already imported** and click **Next**:
     - The key identity certificate for the Media Server is in the Media Server key store.
     - The trust certificate to verify the System Manager key identity certificate is in the Media Server trust store. If the certificate chain is used, the trust certificates of root certificate authority and all intermediate certificate authorities must be in the Media Server trust store.
     - The key identity certificate for the Media Server is at least assigned to the OAM and EM service profiles.

- Select **Create a new System Manager-signed certificate** when System Manager is the signing authority for certificates in the Media Server setup as the root certificate authority and a System Manager-signed certificate is not in the key store of the Media Server. Click **Next** to configure the certificate fields as follows:
  - Select the strength of the certificate key. Avaya recommends using strong security by selecting a Key bit length of 2048 or higher, and a Signature algorithm of SHA256 or higher.
  - Type the name of the organization using the certificate in the **Organization** and **Organization Unit** fields.
  - Type an ISO-3166 country code for the **Country field**.
  - Type the full name of the state or province in the **State/Province field**.
  - Type the location name in the **City/Locality** field.
  - If the subject alternative name with the server IP address is required for the certificate, select **Include Subject Alternative Name with IP address** and enter the IP address.
  - If the subject alternative name with the server FQDN is required for the certificate, select **Include Subject Alternative Name with FQDN** and enter the FQDN.
  - In the Trust Management section, provide the System Manager trust management enrollment password. This is the enrollment password that the media server must use to acquire a System Manager-signed certificate from System Manager Trust Management.

    See *Administering Avaya Aura® System Manager* or the *Avaya Aura® System Manager Online Help* for additional details about this password and when it expires.

Note:

If System Manager is the signing authority and serves as an intermediate certificate authority, do not select **Create a new System Manager-signed certificate** in the enrollment process. See Creating a new certificate signed by System Manager as the root certificate authority in the key store on page 132 to set up the certificates then select **Use existing certificates already imported**.

10. Click **Next**.

    EM displays the final step of the enrollment process.
11. Verify the System Manager enrollment information. Click **Previous** if any information needs to be changed.
12. Click **Enroll**.

    EM displays a progress spinner during the enrollment process. After the enrollment completes, the system restarts the Media Server SOAP service and EM.
13. Close the EM browser window or tab.

    Wait for the EM restart to complete.

14. To verify the Media Server enrollment process, log in to each Element manager in the cluster using System Manager credentials

    After enrolling with System Manager, you can use System Manager credentials to access EM.

Next steps

The enrollment process automatically assigns the System Manager-signed certificate to the media server OAM and EM service profiles. If the System Manager-signed certificate needs to be applied to other Media Server service profiles see Assigning a certificate to a service profile on page 135.

If required by the adopting solution, access System Manager to configure the location and application for the newly enrolled media server. See Location and application assignment on System Manager on page 150.

Related links

Configuring a Secondary server for a cluster on page 35
Configuring a Standard server for a cluster on page 36

Removing a non-primary server from an enrolled cluster

About this task

When a media server is disenrolled and removed from System Manager, the system assigns the media server authentication and authorization source to Avaya Aura® MS based authentication.

Perform the following procedure to disenroll and remove a media server from a cluster that is enrolled in System Manager.

Procedure

1. For the media server that you want to remove from the cluster, sign in to EM then navigate to **Cluster Configuration** > **Server Designation**.

   EM displays a page describing the disenrollment process.

2. Set the local server **Role** to Primary.
3. Remove all entries from the **Server Designation** table by selecting each entry and clicking **Remove**.
4. Click **Save**.
5. Click **Confirm**.

   The system removes the media server from the cluster and automatically disenrolls the media server from System Manager. When the disenrollment completes, the system restarts EM.

6. Close the EM browser window or tab.

   You can sign in again after the EM restart completes.

7. Navigate to **System Status** > **Element Status** and click **Restart** for the server role changes to take effect.
8. Sign in to EM on the Primary media server of the cluster. Navigate to **Cluster Configuration** > **Server Designation**.
9. Select the media server for removal from the **Server Designation** table and click **Remove**.
10. Click **Save**. Click **Confirm**.

Location and application assignment on System Manager

About this task

After you enroll Avaya Aura® MS cluster with System Manager, some services require that the Avaya Aura® MS be assigned both a location and a controlling application. After Avaya Aura® MS is assigned, a controlling application, such as Avaya Aura® Web Gateway, can discover the Media Servers as a resource for application use.

Note:

Media Server clusters can be removed from one application and assigned to another application using this interface.

Perform the following procedure to assign a location and application to the Media Server.

Before you begin

The media server must be enrolled with System Manager.

Procedure

1. Sign in to System Manager Web UI.
2. Navigate to **Elements** > **Media Server** > **Application Assignment**.
3. Select the **Application Name** to assign, for example, **Avaya Aura® Web Gateway**.
4. Click **Edit**.
5. Select the media server clusters that you want to assign to this application.
6. Click **Commit**.

Next steps

Some controlling applications require that a location is assigned to a Media Server. See System Manager documentation for assignment of a location.

Pre-Discovery steps on the on the System Manager

About this task

Prior to an application discovering any assigned Media Server, a special administrator account in System Manager must be prepared to allow the application access. Not all applications perform this discovery step, so this procedure may not be needed. See adopting solution documentation for details.

Procedure

1. Sign into System Manager Web UI.
2. Navigate to **Users** > **Administrators** > **Security** > **Roles**.
3. On the **Roles** page, highlight the role **System Administrator**, and click **New** to create a new role.
4. On the **Add New Role** page, set the role name and description.
5. Click **Commit** and click **Continue**.
6. On the Role Details page, click **Add Mapping…**.
7. On the Select Element and/or Network Service to Map to Role page, select **Avaya Aura Media Server** as **Element** or **Resource Type** and **All** as **Element** or **Resource Instance**.
8. Click **Next**.
9. Click **Commit**.
10. To complete the creation of the new role with the permissions of Media Server element, on the Role Details page, click **Commit**.
11. To assign the new role to an administrative account, sign into System Manager Web UI.
12. Navigate to **Users** > **Administrators** > **User Services** > **Administrative Users**.
13. On the **Administrative Users** page, click **Add…**
14. On the Add New Administrative User Step 1 page, fill in the required field.
15. Click **Commit**. Click **Continue**.
16. On the Add New Administrative User Step 2 page, select and assign the role that has the permissions of AAMS element as **Avaya Aura Media Server Administrator**.
17. Click **Commit**.
18. Sign out of System Manager.
19. Sign into System Manager again using the new administrative user and change the password at the first login.

Note:

The new administrative user and password are required by the Media Server controlling application, see the applications documentation to determine where to configure this information.

Chapter 7: Media file provisioning

Media file format

Avaya recommends that audio to be played by Avaya Aura® MS be encoded as 16 bit, 8 kHz, single channel, PCM files stored in WAV format. Codecs other than PCM or using higher sampling rates for higher quality recordings can be used, however, with reduced system performance. Multiple channels, like stereo, are not supported.

Table 1: Supported audio file formats:

Codec	Type	Channels	Sample Rate	Bits/Sample
Linear PCM	Audio	1	Any (8 KHz recommended)	16
PCMA	Audio	1	8 KHz	8
PCMU	Audio	1	8 KHz	8

Media storage in Avaya Aura® MS Content Store

The Content Store component of Avaya Aura® Media Server (MS) stores media and other files for hosted applications. Content Store provides a reliable, highly available, and persistent storage capability for Avaya Aura® MS. Any application with storage needs that align with the functionality of Content Store can use Content Store. However, not all applications must use the Content Store.

Content Store has an organized storage space consisting of Namespaces that include Content Groups which contain the actual content. Namespaces are the top level containers, under which Content Group containers exist. Namespaces and Content Groups can be considered analogous to folders. Actual content is stored by Content ID within each Content Group. A Content ID is analogous to a filename.

The following example shows the structure of Content Store:

```
Namespace_I
      ContentGroup_A
         Content ID1
         Content ID2
      ContentGroup_B
         Content ID1
         Content ID2
   Namespace_II
```

```
      ContentGroup_A
         Content ID1
         Content ID2
```

To provide high capacity and high availability, Content Store is scaled automatically with the cluster. Content Stores are automatically enabled on each media server in a cluster. The application content in the Content Stores of a cluster is synchronized automatically.

There is a master Content Store configured on both the Primary and Secondary servers of a load sharing cluster or on the Primary and Backup servers of a High Availability cluster. The dual master Content Store configuration provides full hardware and functionally redundancy. Standard cluster nodes provide Content Stores which contain synchronized content for local access.

Content Stores communicate with each other when handling requests. A connection to any one Content Store in a cluster is sufficient for any client application. Data integrity and synchronization in a cluster are handled automatically by the Content Store peers. However, it is more efficient to provision new media files directly to one of the master Content Stores. When a content modification request is received at Standard node Content Store, it is first forwarded to one of the master Content Stores in the cluster for processing.

For examples of content organization and additional information on Content Store functionality, see Using Content Store in *Using Web Services on Avaya Aura® Media Server*.

Overview of the EM Media Management tool

Element Manager (EM) provides a Media Management tool which is used to upload and manage media files in Content Store. Using the Media Management tool, you can perform the operations described in the following table to manage media files stored in Content Store.

Media management operations		
Scope	**Operation**	**Description**
Namespace	Add	Create a new namespace.
	Browse	View the content of a namespace.
	Rename	Give a new name to a namespace.
	Delete	Remove a namespace and its content.
Content Group	Add Content Group	Create new content groups under a namespace or another content group.
	Add Media	Upload media files to a content group.
	Delete	Remove the content group and its files.

Table continues…

Media management operations		
Scope	**Operation**	**Description**
	Rename	Give a new name to a content group.
	Batch File Provision	Upload multiple files contained in a zip archive file.
Content	Cut	Use Cut and paste together to move a media content file from one content group to another.
	Copy	Use Copy and Paste together to duplicate an existing content file.
	Paste	Use with Copy and Cut to move and duplicate media files.
	Rename	Give a new name to a media file.
	Download	Download a media file to the local computer running the browser that you use to gain access to the EM.

Note:

Do not alter the default system namespaces.

Important:

Do not use the file system to manually access or change the media files managed by Content Store. Use appropriate interfaces such as the EM Media Management tool to make any changes.

The following procedures show you how to use each of these operations to organize and manage your media on Avaya Aura® MS.

Media Provisioning

Adding a content namespace

About this task

Perform the following procedure to add a content namespace to contain a group of related media files:

Procedure

1. Navigate to **EM** > **Tools** > **Media Management**.
2. On the Media Management page, click **Add...**

3. On the Add Content Namespace page, type a unique name for the new namespace in the **Name** field.

   The name cannot begin with the at (@) symbol, must be less than 128 characters, must not be case-sensitive, must not contain spaces, or any of the following symbols:

   { } ' * \

4. Click **Save**.

Renaming a content namespace

About this task

Perform the following procedure to rename a content namespace to describe what a namespace contains:

Procedure

1. Navigate to **EM** > **Tools** > **Media Management**.
2. On the Media Management page, select the check box next to the namespace you want to rename.
3. Click **Rename**.
4. On the Rename Content Namespace page, type a unique name for the new namespace in the **Name** field.

   The name cannot begin with the at (@) symbol, must be less than 128 characters, must not be case-sensitive, and must not contain spaces or any of the following symbols:

   { } ' * \

5. Click **Save**.

Deleting a content namespace

About this task

Perform the following procedure to remove a content namespace from the system:

Procedure

1. Navigate to **EM** > **Tools** > **Media Management**.
2. On the Media Management page, select the check box next to the namespace you want to delete.
3. Click **Delete**.
4. In the **Delete Content Namespace** dialog box, click **Confirm**.

Viewing namespace content

About this task

Perform the following procedure to select a content namespace that you want to manage or browse.

Procedure

1. Navigate to **EM** > **Tools** > **Media Management**.
2. On the Media Management page, select the check box next to the namespace that you want to manage or browse.
3. Click **Browse**.
4. On the Provision Media page, in the left pane, select the namespace.

   Navigate the namespace using the plus sign (+) and minus sign (-) to expand and hide the content.

Adding a content group

About this task

Perform the following procedure to add content groups and to organize the media in a content namespace into logical groups:

Before you begin

Ensure that you have an existing namespace on the system.

Procedure

1. Navigate to **EM** > **Tools** > **Media Management**.
2. On the Media Management page, select the check box next to the namespace in which you want to add a new content group.
3. Click **Browse**.
4. On the Provision Media page, in the left pane, select the name of the content namespace in which you want to add a new content group.

   If applicable, navigate to a content group and click the content group to which you want to add the sub content group.
5. Click **Add Content Group**.
6. In the **Name** field of the **New Content Group** dialog box, type a name for the new content group.

   Important:

   The name cannot begin with the at (@) symbol, must be less than 128 characters, must not be case-sensitive, and must not contain spaces or any of the following symbols:

{ } ' * \

Tip:

You can use the forward slash (/) delimiter to specify sub-content groups in the tree structure. For example, typing `music/rock` in the **Name** field creates a `music` content group, with a sub-content group called `rock`, all in one step.

7. Click **Save**.

Adding media files to a content group

About this task

Perform the following procedure to add media files to a content group, by uploading one media file at a time:

Note:

Many browsers have a 2GB limit for file uploads.

Note:

Avaya recommends that audio to be played by Avaya Aura® MS be encoded as 16 bit, 8 kHz, single channel, PCM files. Codecs other than PCM or using higher sampling rates for higher quality recordings can be used, however, with reduced system performance. Multiple channels, like stereo, are not supported.

Before you begin

Ensure that you have an existing namespace and content group on the system.

Ensure that the file to be uploaded is on the same system that is running the web browser you are using to navigate EM.

Procedure

1. Using a browser on the same computer where your file resides, navigate to **EM** > **Tools** > **Media Management**.
2. On the Media Management page, select the check box next to the namespace to which you want to add a media file.
3. Click **Browse**.
4. On the Provision Media page, select the content group to which you want to add a media file.
5. Click **Add Media**.
6. In the **Add Media** dialog box, click **Browse** and navigate to the media file you want to upload.
7. Select **Always overwrite files with the same name** or **Do not overwrite files with the same name**.
8. To remove the extension from the filename, select **Cut extension**.

The system keeps the actual file extension. The **Cut extension** option removes the extension from the content ID display name.

9. To use a different name for the media file that is uploaded, enter a new name in the **New Name** field.
10. Click **Upload**.

Downloading media files to your computer

About this task

Perform the following procedure to download a media file stored on the media server to your computer:

Procedure

1. Using a browser on the computer where you want to download the file to, navigate to **EM** > **Tools** > **Media Management**.
2. On the Media Management page, select the check box next to the namespace that contains the media file you want to download.
3. Click **Browse**.
4. On the Provision Media page, select the content group that contains the media file you want to download.
5. In the **Name** column in the right pane, select the media file you want to download.
6. Right-click the file, and select **Download**, or use the **More Actions** drop-down menu, and select **Download**.
7. In the **Download Media** dialog box, click **Download**.

   The system displays a download window.
8. Click **Save**.

   The procedure to save the file varies depending on the Web browser you use.

Renaming a content group

About this task

Perform the following procedure to rename a content group:

Procedure

1. Navigate to **EM** > **Tools** > **Media Management**.
2. On the Media Management page, select the check box next to the namespace that contains the content group you want to rename.
3. Click **Browse**.
4. On the Provision Media page in the left pane, click the plus sign (+) next to the namespace.

5. Select the content group that you want to rename.
6. Right-click the content group and select **Rename** or use the **More Actions** drop-down menu and select **Rename**.
7. In the **New Name** field of the **Rename Content Group** dialog box, type a name for the new content group.

   Important:

   The name cannot begin with the at (@) symbol, must be less than 128 characters, must not be case-sensitive, and must not contain spaces or any of the following symbols:

   { } ' * \
8. Click **Save**.

Deleting a content group

About this task

Perform the following procedure to remove a content group from the system:

Procedure

1. Navigate to **EM** > **Tools** > **Media Management**.
2. On the Media Management page, select the check box next to the namespace that contains the content group you want to delete.
3. Click **Browse**.
4. On the Provision Media page, in the left pane, click the plus sign (+) next to the namespace containing the content group you want to delete.
5. Select the content group that you want to delete.
6. Click the **Delete** or right-click on the content group and select **Delete**.
7. In the **Confirm Content Group Delete** dialog box, click **Confirm**.

Batch provision media

Perform the following procedures to batch provision media for a content namespace by using a zip file that you create and upload.

Related links

Creating the zip file on page 160
Uploading media archived in a zip file on page 161

Creating the zip file

About this task

Perform the following procedure to create a proper file structure on your local system for the zipped files:

Important:

When creating the zip file, keep these naming restrictions in mind:

- The namespace and content group names cannot begin with the at (@) symbol, must be less than 128 characters, must not be case-sensitive, and must not contain spaces or any of the following symbols: { } ' * \
- The media file names must be less than 128 characters, are case-sensitive, and must not contain any of the following symbols: { } ' * \

Note:

Many browsers have a 2GB limit for file uploads.

Note:

Avaya recommends that audio to be played by Avaya Aura® MSbe encoded as 16 bit, 8 kHz, single channel, PCM files. Codecs other than PCM or using higher sampling rates for higher quality recordings can be used, however, with reduced system performance. Multiple channels, like stereo, are not supported.

Before you begin

Ensure that you have already created a namespace to contain the new media files and know the name of that namespace.

Procedure

1. Select a target namespace already configured on Avaya Aura® MS, for example, *MyNamespace*.
2. Create a directory on your system with the same name as the target content namespace name.

   The directory that you create is the root directory for your zip archive.
3. Create subdirectories in the namespace directory.

   Subdirectories represent the content groups that the system creates in the target namespace. The file structure in the uploaded zip file must match the namespace and content group structure that you want on Avaya Aura® MS.

   If the structure is not as described in the example, the upload fails.

   For example, to upload media zip files to a namespace called MyNameSpace with a content group called MyContentGroup, the zip file structure must be as follows:

```
MyNameSpace\MyContentGroup\MyMediaFile1.wav
MyNameSpace\MyContentGroup\MyMediaFile2.wav
MyNameSpace\MyContentGroup\MyMediaFileX.wav
```

4. Follow the instructions of the zip archiving tool to zip up the entire MyNameSpace directory.

Uploading media archived in a zip file

About this task

Perform the following procedure to batch provision media files on Avaya Aura® MS by using a zip archive.

Before you begin

Ensure that you have a properly constructed zip file that contains the media files to be uploaded.

Procedure

1. Using a browser on the same computer where your zip file resides, navigate to **EM** > **Tools** > **Media Management**.
2. On the Media Management page, select the check box next to the namespace to which you want to add media files.
3. Click **Browse**.
4. On the Provision Media page, right-click the content namespace and select **Batch File Provision**. Alternatively, you can select **Batch File Provision** on the **More Actions** drop-down menu.
5. In the **Batch File Provision** dialog box, click **Browse** to navigate to the zip file to upload.
6. Select **Always overwrite files with the same name** or **Do not overwrite files with the same name**.
7. To remove the extension from the filenames, select **Cut extension**.
8. Click **Upload**.
9. Verify that the media is uploaded by browsing the namespace and content groups with the Media Management tool.

Searching for a media file

About this task

Perform the following procedure to search for a stored media file on the system:

Procedure

1. Navigate to **EM** > **Tools** > **Media Management**.
2. On the Media Management page, select the check box next to the namespace that you want to search.
3. Click **Browse**.
4. On the Provision Media page, click **Search** in the upper-right corner.
5. In the **File Name** field, type the full or partial name of the content that you want to find.

6. In the **Search In Content Group** list, select the name of the content group in which you want to search for media files.
7. Click **Search**.

   The system displays matching results.
8. To perform media file operations, select the content and right-click to select the required operation. You can also use the **More Actions** drop-down menu and select the required operation.

Renaming a media file

About this task

Perform the following procedure to rename a media file:

Procedure

1. Navigation to **EM** > **Tools** > **Media Management**.
2. On the Media Management page, select the check box next to the namespace that contains the content to be renamed.
3. Click **Browse**.
4. To locate the content to be removed, use the left pane of the **Provision Media** page to navigate the namespace and content groups.

   Use the plus sign (+) and the minus sign (–) to expand and hide the content as needed. Alternatively, you can click **Search** in the upper-right corner of the page.
5. After you locate the file on the page, right-click the content name, and select **Rename**. You can also use the **More Actions** drop-down menu and select **Rename**.
6. In the **Rename Media** dialog box, type a new name for the file in the **New Name** field.

   Tip:

   The name must be less than 128 characters, is case-sensitive and must not contain any of the following symbols: { } ' * \
7. Click **Save**.

Moving a media file

About this task

Perform the following procedure to move a media file to another content group:

Procedure

1. Navigate to **EM** > **Tools** > **Media Management**.
2. On the Media Management page, select the check box next to the namespace that contains the content to be moved.

3. Click **Browse**.
4. To locate the content to be moved, use the left pane of the Provision Media page to navigate the namespace and content groups.

   Use the plus sign (+) and the minus sign (-) to expand and hide the content as needed.
5. After you locate the file you want to move, right-click the content name and select **Cut**. You can also use the **More Actions** drop-down menu and select **Cut**.
6. In the left pane, navigate to the new content group.
7. Right-click on the new content group and select **Paste** from the menu or use the **More Actions** drop-down menu and select **Paste**.

Copying a media file

About this task

You can duplicate media content within the same content group or duplicate the media content to a different content group. The system creates the copy with the name `Copy of filename`. You must give the file an appropriate name using the rename procedure.

Procedure

1. Navigate to **EM** > **Tools** > **Media Management**.
2. On the Media Management page, select the check box next to the namespace that contains the content to be copied.
3. Click **Browse**.
4. In the left pane of the Provision Media page, navigate the namespace and content groups to locate the content to be copied.

   Use the plus sign (+) and the minus sign (-) to expand and hide the content as needed.
5. After you locate the file to be copied, right-click the content name and select **Copy** or use the **More Actions** drop-down menu and select **Copy**.
6. In the left pane, navigate to the content group where you want to copy the media file.
7. Right-click on the content group and select **Paste** from the menu or use the **More Actions** drop-down menu and select **Paste**.
8. To rename the copied file, right-click the new copy of the file with `Copy of filename` format and select **Rename** from the menu. You can also use the **More Actions** drop-down menu and select **Rename**.

Deleting a media file

About this task

Perform the following procedure to remove a media file from the system:

Procedure

1. Navigate to **EM** > **Tools** > **Media Management**.
2. On the Media Management page, select the check box next to the namespace that contains the media file you want to delete.
3. Click **Browse**.
4. To locate the content that is to be removed, in the left pane of the Provision Media page, navigate the namespace and content groups.

   Use the plus sign (+) and the minus sign (-) to expand and hide the content. Alternatively, you can click **Search** in the upper-right corner.
5. Select the content item that you want to remove and click **Delete** or right-click on the content item and select **Delete**.
6. In the **Confirm Media Delete** dialog box, click **Confirm**.

Chapter 8: Application management

Enabling the VoiceXML interpreter

About this task

By default, the VoiceXML application interpreter is disabled on Avaya Aura® Media Server (MS).

Perform the following procedure to enable the VoiceXML interpreter.

Procedure

1. Navigate to **EM** > **System Configuration** > **Server Profile** > **General Settings** > **Server Function**.
2. Select **VoiceXML Interpreter**.
3. Click **Save**.

Adding VoiceXML custom applications

About this task

In addition to packaged applications, you can define custom VoiceXML applications on Avaya Aura® MS.

Perform the following procedure to add a custom application and the SIP translations for the custom application:

Before you begin

Ensure that you have enabled the VoiceXML interpreter.

Procedure

1. Navigate to **EM** > **Applications** > **Custom Applications**.
2. Click **Add...**
3. Select **URL** for the **Application Type**.
4. Enter a name for your application in the **Application Name** field.
5. In the **URL** field, specify the URL which each incoming call fetches.
6. Select the **Initial Interpreter Type** as **VoiceXML**.

7. (Optional) Select **Add SIP Translation** to specify the SIP translation **Mode**, **Algorithm**, **Pattern**, and **Rank** for this application. You can configure the SIP translation later.

   Note:

   Sip Account Association is currently not used.

8. Click **Save**.

Editing VoiceXML custom applications

About this task

Perform the following procedure to edit an existing custom application:

Procedure

1. Navigate to **EM** > **Applications** > **Custom Applications**.
2. Click on the name of the application you want to edit, or select the check box next to the application and click **Edit…**
3. On the **Edit Custom Application** page, alter the fields for this application.

   Note:

   Sip Account Association is currently not used.

4. Click **Save**.

Application interpreter configuration

Configuring RFC5707 (MSML) interpreter

About this task

Perform the following procedure to configure the RFC5707 Media Server Markup Language (MSML) settings:

Procedure

1. Navigate to **EM** > **System Configuration** > **Application Interpreters** > **RFC5707 (MSML)** > **General Settings**.
2. Select **MSML Video Capability Negotiation** to enable video negotiation if offered by the SIP client endpoints.
3. Select **MSML HA Event Notification** to enable MSML event notification when failover occur in High Availability mode.

4. Enter the default announcement namespace in the **MSML Default Namespace** field.
5. Click **Save**.
6. Restart Avaya Aura® MS for the changes to take effect.

Configuring VoiceXML interpreter

About this task

Perform the following procedure to configure the Voice Markup Language (VoiceXML) default interpreter settings:

If the application defines the settings, then you do not need to change the default VoiceXML settings.

Procedure

1. Navigate to **EM** > **System Configuration** > **Application Interpreters** > **VoiceXML** > **General Settings**.
2. Alter the fields to change the default functionality for VoiceXML applications.
3. Click **Save**.
4. Restart Avaya Aura® MS for the changes to take effect.

Viewing or changing application operational state

About this task

Perform the following procedure to manage the operational state of installed applications:

Procedure

1. Navigate to **EM** > **Applications** > **Operational State**.
2. You can view the current state of each listed application in the **State** column.
3. To change application states, select the check box next to one or more listed applications and then click **Lock**, **Unlock**, or **Pending Lock**.

Viewing or changing custom application operational state

About this task

Perform the following procedure to manage the operational state of custom applications:

Procedure

1. Navigate to **EM** > **Applications** > **Custom Applications**.

2. You can view the current state of each listed application in the **State** column.
3. To change application states, select the check box next to one or more listed applications. Then select **Lock**, **Unlock**, or **Pending Lock** from the **More Actions** drop-down menu.

Configuring application signaling translations

About this task

Application signaling translations map incoming SIP INVITE requests to an application. Then the system invokes the application.

The system performs translations by using the configured comparison **Algorithm** to match a configured string **Pattern**. The configured **Mode** determines where in the SIP INVITE the system looks for the pattern.

If the **Pattern** field contains the same value for multiple translations, then the system uses the **Rank** of the translation to determine which application to invoke. Translations with the same **Pattern** must not be configured with the same **Rank**.

Perform the following procedure to add or modify application signaling translations.

Use the following tables as aids for configuring the translations:

Definitions for mode options	
Option	**Description**
None	Translations fail if **Mode** is set to `None`. The system responds with 404 Not Found.
SIP request URI	Translations use the entire Request URI, including arguments, from the SIP INVITE.
Called DN	Translations use the directory number of the called user. The system uses the SIP INVITE To header, excluding arguments, as the called DN.
Calling DN	Translations use the directory number of the user making the call. The system uses the SIP INVITE From header, excluding arguments, as the calling DN.
SIP request URI user	Translations use the user name found before the server address in the request URI of the SIP INVITE.
SIP To	Translations use the To header from the SIP INVITE.
SIP From	Translations use the From header from the SIP INVITE.

Definitions for algorithm options	
Option	**Description**
None	Translations fail if **Algorithm** is set to `None`. The system responds with 404 Not Found.
Substring Match	For successful translation to the application, the string specified by **Mode** must contain the string specified by **Pattern**.

Table continues…

Definitions for algorithm options	
Option	**Description**
Regular Expression	For successful translation to the application, the string specified by **Mode** must match the regular expression specified in **Pattern**. A regular expression (regexp) is a syntax consisting of a sequence of literal characters and metacharacters that forms a match pattern. Avaya Aura® MS supports regexp V8 syntax.
Exact Match	For successful translation to the application, the string specified by **Mode** must exactly match the string specified by **Pattern**.
Case-Insensitive Match	For successful translation to the application, the string specified by **Mode** must match the string specified by **Pattern**. The system does not consider case in the comparison.
Dial Plan Notation	For successful translation to the application, the string specified by **Mode** must match the dial plan expression specified by **Pattern**. The x character is the wild card match character in the dial plan notation. The x can be upper or lower case. Instead of using the wild card character, explicitly include characters that must exactly match, in the required position of the pattern. Examples: An example emergency dial plan pattern is 911. If a user dials 911, then the system translates to the emergency application. An example extension dial plan contains four digits and is represented as xxxx. If a user dials any four digits or letters, for example, 3512, then translations complete successfully. Dialing only three digits would not match this dial plan. A dial plan can contain a combination of explicit letters and wild card characters. For example, 972XXXXXX. Any ten digit number starting with 972 matches the dial plan and translates successfully.

Procedure

1. Navigate to **EM** > **Applications** > **Signaling Translations**.
2. Click **Add...** to create a new translation, or select an existing translation from the list and click **Edit…**
3. Select an existing application for **Application name**.
4. Select the translation **Mode**.
5. Select an **Algorithm** from the options.
6. Specify a match pattern in the **Pattern** field.
7. Enter a translation **Rank**.

   The lower the number, the higher the priority of the translation.
8. Click **Save**.

Deleting application signaling translations

About this task

Perform the following procedure to remove defined translation from the application translations listed on the **Signaling Translations** page:

Procedure

1. Navigate to **EM** > **Applications** > **Signaling Translations**.
2. Select one or more translations from the list and click **Delete**.

Deleting a custom application

About this task

Perform the following procedure to remove a custom application from the system:

Before you begin

Lock custom applications before deleting them.

Procedure

1. Navigate to **EM** > **Applications** > **Custom Applications**.
2. Select the check box next to one or more listed applications that you want to delete.
3. Select **More Actions** > **Delete**.

Chapter 9: Backup and restore

Backup and restore overview

Avaya Aura® Media Server (MS) can backup and restore system configuration data and application content stored in Content Store. You must maintain backups of your system to recover from hardware failure or to restore data to a previous point in time.

Using Element Manager (EM), you can define, manage, and schedule backup and restore tasks. Use the Avaya Aura® MS command line backup and restore tool when you use a management interface other than Avaya Aura® MS EM.

Important:

- Storing the backup file locally on the same disk does not protect data from disk drive failure.
- If you reimage your system or replace the disk drive, you must preserve the backup file in a safe location. This is required, if you have stored the backup file on the disk being replaced. Preserving the backup file ensures the backup is available for you to restore or upgrade the Avaya Aura® MS system
- Backup data is not portable from one server to another. If you need to replace a server, you must configure the server with the same IP address and hostname so that the data is compatible. See Server replacement in *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS*.

Configuring a backup task

About this task

EM organizes backups as tasks. These tasks contain your selected backup options and specify the location where the backup is stored.

You can create an automated backup task to create backups daily, weekly, monthly or at one particular time. You can store the backup in a local destination directory. Alternatively, you can push the backup file to a remote server by using File Transfer Protocol (FTP) or SFTP (Secure File Transfer Protocol).

You cannot change the predefined local Default Backup Destination. If the administrator chooses to create a backup using this destination, EM stores the backup files in the following predefined local directory on Avaya Aura® MS.

`$MASHOME/platdata/EAM/Backups`

You can configure remote backup destinations and these destinations can be shared by multiple backup tasks. When you perform backups to remote destinations, EM uploads the backup files to the specified FTP or SFTP server. If required, EM deletes the local backup file from Avaya Aura® MS after the file transfer completes.

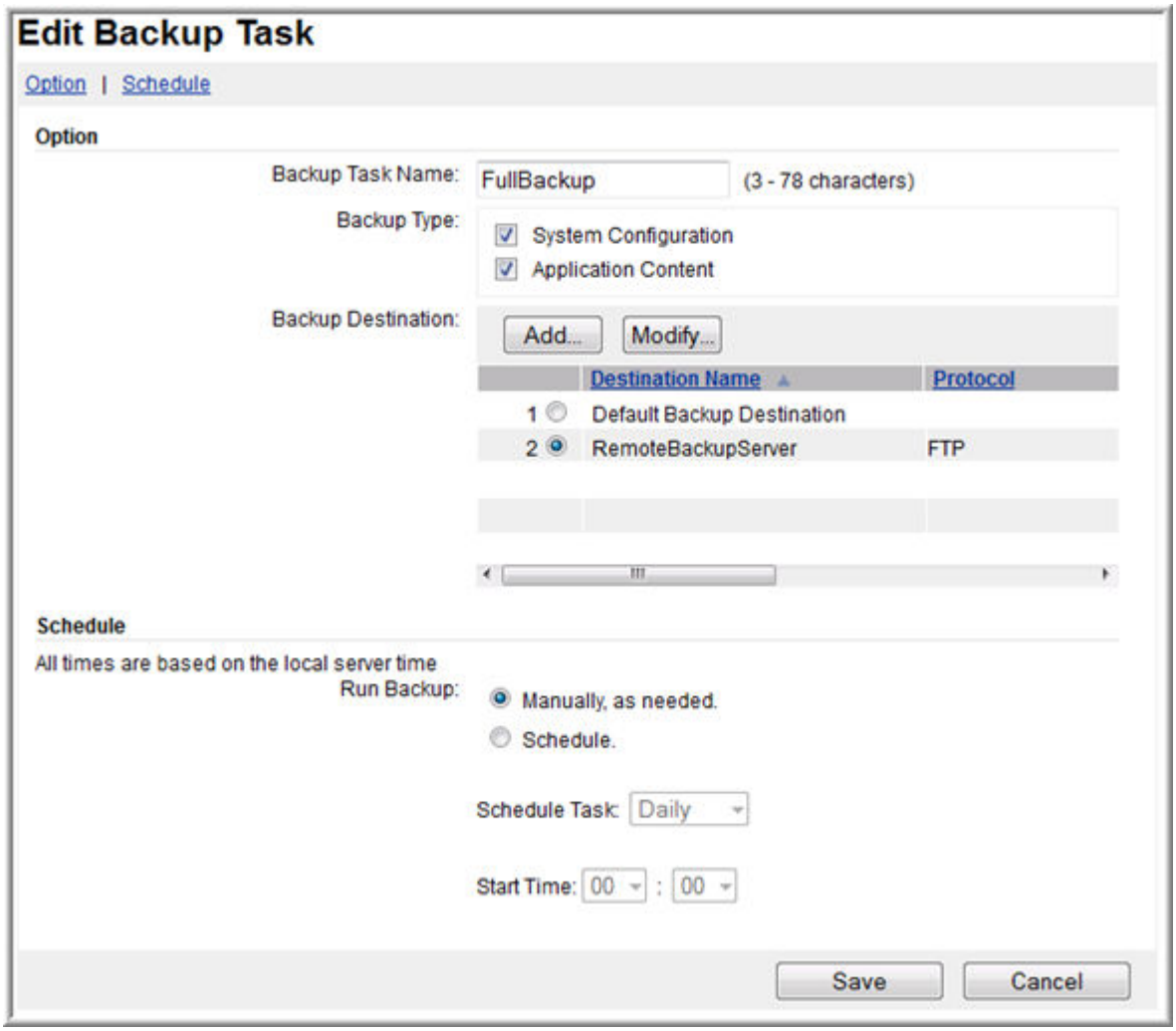
There are two types of content that you can include in the backups: System Configuration and Application Content. You can create one task for both the backup types or create separate tasks, each with independent schedules. Each backup type contains the following information:

Type of content	Description
System Configuration	Contains all the Avaya Aura® MS system settings that the Avaya Aura® MS management system has configured. For example, the settings you configure with the EM.
Application Content	Includes data that the Avaya Aura® MS Content Store manages. The data can either be the data that the applications generate or subscribers save. Examples of these data include, application prompts, subscriber preferences for a conferencing service or deposited recordings and user preferences for a service. The backup type does not include files stored on Avaya Aura® MS which are not stored in Content Store.

Perform the following procedure to define or update backup tasks and destinations using EM:

Procedure

1. Navigate to **EM** > **Tools** > **Backup and Restore** > **Backup Tasks**.
2. To create a new backup task either click **Add** or select an existing task from the list and click **Edit**.



3. Enter a name without spaces for this backup task in the **Backup Task Name** field.
4. For a complete backup, select both **System Configuration** and **Application Content** backup types.
5. Configure the destination for your backup files by selecting one of the following options:
   - Select the **Default Backup Destination** to store the backup on the local disk.

     This option does not protect your system from Avaya Aura® MS disk drive failure.
   - Select **Add...** to define a new remote FTP or SFTP location for your backup file.
   - Select an existing destination and click **Modify...** to alter the remote FTP or SFTP properties.

   For SFTP configuration, the **Secure FTP Remote Server Fingerprint** field can be set in MD5 or Base64 format.

Both the formats are supported by PuTTY tool which is used to perform the SFTP.

- MD5 based key fingerprint based on PuTTY's display form (sixteen 2-digit hex numbers separated by a colon)
- Base64 encoded blob describing SSH-2 public key in OpenSSH's public key format

Base64 can be obtained using the following command (note than you need to replace IP with hostname or IP of your backup server).

```
cust@someserver ~]$ ssh-keyscan 192.168.127.53 2>/dev/null
# 192.168.127.53:22 SSH-2.0-OpenSSH_7.4
192.168.127.53 ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCrC1oA7jRu1qQ/
9FFkEI0VIdeSJq9QRH1dsLwm1Veo0sEULHBUJYTT8TGU5B/
mnk4Zmkav8O6H9IZi7hDuexq0PHFTuNjUKHnvlmVirt/
4W+rWmSIgLwLXJonQA9tlYqC28CfDFOLIp+ajUTWa1Lu2PoZvthGdiAgJKpBLqnXE9F+
PY3jkZkrxdOzV+VC7S8p0wa3YPfj1/
I4CnFvBbZDRCz3587GQFv8CeCkTKPkaNk9MoNCrqDxdhxcg+wlaKPW21gyThdXrn6bILzaEaM/
C9q2NZ6+rSkqY0TvNHQ3wLZTZkxg0btX+kR9grv+en/TJq6/s9Y/YeW3YIHebVxsX
# 192.168.127.53:22 SSH-2.0-OpenSSH_7.4
192.168.127.53 ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCzzPykTVYjYmdQjYM1JTPmq1hdGpT
oHlAk1lTgB4QGxxykEbVZdUgP2lXdWooKgz1qmZ7jnuGD+QyMSJN/+aVU=
# 192.168.127.53:22 SSH-2.0-OpenSSH_7.4
192.168.127.53 ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIA1kZVjNDMvODdKITolT5KUbA3hJlgc6X9BiLHRDWZbL
```

The MD5 can be obtained using the following command.

```
[cust@someserver ~]$ ssh-keygen -l -E md5 -f <(ssh-keyscan
192.168.127.53 2>/dev/null)
2048 MD5:9a:71:b9:79:10:27:b1:a3:cb:66:c6:98:13:67:14:3f 192.168.127.53 (RSA)
256 MD5:5b:04:06:fa:07:60:9d:b9:d9:53:cc:11:95:2a:2a:5e 192.168.127.53 (ECDSA)
256 MD5:e0:4d:31:a4:22:71:d8:9b:17:34:87:40:d3:fc:5f:15 192.168.127.53 (ED25519)
```

When FIPS is enabled on Avaya Aura® MS, MD5 hash cannot be calculated. However, Base64 can be retrieved and used always.

Crypto algorithm needs to be selected according to the following PuTTY priority list: ED25519, ECDSA, RSA, DSA. In the above example, we use ED25519 and value marked as bold for the fingerprint field.

For example, if backup server is configured to use only DSA and RSA, use RSA as it has higher priority for PuTTY.

6. If you choose to add or modify a backup destination, then fill in the **Backup Destination Properties**:
   a. Enter the server properties in the fields.
   b. Check that path exists on the backup server and has write permissions for user specified in the properties.
   c. If you select FTP, click **Test** to verify whether your configuration can contact the server.
   d. Click **Save**.
7. Select either **Manually**, **as needed**, or **Schedule** depending on how you want the backup to run.

8. If you selected **Schedule**, then configure the **Schedule Task** either as Daily, Weekly, Monthly, or Once, and the date and time.
9. Click **Save**.

   The new backup task is included in the list of Backup Tasks.

Running a backup task

About this task

Perform the following procedure to manually run a defined backup task.

Procedure

1. Navigate to **EM** > **Tools** > **Backup and Restore** > **Backup Tasks**.
2. Select the check box next to the required backup task in the list.
3. Click **Run Now**.
4. Click **Confirm** to execute the backup task.

   Note:

   The time required to complete the application content backup depends on the amount of application data.
5. Monitor the Backup and Restore History Log at **Tools** > **Backup and Restore** > **History Log**.

   After the backup is complete, the log shows a completed backup task entry.
6. Confirm whether the backup files were saved to the FTP or SFTP location or local default destination. If the backup files are saved to the local destination, the local backups are found in the following directory:

   `$MASHOME/platdata/EAM/Backups`

Deleting a backup task

About this task

Perform the following procedure to remove a defined backup task:

Procedure

1. Navigate to **EM** > **Tools** > **Backup and Restore** > **Backup Tasks**.
2. Select the check box next to the backup task in the list.

3. Click **Delete**.
4. Click **Confirm** to remove the backup task.

Adding or editing a backup destination

About this task

Perform the following procedure to add or edit an existing backup destination to alter the FTP or SFTP settings for storing backup files.

Procedure

1. Navigate to **EM** > **Tools** > **Backup and Restore** > **Backup Destinations**.
2. Do one of the following:
   - If you want to add a new destination, click **Add**.
   - If you want to change an existing destination, either click on the name of the backup destination, or select it using the checkbox located next to the name of backup destination, and click **Edit**.
3. Modify the fields on the **Backup Destination Properties** page. For more information, see Configuring a backup task on page 171.
4. For FTP, click **Test** to verify if your configuration can contact the server.
5. For SFTP, configure only **Secure FTP Remote Server Fingerprint** field, and leave the **Secure FTP Key File Name** field blank.
6. Click **Save**.

Restoring from the local destination

About this task

Perform the following procedure to reconstruct data on Avaya Aura® MS by restoring data using a backup saved in the default backup destination:

The local backups that you can choose from are stored in:

```
$MASHOME/platdata/EAM/Backups
```

Procedure

1. Navigate to **EM** > **Tools** > **Backup and Restore** > **Restore**.

2. On the **Restore** page, in the **Restore Source** drop-down list, select **Default Backup Destination**.
3. In the **Restore Task List**, select the backups from the list which you want to use for the restore.

   Important:

   To ensure that the application data is restored to the configured location, restore the system configuration data before restoring the application data.
4. Click **Restore Now**.
5. On the **Confirm Restore** page, click **Confirm** to proceed with the restore.

   Important:

   Restoring a backup archive might impact running applications. After you click **Confirm**, the system invokes the restore task. EM and Avaya Aura® MS close the connections to all users until the system completes the restoration.

   Note:

   The time required to restore the application content depends on the amount of application data in the backup file.

Uploading a backup file for restore

About this task

Perform the following procedure to restore using an uploaded backup file to reconstruct data on your Avaya Aura® MS.

Important:

Backup data is not portable from one server to another. If you need to replace a server, you must configure the server with the same IP address and hostname so that the data is compatible. See Server replacement in *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS*.

Procedure

1. Navigate to **EM** > **Tools** > **Backup and Restore** > **Restore**.
2. On the **Restore** page, in the **Restore Source** drop-down list, select **Upload Backup Files**.
3. Click **Browse** to select the backup files.

   You can upload a System Configuration and Application Content backup at the same time.
4. On the **Confirm Restore** page, click **Confirm** to proceed with the restore.

Important:

Restoring a backup archive might impact running applications. After you click **Confirm**, the system invokes the restore task. EM and Avaya Aura® MS close the connections to all users until the system completes the restoration.

Note:

The time required to restore the application content depends on the amount of application data in the backup file.

Viewing the backup and restore history log

About this task

Each backup and restore operation, whether a success or a failure, is recorded in the backup and restore history log. You can use this log to see when the last backup and restore was executed. You can also use the log to verify when a manually executed backup or restore was completed. The logs also report the elapsed time and size of each executed task.

Perform the following procedure to view the backup and restore history log:

Procedure

1. Navigate to **EM** > **Tools** > **Backup and Restore** > **History Log**.
2. Use the **View** drop-down menu to select **All**, **Backup**, or **Restore** to filter the list of logs the system displays.
3. **(Optional)** Use the **Refresh Interval** to select the required update frequency of the logs, in case you are monitoring backup or restore for completion.
4. **(Optional)** Click **Export** to save the log history.
5. **(Optional)** Click **Clear** to delete the current log history.

Configuring the history log

About this task

Perform the following procedure to configure the number of days for saving backup files and restoring history logs on the server before the files or logs are automatically removed:

Procedure

1. Navigate to **EM** > **Tools** > **Backup and Restore** > **General Settings**.

2. Enter the number of days that you want to save backup and restore history log files on the server before the files are removed in the **Store history and log files for up to** field.
3. Click **Save**.

Using the command-line backup and restore tool

About this task

The command-line backup and restore tool backs up the same System Configuration and Application Content data as EM does when using task based system.

The executable file name is `backuprestore`. The following backup and restore tool description provides an overview of the options and the functionality.

Usage:

```
backuprestore <-b | -r> <filename> -t <taskid> [-ftp server user
password destpath [-d]] [-c]
```

```
backuprestore <-b | -r> <filename> -t <taskid> [-sftp server user
"serverfingerprint"] [-p pass] [-k severkey] [-dp destpath] [-d] [-c]
```

Backup Examples:

```
backuprestore -b /backup/SERVICE_DATA_HOSTNAME.zip -t service
```

```
backuprestore -b /backup/AMS_CONFIG_DATA_HOSTNAME.zip -t config -ftp
ftpserver1 anonymous 1234 /export/home/anonymous/ -d
```

Restore Example:

```
backuprestore -r /backup/CONFIG_DATA_HOSTNAME.zip
```

Important:

- Quotation marks must be used if there are spaces in the filenames.
- The order of the parameters is important. Follow the earlier examples.
- You must include the `.zip` extension in your filename.
- When creating a backup destination using the SFTP protocol, you must use one of the following authentication options:
  - A password and a fingerprint.
  - A fingerprint and a private key.

Backup and Restore tool options	
Option	**Description**
-h	Display the help message and more examples.

Table continues…

Backup and Restore tool options	
Option	**Description**
-b	Backup indicator followed by the *filename* to use for the backup. The filename must include the `.zip` extension.
-r	Restore indicator followed by the *filename* of the file to restore. The file must be an archive with the `.zip` extension
-t	Backup Task type: Defines what will be backed-up: `config` indicates System Configuration `service` indicates Application Content.
-ftp	Transfer the resulting backup file to an FTP destination. This is optional.

Table continues…

Backup and Restore tool options	
Option	**Description**
-sftp	Transfer the resulting backup file to an SFTP destination. The -sftp switch must be followed by the server address, username and fingerprint of the SFTP destination in quotes. This is optional. For example, `-sftp 10.0.12.23 sftpuser "ecdsa-sha2 nistp256 256 AAAAE2VjZHNhLXNoYTItbmIzdHAyNTYAAAAIbmIzdHAyNTYAAABBBGbVB+kh1TGWdgY+nxgW QSkh+OTDHhuU4eDE6apaoogGUvWTCROw6+vIQfipMbf4WAo2OObAObC+RU9dMX1G+Gc="` The fingerprint field is a combination of three space delimited tokens in the following format: <public key fromat> <key length> <host key text> PuTTY is used to perform the SFTP and supports the following formats for <host key text>: • MD5 based key fingerprint based on PuTTY's display form (sixteen 2-digit hex numbers separated by a colon) • Base64 encoded blob describing SSH-2 public key in OpenSSH's public key format The MD5 has can be obtained by SSH to the FTP server and issuing the following command. `[cust@someserver ~]$ ssh-keyscan localhost` `# localhost:22 SSH-2.0-OpenSSH_7.4` `localhost ssh-ed25519` `AAAAC3NzaC1IZDI1NTE5AAAAIH1w1UO0JWMJGNYnLePhVBP7XI/UjgMKVx1ACHvTIvI` `# localhost:22 SSH-2.0-OpenSSH_7.4` `localhost ssh-rsa` `AAAAB3NzaC1yc2EAAAADAQABAAABAQCnh9Tz5ZshgaTtz6fPtIZ9Ij7TGSqsPTEa4urhffqw 4W3QHvFz1UR8I8OjCVDtDhhqYDqELG5T8mKM/X6q2v0vb5EywB680jEO/ RL26YXPPDK3QCN+OeE75+RIwWXPkcKkkZdWHPFvBW3Y6IHEQ9i8GGJPNAMHFVwZ1q3YFmdd/ ttlmAtSa// X1mIzARLwPDqSupPk7VhFqdeyu9IqB9Fepay4IHeegxiWEx+mub6J1ko2sswg+D/ Aa9CCHKCrBs+ +tOJnCXTHIW0yIgiuVY35bDyklrgdxaJs6k4XhI8Hwoa6IkxH4hU3rVX2NtDsRPwatzO+gJH OiZLtsrAX7HrB` `# localhost:22 SSH-2.0-OpenSSH_7.4` `localhost ecdsa-sha2-nistp256` `AAAAE2VjZHNhLXNoYTItbmIzdHAyNTYAAAAIbmIzdHAyNTYAAABBBGbVB+kh1TGWdgY+nxgW QSkh+OTDHhuU4eDE6apaoogGUvWTCROw6+vIQfipMbf4WAo2OObAObC+RU9dMX1G+Gc=` Using the example above you would configure the following for **Secure FTP Remote Server Fingerprint** for ecdsa-sha2–nistp256 key type. `ecdsa-sha2-nistp256 256 AAAAE2VjZHNhLXNoYTItbmIzdHAyNTYAAAAIbmIzdHAyNTYAAABBBGbVB+kh1TGWdgY+nxgW QSkh+OTDHhuU4eDE6apaoogGUvWTCROw6+vIQfipMbf4WAo2OObAObC+RU9dMX1G+Gc=`

Table continues…

Backup and Restore tool options	
Option	**Description**
-p	Password for SFTP authentication. Use quotes around passwords containing special characters. Additionally, if the password contains a backslash (\) or a quote (") then each of these characters must be escaped by a preceding backslash (\). This is optional. For example, the password `12;;33\MS"pw` should be entered in quotes as follows: `"12;;33\\MS\"pw"` This is optional.
-k	Private key for SFTP server. This is optional.
-dp	Destination path for backup on the SFTP server. This is optional.
-d	Delete the local file upon successful ftp transfer or restore. This is optional.
-c	Direct output that is sent to the console instead of the debug file. This is optional.

Procedure

1. Stop Avaya Aura® MS.
2. Open a Linux® shell command prompt on Avaya Aura® MS.
3. Execute the **backuprestore** tool following the usage guidelines.

   For example:

   ```
   backuprestore -b backupfilename.zip -t config
   ```

   or

   ```
   backuprestore -r backupfilename.zip
   ```

   Important:

   To ensure that the application data is restored to the configured location, restore the system configuration data before restoring the application data.

   Note:

   The time required to complete the application content backup or restore depends on the amount of application data on the system.
4. Start Avaya Aura® MS.
5. If Avaya Aura® MS EM is installed, restart EM with the following command:

   ```
   /sbin/service avaya.em restart
   ```

Chapter 10: Avaya Aura® MS monitoring

Element Manager (EM) provides ways to monitor the processing status of Avaya Aura® MS. Administrators can view alarms, logs, protocol traces, and performance metrics of an individual element or an entire cluster using the available monitoring tasks.

In EM, the monitoring tasks are grouped under the System Status category in the left menu pane.

Element status viewing

The current operational status of a particular element, for example, the server you are administrating, is available on EM. For information on procedures to view and change the status of Avaya Aura® MS, see Chapter 5, Basic management tasks.

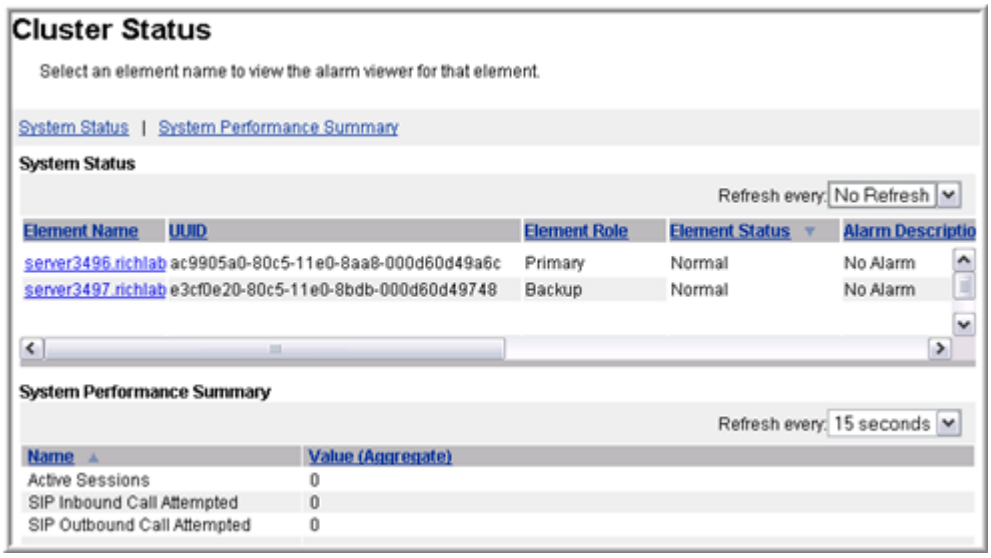
Viewing cluster status

About this task

The system displays the **Cluster Status** page with the operational state of the cluster and the member elements.

Procedure

1. Navigate to **EM** > **System Status** > **Cluster Status**.



2. Scroll through the **System Status** pane to view the columns and the status of each element.

   The **System Performance Summary** pane is present under the **System Status** pane. The **Key Performance Indicators** listed are an aggregate of all the cluster elements and represent the cluster as a whole.

   The **System Performance Summary** pane is available only on Primary servers and displays only the operational measurements that are configured as **Key Performance Indicators** (KPIs).

3. Click the **Element Name** of an individual element in the **System Status** pane.

   The system displays the detailed alarm information for that particular element.

Related links

Configuring OM settings on page 213

Monitoring alarms

About this task

Avaya Aura® MS generates an active alarm any time Avaya Aura® MS detects an operational error condition that requires corrective action by the administrator.

Avaya Aura® MS contains many individual system components that perform specific functions during operation. When a component detects an error condition the component raises an alarm. The component that raises the alarm automatically clears the alarm after the administrator resolves the error condition.

The system generates an event log each time a component raises or clears an alarm. The event log provides a clear record of all state changes on Avaya Aura® MS long after the error condition is resolved.

You can view the list of active alarms in the EM alarm viewer. The system updates the alarm viewer by using a refresh interval that you select.

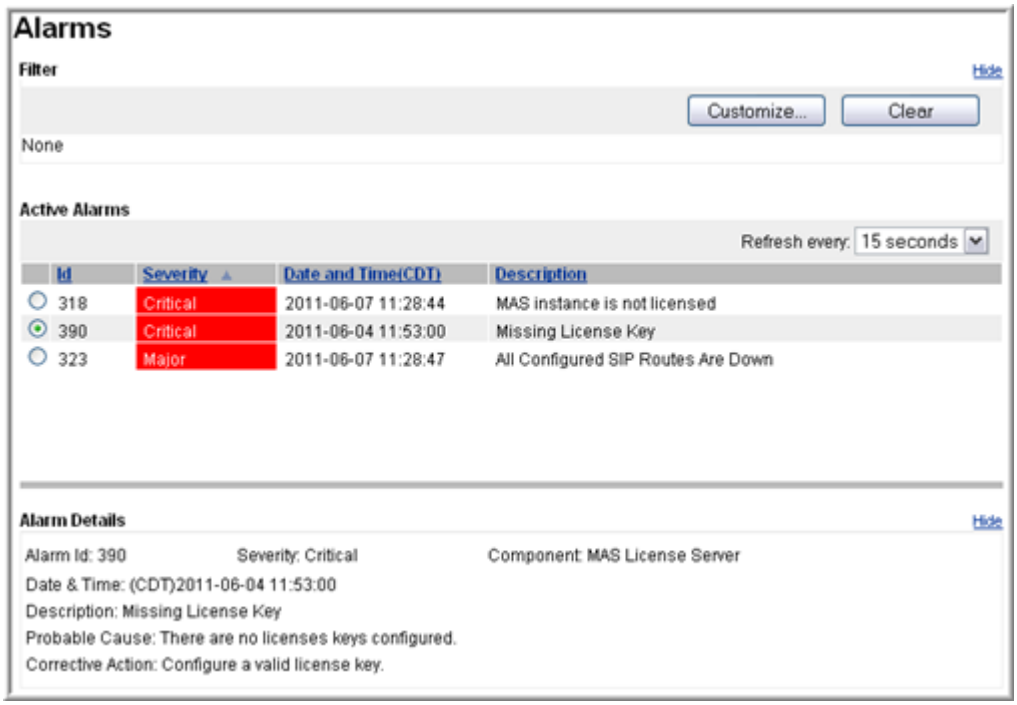
EM displays the following information for each alarm:

Alarm field descriptions	
Field	**Description**
ID	A unique identifier assigned to the alarm.
Severity	The severity rank of alarms from most severe to least severe is Critical, Major, Minor, and Warning.
Date and Time	The timestamp of the exact time the alarm is raised. You can configure timestamps to display as either local time or Universal Time Coordinated (UTC) time. UTC time can be useful for correlating alarms with events in other time zones.
Description	A description of the type of error condition encountered.
Component	The name of Avaya Aura® MS software component reporting the alarm.
Probable Cause	A description of the probable cause of this alarm.
Corrective Action	A suggested corrective action that can be performed to resolve the error condition.

Perform the following procedure to view the active alarms on Avaya Aura® MS:

Procedure

1. Navigate to **EM** > **System Status** > **Alarms**.
2. To set the alarm data refresh interval, use the **Refresh every** drop-down menu.



3. Select an alarm that is listed.

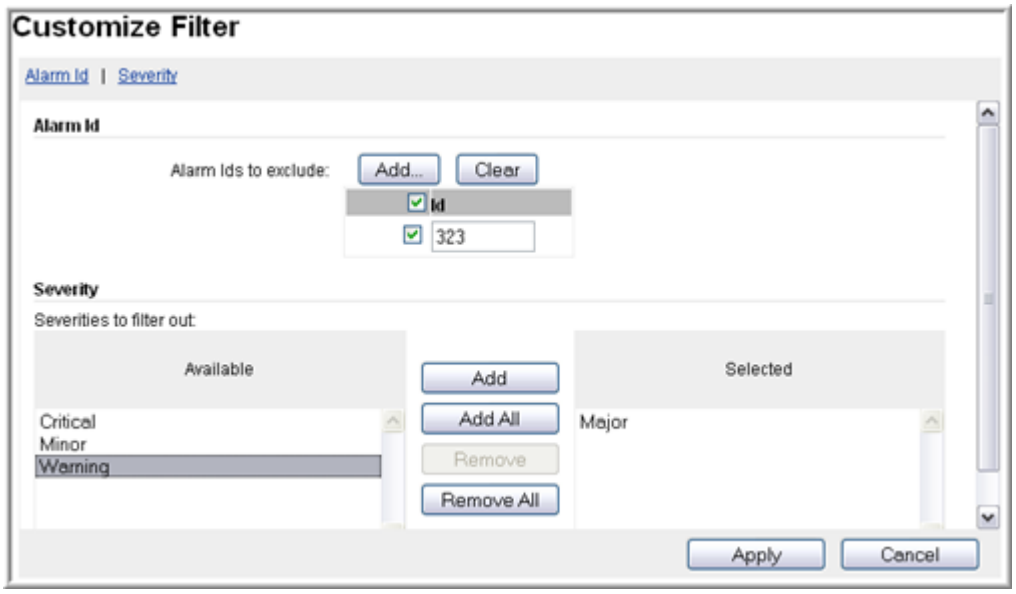
   The system displays the details at the bottom of the page.

   Use the vertical and horizontal scroll bars to view information.

4. Click one of the heading names, **Id**, **Severity**, **Date and Time**, or **Description**.

   The system sorts and displays alarms in ascending or descending order.

5. Click **Customize...** in the upper-right corner of the **Alarms** pane to create a filter for the displayed alarms.



6. On the **Customize Filter** page, select the **Alarm ID** and the **Severity** types to include, using the **Add** button.
7. Click **Apply** to return to the **Alarms** page with the filtered results.
8. To clear the applied filter, click **Clear** in the upper-right corner of the **Alarms** pane.

Event Logs

Event logs provide a historical view of events that occurred in the system.

If required, then you can configure Avaya Aura® MS to deliver event logs as SNMP traps or SysLog destinations. You need to perform the commissioning procedures for SNMP to deliver SNMP traps.

You can control the age of saved logs, enable or disable log throttling, and apply advanced filters based on log severity and class.

EM displays the following information for each alarm:

Event log field descriptions	
Field	**Description**
ID	A unique identifier assigned to the alarm.
Severity	The severity ranks events from most severe to least severe are as follows: Critical, Major, Minor, and Warning.
Origin	The name of the server reporting the event.

Table continues…

Event log field descriptions	
Field	**Description**
Date and Time	The timestamp of the exact time that the event is raised. You can configure timestamps to display as either local time or Universal Time Coordinated (UTC) time. UTC time can be useful for correlating alarms with events in other time zones.
Class	The type of information the log is reporting. Class values include Audit, Configuration, Data, Fault, Information, Maintenance, Metrics, Security, and State.
Category	Always reports a value of General in this release.
Instance Count	The number of times this event occurred when event throttling collects repeated events.
Description	Provides a summary of the type of error condition encountered.
Component	The name of Avaya Aura® MS software component reporting the alarm.
Probable Cause	A description of what probably caused this event to be raised.
Corrective Action	Suggested corrective action that can be used to resolve the error condition.
Application Id	The application reporting the event.
Customer Id	A custom value set by an application.
Document Reference Link	An optional link to documentation related to the event.

Viewing event logs

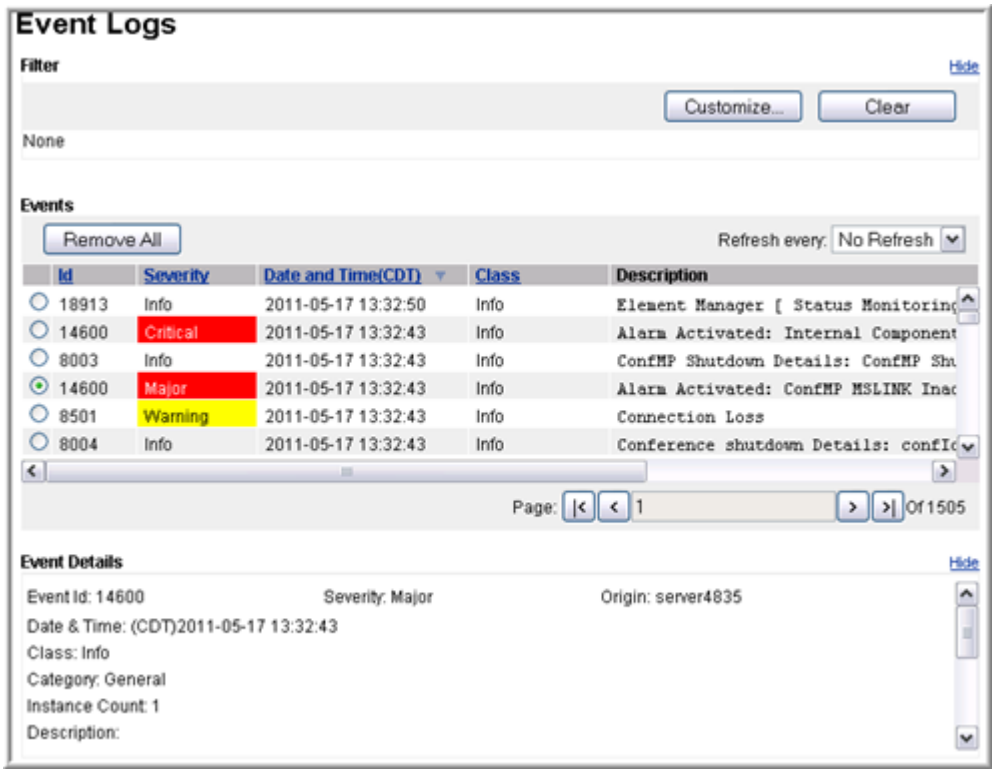
About this task

The Event Logs reflect system state and alarm transitions, error conditions and system operational details.

Perform the following procedure to gain access to the saved Avaya Aura® MS Event Logs:

Procedure

1. Navigate to **EM** > **System Status** > **Logs** > **Event Logs**.
2. To set the event data refresh interval, use the **Refresh every** drop-down menu.



3. Select an event that is listed.

   The system displays the details at the bottom of the page.

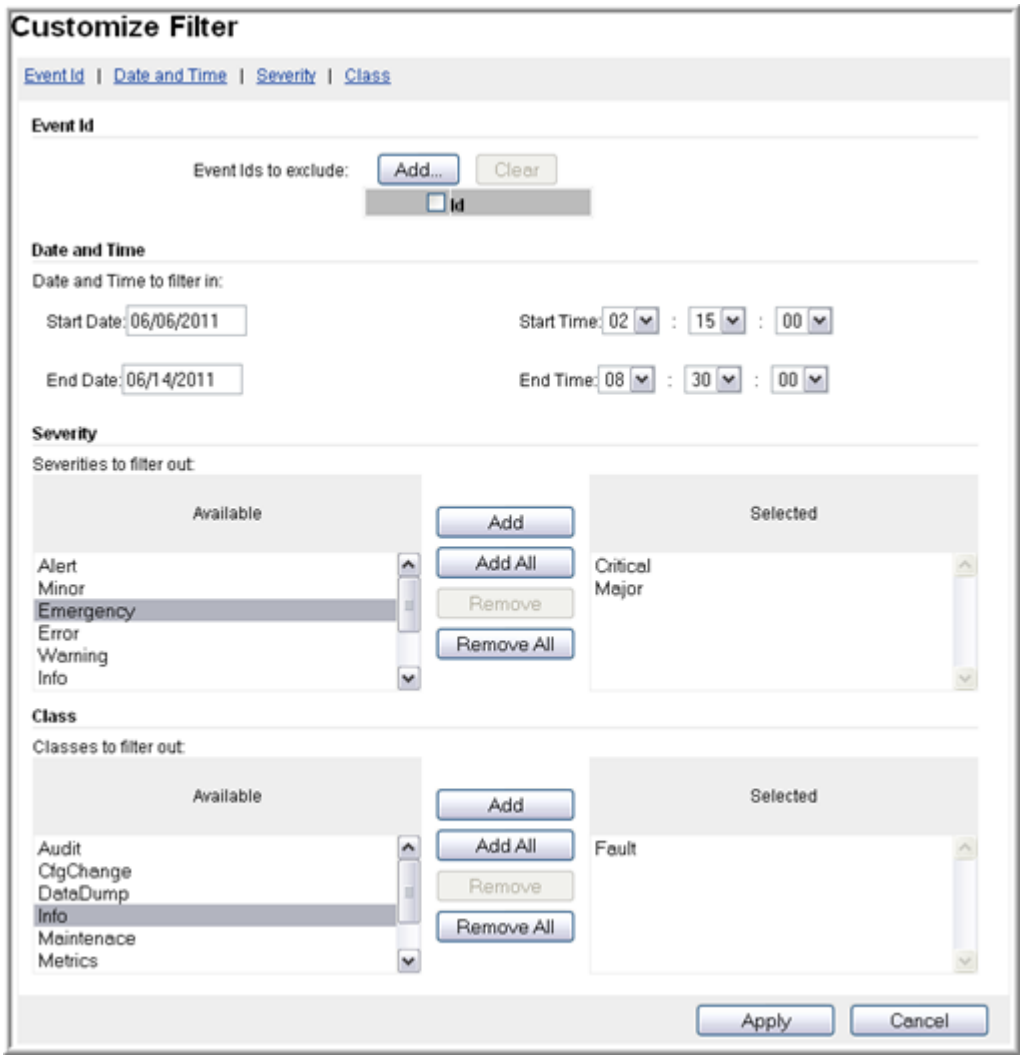
   Use the vertical and horizontal scroll bars to view the information.

4. Click on one of the heading names: **Id**, **Severity**, **Date and Time**, or **Description**.

   The system sorts and displays alarms in ascending or descending order.

5. To go back in the history of the Event Logs, use the **Page** navigation buttons.

6. Click **Customize…**, in the upper-right corner of the **Event Logs** page, to filter the logs which are displayed.



7. On the **Customize Filter** page, select the **Event Id**, **Date and Time**, **Severity**, and **Class** types to include, using the **Add** buttons.
8. Click **Apply** to return to the **Event Logs** page with the filtered results.
9. To clear the applied filter, click **Clear** in the upper-right corner of the **Event Logs** page.

Configuring event log throttling

About this task

You can enable and configure event log throttling for a particular event. When throttling is enabled, the system reports only the most recent event log and its contents. Log throttling prevents the event logs from being flooded with recurring identical events. When you enable throttling, the system generates an event log and its occurrence count at the end of the interval specified by **Event Log Throttle Check Window (Secs)**.

Procedure

1. Navigate to **EM** > **System Configuration** > **Monitoring Settings** > **Event Logs** > **General Settings**.
2. Select **Event Log Throttling** to enable log throttling for events.
3. Configure **Event Log Throttle Check Window (Secs)** to set the interval in seconds to audit the throttled logs.
4. Configure **Event Log Archive Minimum Log Age (Days)** to set the minimum time in days to keep an event log archive before the system deletes it.
5. Click **Save**.

Configuring log filter settings

About this task

Each log destination you configure on Avaya Aura® MS, whether SNMP, SysLog, or Archive, has filter settings which you can customize independently.

You can filter logs based on the severity and the class in which the logs are grouped, as described in the following tables.

Filter options by log class	
Event type	**Description**
Audit	Audit events provide notification of very specific actions within a managed device. In isolation, an audit event provides limited data. However, a collection of audit information forms an audit trail.
Security	A security event happens in the interest of security. A security event occurs in the interest of security. A security event is often combined with other classes such as fault and audit to form a record or notification.
Configuration Change	A configuration event, also known as an inventory event, is used to notify the system that hardware, software, or a service has been added, changed, or removed.
Fault	The system generates a fault notification after a fault condition occurs. A fault notification can result in an alarm.
State	A state includes both administrative states that can be manually configured and operational states that are read-only and determined by the managed entity.

Table continues…

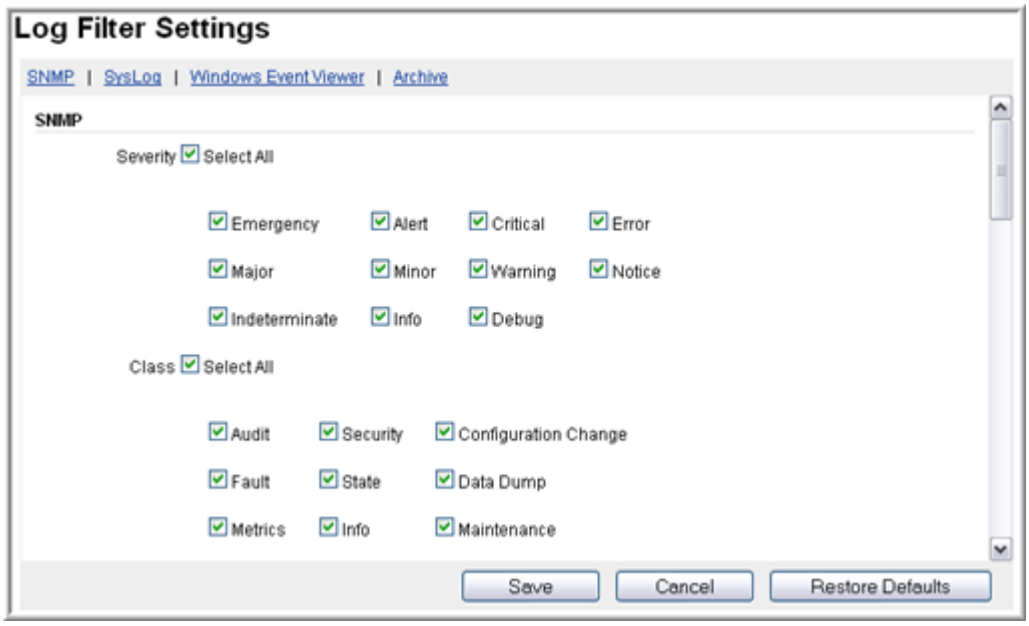
Filter options by log class	
Event type	**Description**
Data Dump	A data dump event is an asynchronous event that contains information about a system, such as the configuration and the state. The system generates these events as a result of a scheduled activity. Data dump events are not intended for a traditional poll-response type interaction.
Metrics	A metrics event contains a metric or a collection of metrics, including performance metrics, for an application, platform, or another device or network element. The record can be in a number of different formats, for example, XML, CSV.
Info	An event of interest which requires no action but can be used for troubleshooting purposes.
Maintenance	A maintenance event signals the beginning, process, or end of an action generated either by a manual or an automated maintenance action. Typically, the system reports the actual action initiation and the maintenance action.

Filter options by log severity	
Event type	**Description**
Emergency	An unusable system.
Alert	An action must be taken immediately.
Critical	An immediate corrective action that is required due to loss of service, loss of bandwidth, outage, and loss of data or functionality.
Error	An error condition has occurred.
Major	An urgent corrective action that is required due to a pending loss of service, outage, and loss of data or functionality.
Minor	A corrective action is required to prevent an eventual degeneration of services.
Warning	A potential or impending service-affecting condition that is detected that requires some diagnostic action.
Notice	A normal but significant condition.
Indeterminate	A service-affecting condition that is detected whose impact is unknown.
Info	Audit-type information and configuration changes.
Debug	Diagnostic information.

Perform the following procedure to configure your log filters for each destination:

Procedure

1. Navigate to **EM** > **System Configuration** > **Monitoring Settings** > **Event Logs** > **Log Filter Settings**.



2. Scroll down in the window to configure the filters for each destination: **SNMP**, **SysLog**, and **Archive**.
3. Click **Save**.

Viewing security logs

About this task

Using security logs, you can track all configuration changes to the system. Security logs contain details about changes to the system. The tracked changes include:

- Exact configuration item that was changed.
- Old and the new values.
- Time of the change.
- IP address of the user who made the change.

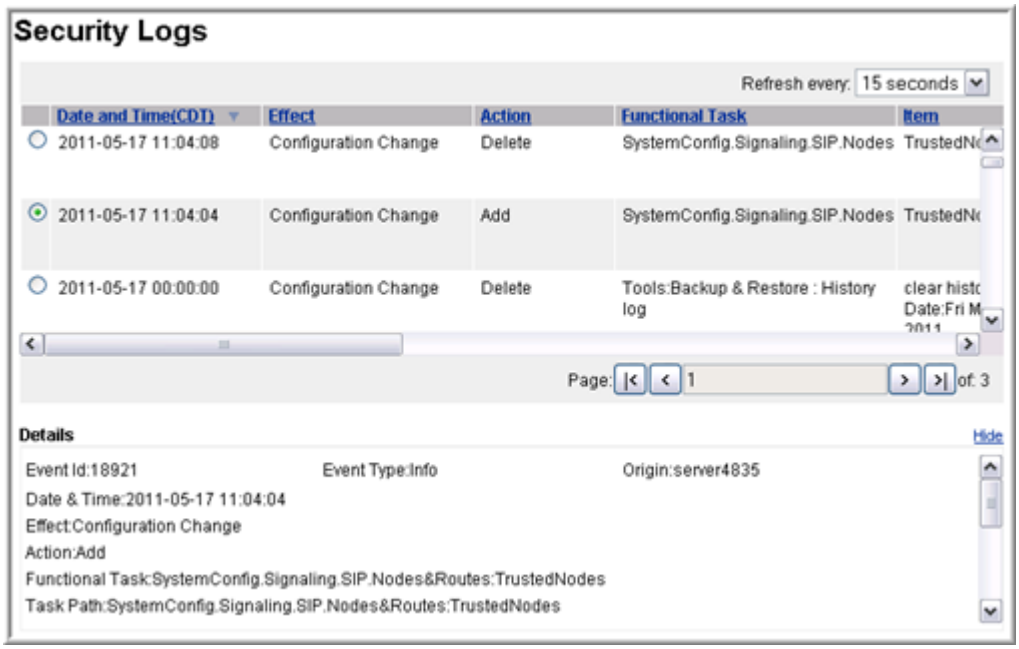
Perform the following procedure to gain access to the saved Avaya Aura® MS Security Logs:

Procedure

1. Navigate to **EM** > **System Status** > **Logs** > **Security Logs**.
2. Select a security log.

   The system displays details of the log in the lower part of the page.

   Use the vertical and horizontal scroll bars to view information.



3. To set the security data refresh interval, use the **Refresh every** drop-down menu.
4. To move back further in the history of the **Security Logs**, use the **Page** navigation buttons.

Configuring log privacy settings

About this task

Perform the following procedure to remove sensitive data from debug logs and SDRs.

Procedure

1. Navigate to **EM** > **System Configuration** > **Logging Settings** > **Privacy**.
2. To remove all sensitive data from debug logs and SDRs, click **Select all**.

   To remove individual sensitive data items, select the data you want to remove.
3. Click **Save**.

Configuring SysLog settings

About this task

Perform the following procedure to enable the delivery of SysLog events and configure the destination server that receives the SysLog events:

Procedure

1. Navigate to **EM** > **System Configuration** > **Logging Settings** > **SysLog**.
2. Select **SYSLOG Delivery of Logs** to enable delivery of SysLogs.
3. Click **Add** to add destination server to **SYSLOG Destination Server List**.

4. Enter the IP address and the port of the destination server in text boxes in the **Server Address** and **Port** columns.

   Note that the virtual and physical appliances are currently limited to one syslog destination.

5. Click **Save**.
6. Click **Confirm**.
7. Restart Avaya Aura® MS for the changes to take effect.

Configuring event log settings

About this task

Perform the following procedure to configure how long the system saves event logs.

Procedure

1. Navigate to **EM** > **System Configuration** > **Logging Settings** > **Event Log**.
2. Configure **Event Log Minimum Record Age** to set the minimum time in days to keep an event log before the system deletes the event log.
3. Configure **Event Log Size** to set the maximum number of megabytes of event log data to keep before the system deletes the event logs.

   The system does not delete event logs unless the event logs are at least the age specified in **Event Log Minimum Record Age**.

4. Click **Save**.

Monitor active sessions

This section describes the procedures for monitoring Active Sessions on Avaya Aura® MS and for customizing the Active Sessions monitor display.

Viewing current active sessions

About this task

The active session display has several features you can use to find sessions of interest. You can also obtain detailed information related to each session, including the SIP messaging.

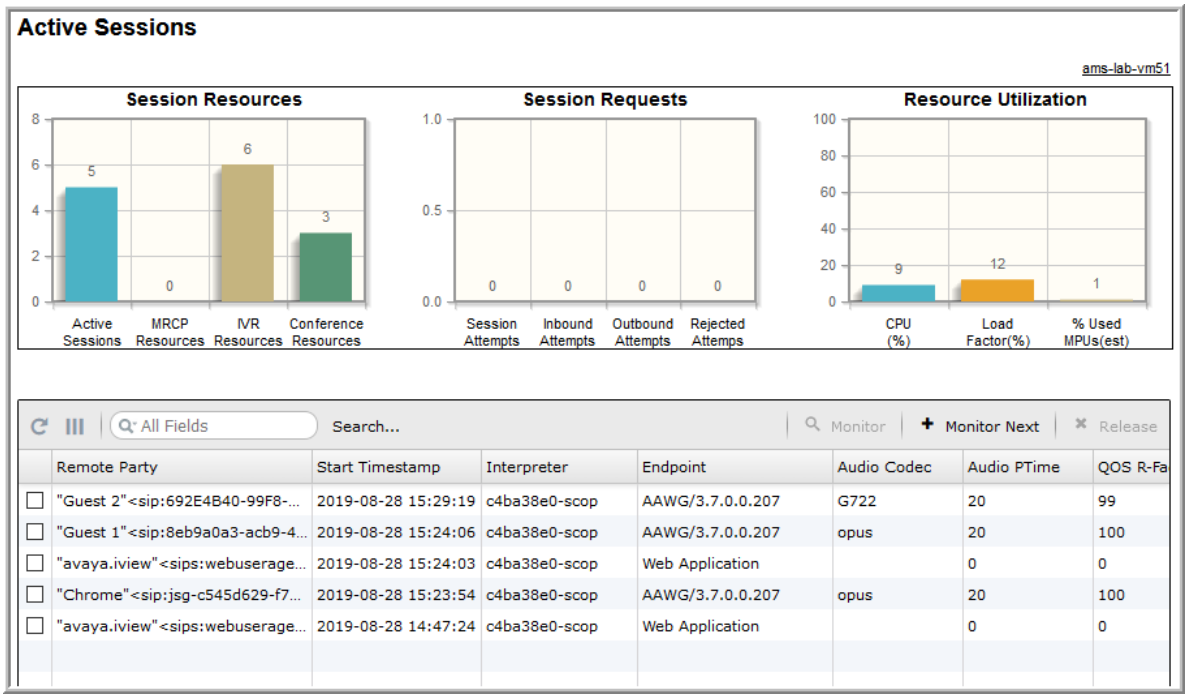
The default view of the **Active Sessions** pane in EM shows an unfiltered list of the active sessions. The unfiltered list can be a list of sessions only on one node or across the entire cluster. You can define a filter with very specific criteria to find sessions of interest.

Procedure

1. Navigate to **EM** > **System Status** > **Monitoring** > **Active Sessions**.

On the **Active Sessions** page, you can see a summary of resources that any current active sessions are consuming.

Use the horizontal scroll bars to see all the columns of information.



2. To find a particular session, click **Search...**. Enter the match criteria of interest in the fields then scroll down and click **Search**.
3. To disable filtering and again show all the active sessions, click the **X** in search field.
4. To toggle the active sessions view between cluster-wide view and nodal view, click the **(Cluster)** toggle button on the upper-right corner of the **Active Sessions** page.

   The **(Cluster)** toggle button is present only if you have configured a cluster. If you click **(Cluster)** to enter the cluster aggregated view, the button name changes to the host name of the local server

Viewing details for a specific session

About this task

The **Active Sessions** page is a useful debugging tool to use when you encounter difficulties. There are options available to collect data for analysis. These options include graphical SIP message flows and SIP traces which show the details of the messages for a particular session.

Perform the following procedure to collect a message trace of a session:

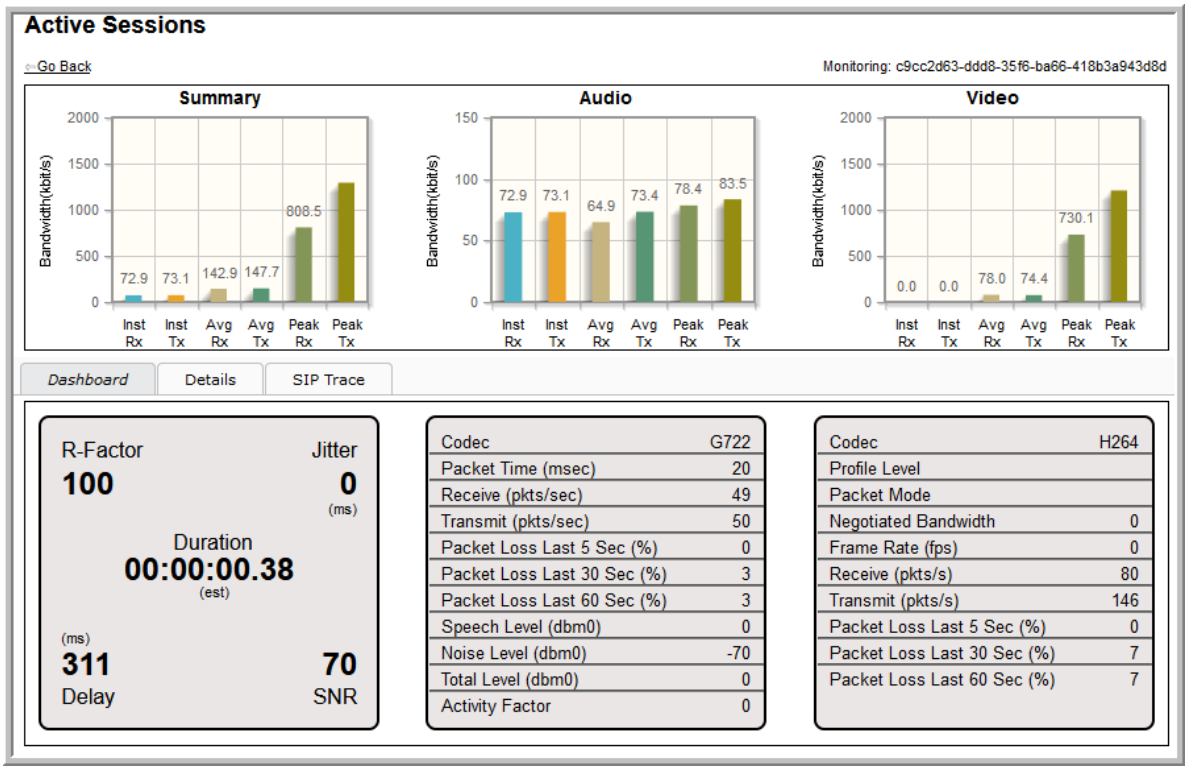
Procedure

1. Set up the trace monitoring by navigating to **EM** > **System Status** > **Monitoring** > **Active Sessions**.

2. Click **Monitor Next** or select a session in the list, and click **Monitor**.

   EM displays a message that the system is waiting for a new session to start.

   After the next session arrives, the system displays the **Active Sessions** page with a detailed call performance summary.



   Click on **Details** to display the SIP messages.

3. Click on **SIP Trace** to display a graphical message flow.

Releasing a session

About this task

Perform the following procedure to release an active session:

Procedure

1. Navigate to **EM** > **System Status** > **Monitoring** > **Active Sessions**.
2. As described in this section, apply filters to find the session you need to release.
3. Select the session or sessions that you want to release from the list of **Active Sessions** that the system displays.
4. To end the selected session, click **Release**.

Monitoring system performance

About this task

Avaya Aura® Media Server provides performance monitoring tools in **Element Manager**. The tools provide real-time displays of the key operational measurement counters and gauges.

The performance monitoring tools use HTML5/JavaScript and require you to use Chrome, Firefox, Safari, or Microsoft Edge.

There are seven different views that display over 140 unique operational measurements. You can select the required view using the textual view link on the top left of the page.

The default cluster display mode is nodal. When the clustered mode is selected, the type of cluster is listed and the display adjusts for the cluster type.

Avaya Aura® MS supports two types of clusters:

- 1+1 High Availability
- N+1 Load Sharing

A “standalone cluster” is sometimes used to describe an Avaya Aura® Media Server which does not belong to a cluster. 1+1 HA clusters are active/standby, so toggling this mode does not result in aggregation of the measurements.

Operational measurements are grouped by type: Gauges are grouped with other gauges and counters with other counters. Counter displays reset to zero every 15 minutes. Gauges display the current real-time value.

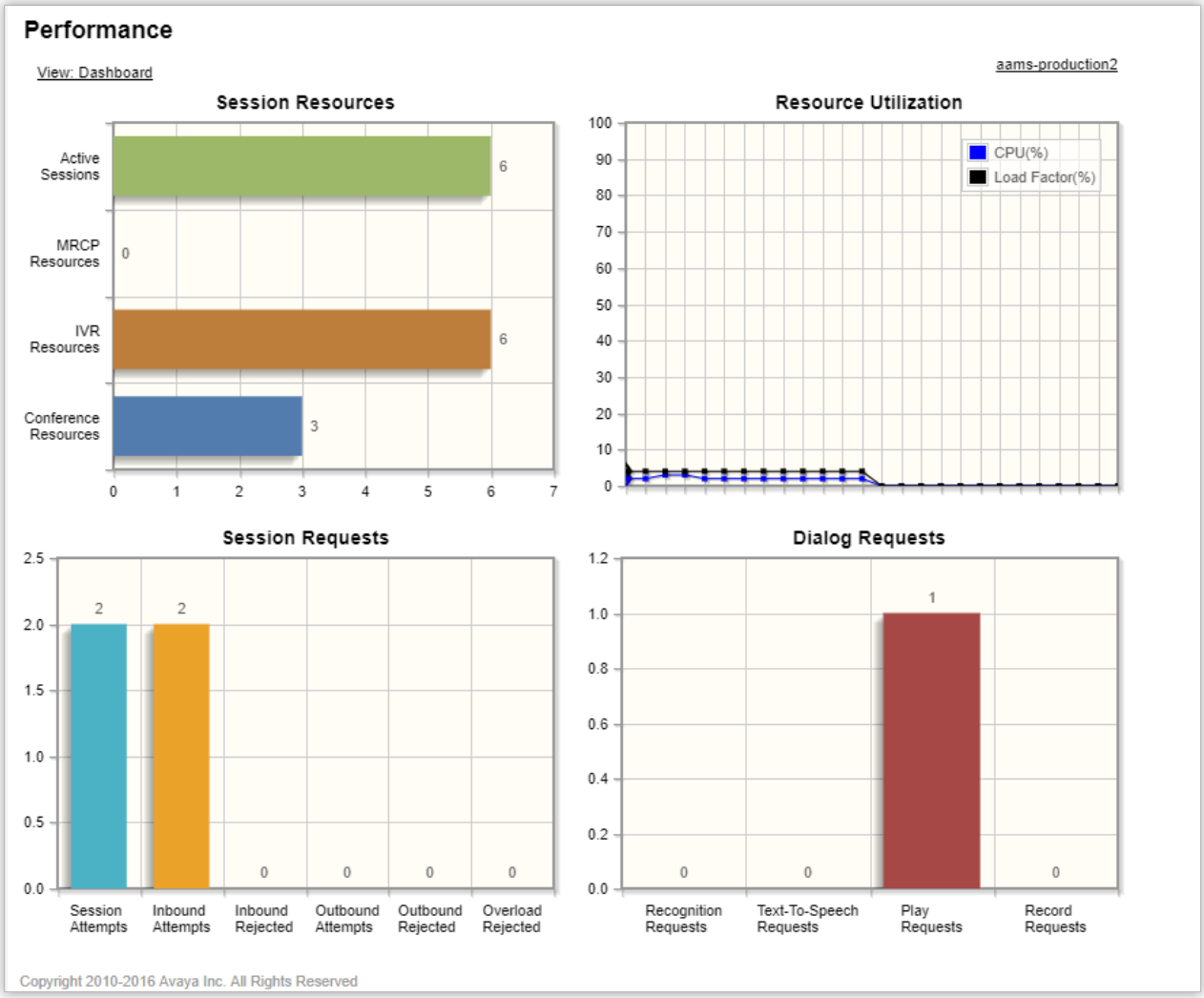


Figure 1: Example Performance page: Dashboard view.

Measurement	Type	Description
Active Sessions	Gauge	The total number of sessions currently in use. This includes media and control channels, and both REST and SIP protocols.
MRCP Resources	Gauge	The total number of MRCP channel resources (ASR and TTS) currently in use.
IVR Resources	Gauge	The total number of internal IVR resources allocated. An IVR resource is typically attached to active sessions and conferences.
CONF Resources	Gauge	The total number of conference resources allocated.
CPU	Gauge	The CPU usage on the virtual or physical server hosting AAMS.

Table continues…

Measurement	Type	Description
Load Factor(%)	Gauge	The load factor on the virtual or physical server hosting AAMS. Most products use load factor instead of CPU to determine the actual capacity remaining on the media server.
Session Attempts	Counter	The total number of SIP and REST session requests to AAMS.
Inbound Attempts	Counter	The number of inbound SIP and REST session requests to AAMS.
Inbound Rejected	Counter	The number of inbound SIP and REST session requests rejected by AAMS. Inbound requests can be rejected for a number of reasons and are typically logged in AAMS event logs.
Outbound Attempts	Counter	The number of outbound SIP session requests solicited by OOD REFER.
Outbound Rejected	Counter	The number of SIP requests which have been rejected or cancelled by the remote application server. This does not always indicate an error. It is common for remote application servers to cancel requests which are released mid-call setup.
Overload Rejected	Counter	The number of requests rejected due to engineering limits.
Recognition Requests	Counter	The number of recognition requests.
Text-To-Speech Requests	Counter	The number of text-to-speech requests.
Play Requests	Counter	The number of play announcement requests.
Record Requests	Counter	The number of record requests.

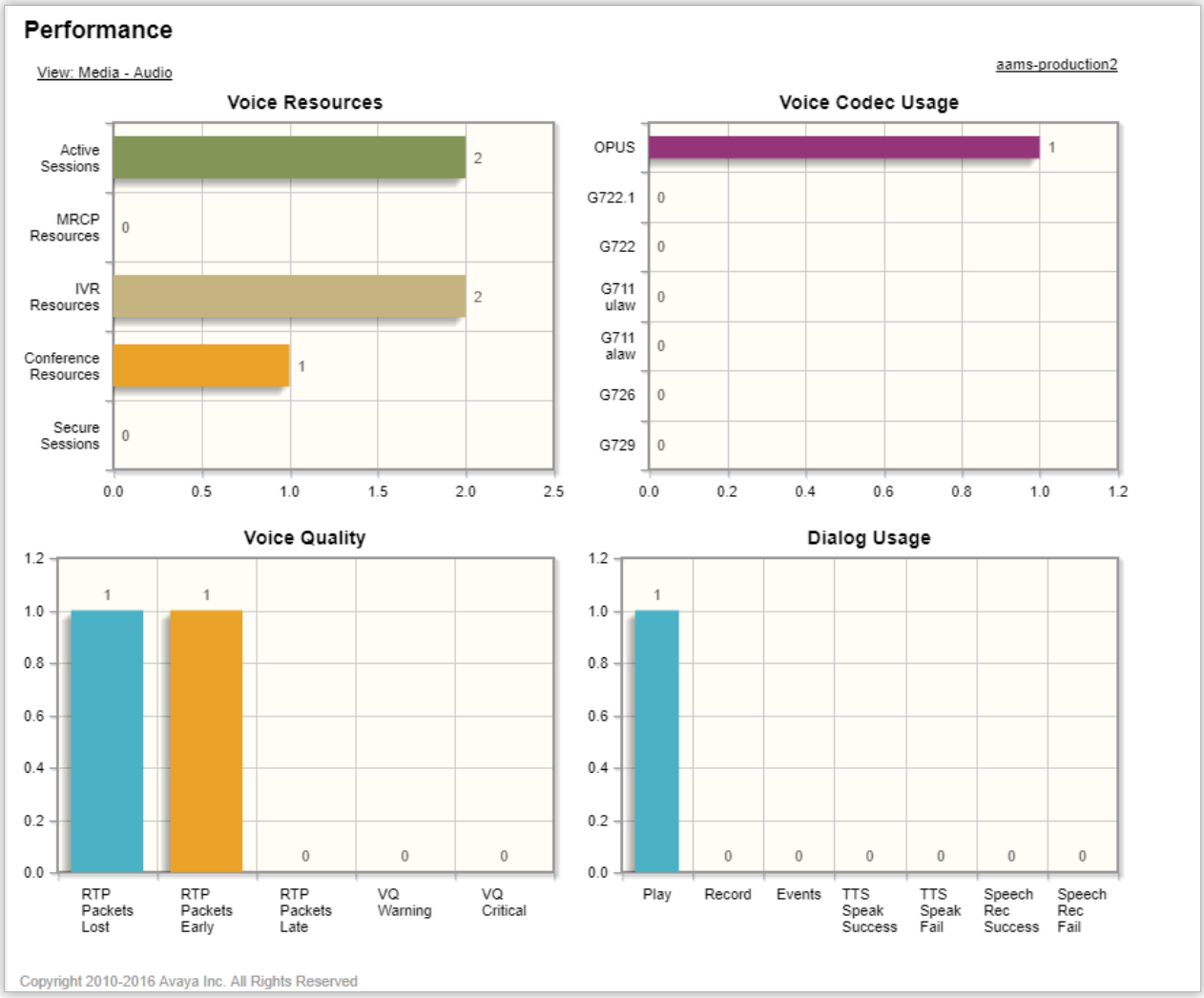


Figure 2: Example Performance page: Media — Audio view.

Measurement	Type	Description
Active Sessions	Gauge	The total number of voice sessions currently in use. This includes media and control channels, and both REST and SIP protocols.
MRCP Resources	Gauge	The total number of MRCP channel resources (ASR and TTS) currently in use.
IVR Resources	Gauge	The total number of internal IVR resources allocated. An IVR resource is typically attached to active sessions and conferences.
CONF Resources	Gauge	The total number of voice conference resources allocated.
Secure Sessions	Gauge	The total number of audio sessions using secure RTP.
OPUS	Gauge	The number of voice sessions using the OPUS codec.
G.722.1	Gauge	The number of voice sessions using the G.722.1 codec.

Table continues…

Measurement	Type	Description
G.722	Gauge	The number of voice sessions using the G.722 codec.
G.711ulaw	Gauge	The number of voice sessions using the G.711ulaw codec.
G.711alaw	Gauge	The number of voice sessions using the G.711alaw codec.
G.726	Gauge	The number of voice sessions using the G.726 codec.
G.729	Gauge	The number of voice sessions using the G.729 codec.
RTP Packets Lost	Gauge	The number of inbound lost RTP packets across all sessions.
RTP Packets Early	Counter	The number of inbound out of order packets across all sessions.
RTP Packets Late	Counter	The number of inbound late packets across all sessions.
VQ Warning	Counter	The number of voice quality warning thresholds passed.
VQ Critical	Counter	The number of voice quality critical thresholds passed.
Play	Counter	The number of play announcement requests.
Record	Counter	The number of record requests.
Events	Counter	The number of dialog events processed, which include digit collection and notifications.
TTS Speak Success	Counter	The number of successful TTS requests.
TTS Speak Fail	Counter	The number of failed TTS requests.
Speech Rec Success	Counter	The number of successful ASR requests.
Speech Rec Fail	Counter	The number of failed ASR requests.

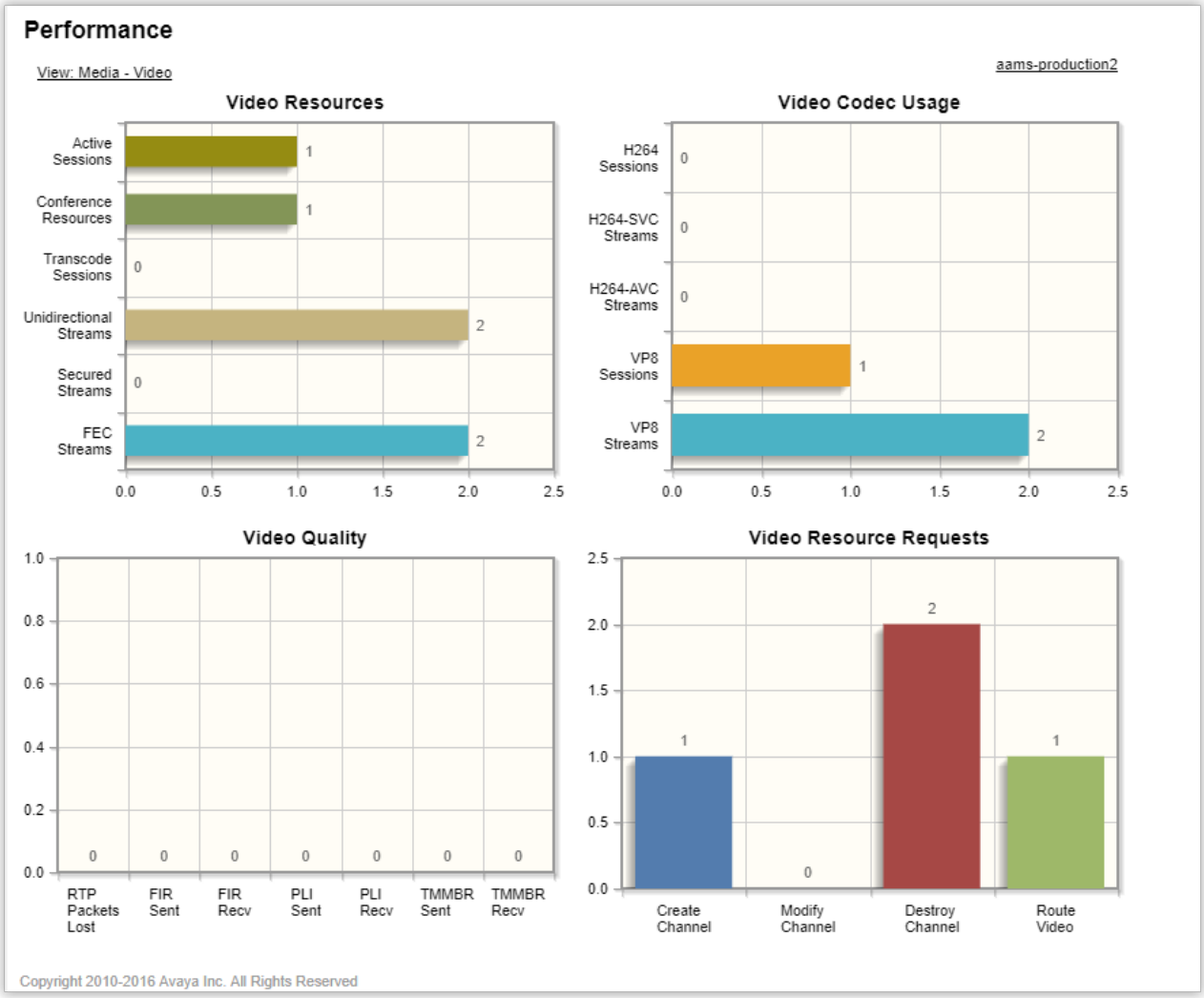


Figure 3: Example Performance page: Media — Video view.

Measurement	Type	Description
Active Sessions	Gauge	The total number of video sessions currently in use.
Conference Resources	Gauge	The total number of video conference resources allocated.
Transcode Sessions	Gauge	The total number of video transcoding resources allocated.
Unidirectional Streams	Gauge	The number of unidirectional video streams in use.
Secured Streams	Gauge	The number of secure RTP video sessions in use.
FEC Streams	Gauge	The number of video streams using forward error correction.

Table continues…

Measurement	Type	Description
H.264 Sessions	Gauge	The number of sessions using H.264-AVC or H.264-SVC.
H.264-SVC Streams	Gauge	The number of H.264-SVC unidirectional streams in use.
H.264-AVC Streams	Gauge	The number of H.264-AVC unidirectional streams in use.
VP8 Sessions	Gauge	The number of sessions using VP8.
VP8 Streams	Gauge	The number of VP8 unidirectional streams in use.
RTP Packets Lost	Counter	The number of video RTP packets lost across all sessions.
FIR Sent	Counter	The number of full intra requests sent.
FIR Recv	Counter	The number of full intra requests received.
PLI Sent	Counter	The number of picture loss indication requests sent.
PLI Recv	Counter	The number of picture loss indication requests received.
TMMBR Sent	Counter	The number of temporary maximum media bit stream rate requests sent.
TMMBR Recv	Counter	The number of temporary maximum media bit stream rate requests received.
Create Channel	Counter	The number of video channel create requests.
Modify Channel	Counter	The number of video channel modify requests.
Destroy Channel	Counter	The number of video channel destroy requests.
Route Video	Counter	The number of route video requests.

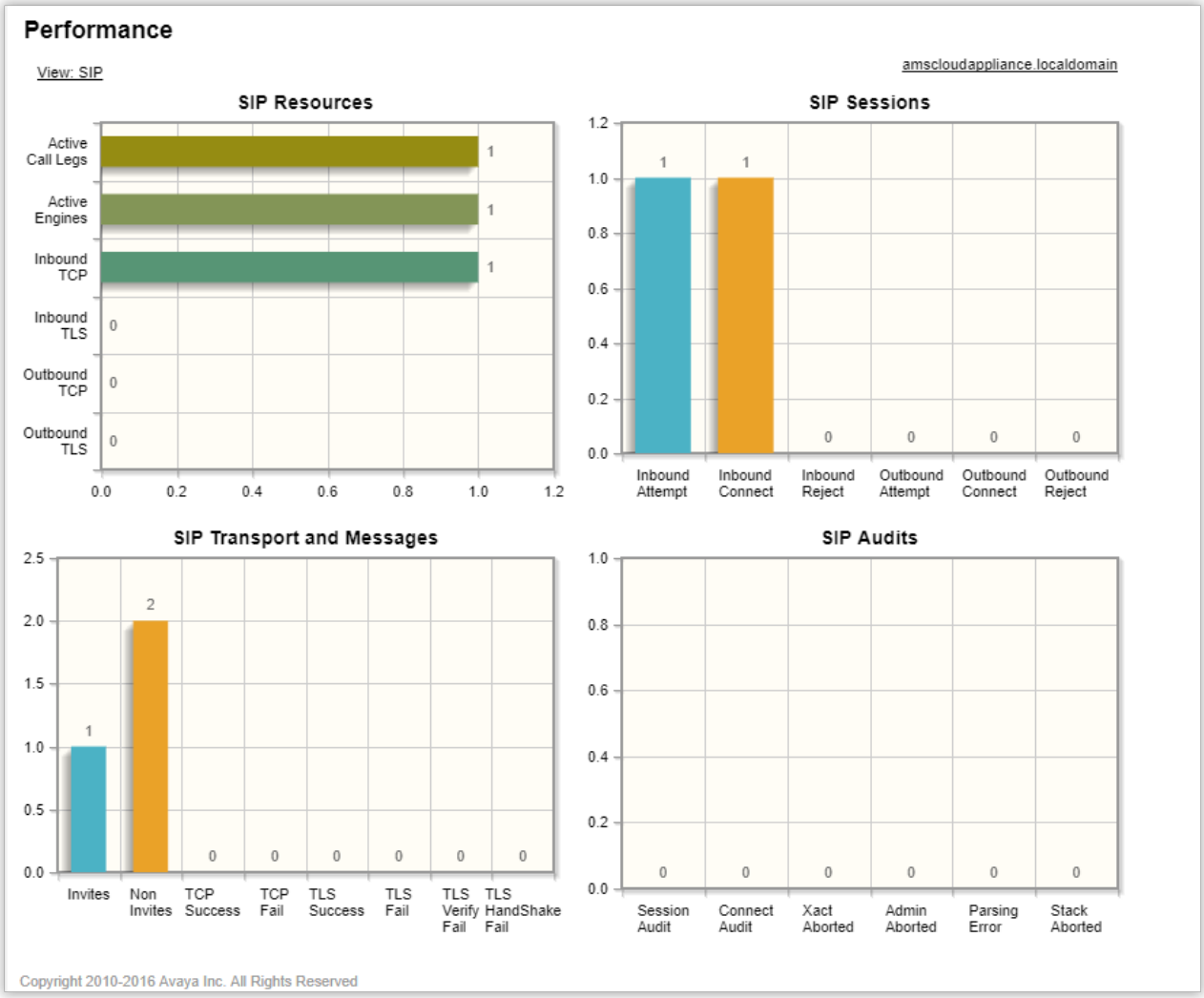


Figure 4: Example Performance page: SIP view.

Measurement	Type	Description
Active Call Legs	Gauge	The total number of active SIP call legs.
Active Engines	Gauge	The total number of active SIP engines. An engine per session is used.
Inbound TCP	Gauge	The number of inbound SIP TCP (unencrypted) connections.
Inbound TLS	Gauge	The number of inbound SIP TLS connections.
Outbound TCP	Gauge	The number of outbound SIP TCP (unencrypted) connections.
Outbound TLS	Gauge	The number of outbound SIP TLS connections.
Inbound Attempt	Counter	The number of inbound SIP session attempts to AAMS.

Table continues…

Measurement	Type	Description
Inbound Connect	Counter	The number of successful inbound SIP session requests to AAMS.
Inbound Reject	Counter	The number of inbound SIP session requests rejected by AAMS.
Outbound Attempt	Counter	The number of outbound SIP session attempts to AAMS.
Outbound Connect	Counter	The number of successful outbound SIP session requests to AAMS.
Outbound Reject	Counter	The number of outbound SIP session requests rejected.
Invites	Counter	The number of SIP invites processed.
Non Invites	Counter	The number of SIP non invites processed.
TCP Success	Counter	The number of successful outbound TCP connections.
TCP Fail	Counter	The number of failed outbound TCP connections.
TLS Success	Counter	The number of successful TLS connections.
TLS Fail	Counter	The number of failed TLS connections.
TLS Verify Fail	Counter	The number of failed TLS host or certificate validations.
TLS Handshake Fail	Counter	The number of failed TLS handshakes.
Session Audit	Counter	The number of SIP sessions released by the session audit.
Connect Audit	Counter	The number of SIP sessions released by the connection audit.
Xact Aborted	Counter	The number of SIP transactions aborted due to network or unresponsive SIP peers.
Admin Aborted	Counter	The number of admin aborted SIP sessions.
Parsing Error	Counter	The number of SIP message parsing failures.
Stack Aborted	Counter	The number of transactions aborted by the SIP stack.

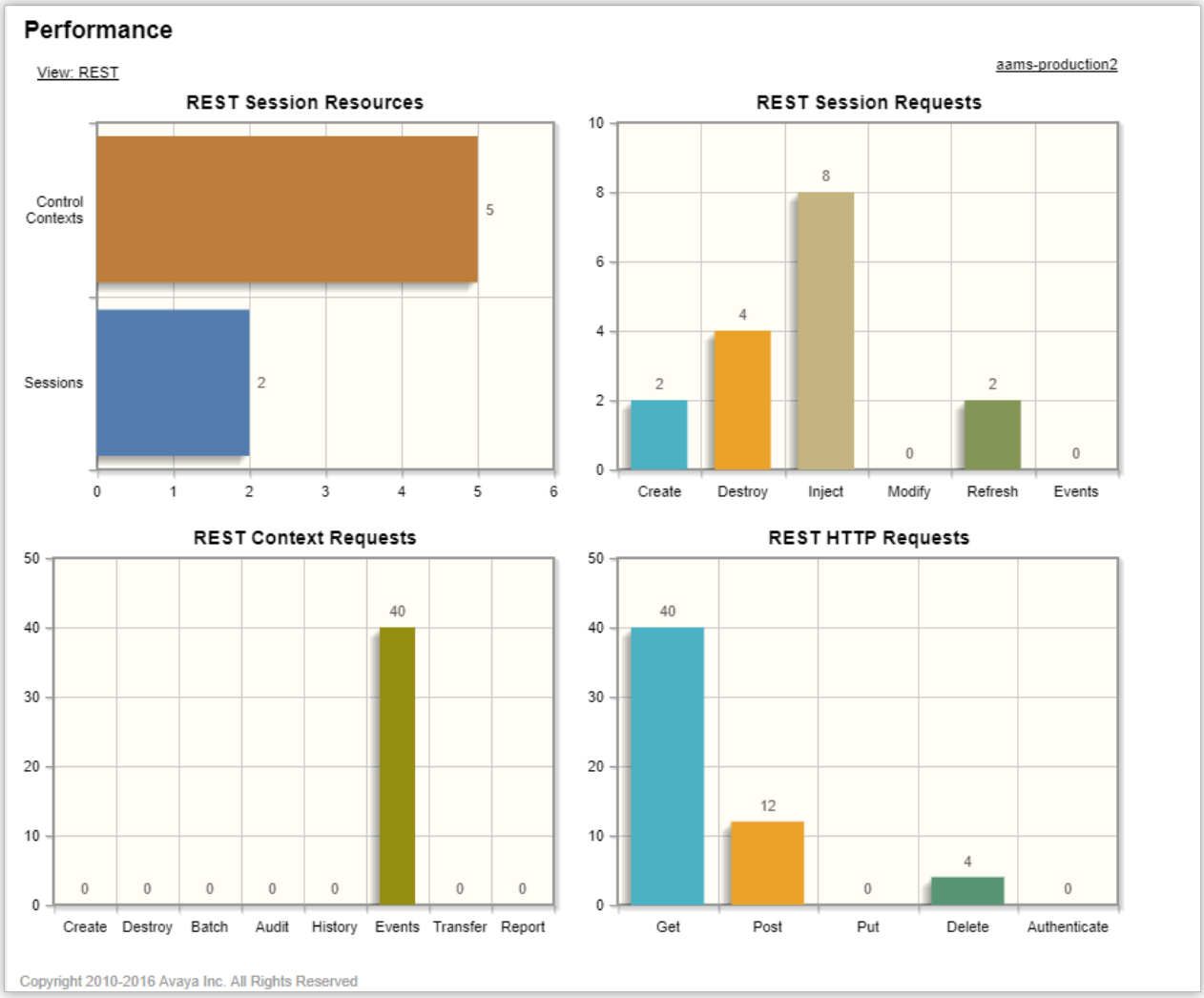


Figure 5: Example Performance page: REST view.

Measurement	Type	Description
Control Contexts	Gauge	The current number of REST control contexts in use.
Sessions	Gauge	The current number of REST sessions in use.
(Session) Create	Counter	The number of session create requests processed.
(Session) Destroy	Counter	The number of session destroy request processed.
Inject	Counter	The number of MSML injection requests processed.
Modify	Counter	The number of session modify requests processed.
Refresh	Counter	The number of session refresh requests processed.
(Session) Events	Counter	The number of session event stream requests processed.
(Context) Create	Counter	The number of context create requests processed.

Table continues…

Measurement	Type	Description
(Context) Destroy	Counter	The number of context destroy requests processed.
Batch	Counter	The number of batch requests processed.
Audit	Counter	The number of audit requests processed.
History	Counter	The number of history requests processed.
(Context) Events	Counter	The number of context event stream requests processed.
Transfer	Counter	The number of context transfer requests processed.
Report	Counter	The number of report requests processed.
Get	Counter	The number of web user agent RESTFul HTTP get requests processed.
Post	Counter	The number of web user agent RESTFul HTTP post requests processed.
Put	Counter	The number of web user agent RESTFul HTTP put requests processed.
Delete	Counter	The number of web user agent RESTFul HTTP delete requests processed.
Authenticate	Counter	The number of web user agent RESTFul authenticate requests processed.

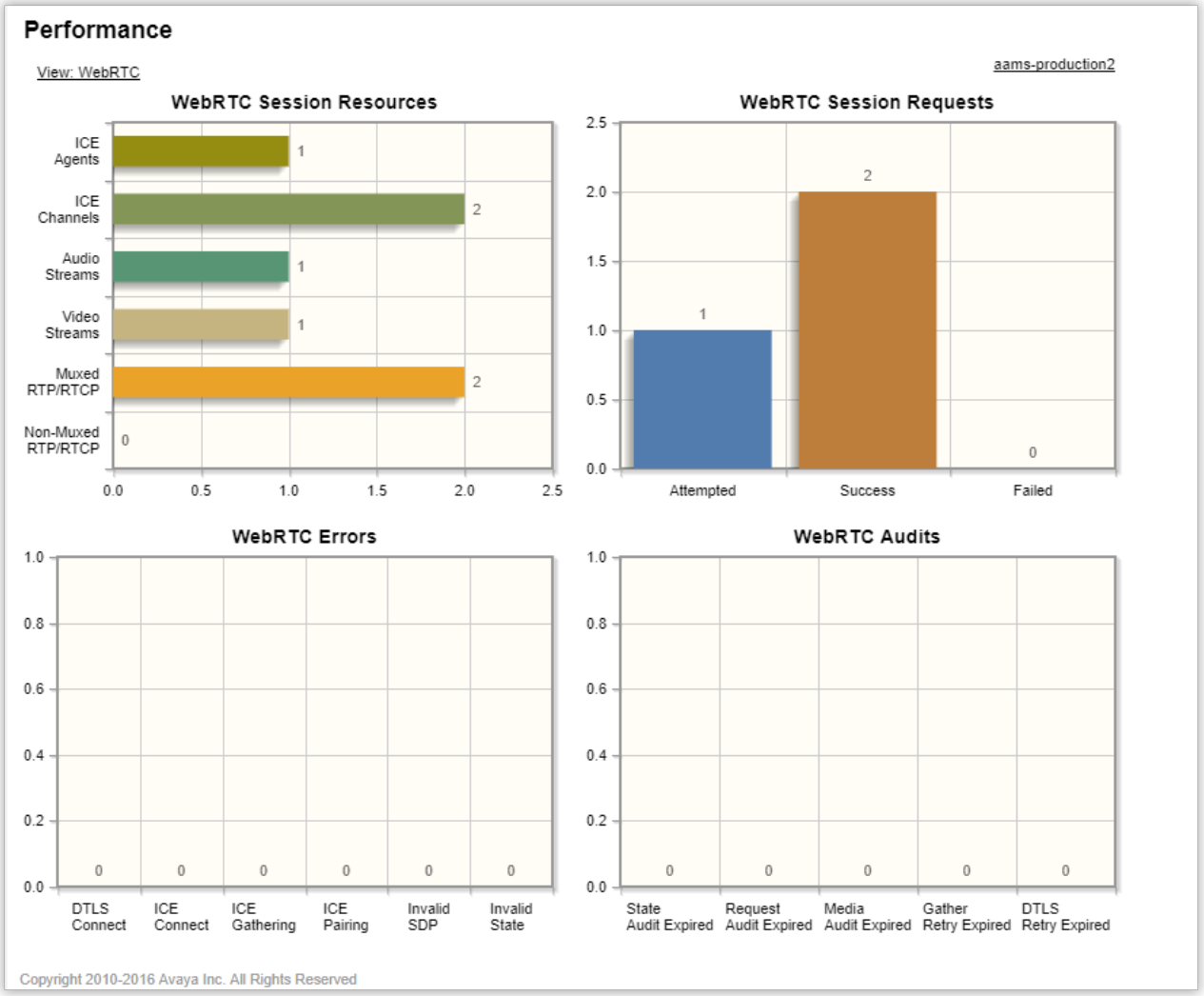


Figure 6: Example Performance page: WebRTC view.

Measurement	Type	Description
ICE Agents	Gauge	The current number of active WebRTC ICE agents. One ICE agent per session is required.
ICE Channels	Gauge	The current number of media channels utilizing ICE.
Audio Streams	Gauge	The current number of WebRTC audio streams.
Video Streams	Gauge	The current number of WebRTC video streams.
Muxed RTP/RTCP	Gauge	The current number of muxed WebRTC RTP/RTCP sessions.
Non-Muxed RTP/ RTCP	Gauge	The current number of non-muxed WebRTC RTP/RTCP sessions.
Attempted	Counter	The number of WebRTC session requests.
Success	Counter	The number of successful WebRTC session requests.

Table continues…

Measurement	Type	Description
Failed	Counter	The number of failed WebRTC session requests.
DTLS Connect	Counter	The number of failed DTLS-SRTP negotiations.
ICE Connect	Counter	The number of failures at ICE connect stage.
ICE Gathering	Counter	The number of failures at the ICE candidate gathering stage.
ICE Pairing	Counter	The number of failures at the ICE candidate pairing stage.
Invalid SDP	Counter	The number of failures due to invalid SDP.
Invalid State	Counter	The number of failures due to invalid state.
State Audit Expired	Counter	The number of state audit expirations.
Request Audit Expired	Counter	The number of request audit expirations.
Media Audit Expired	Counter	The number of media audit expirations.
Gather Retry Expired	Counter	The number of gather retry audit expirations.
DTLS Retry Expired	Counter	The number of DTLS retry audit expirations.

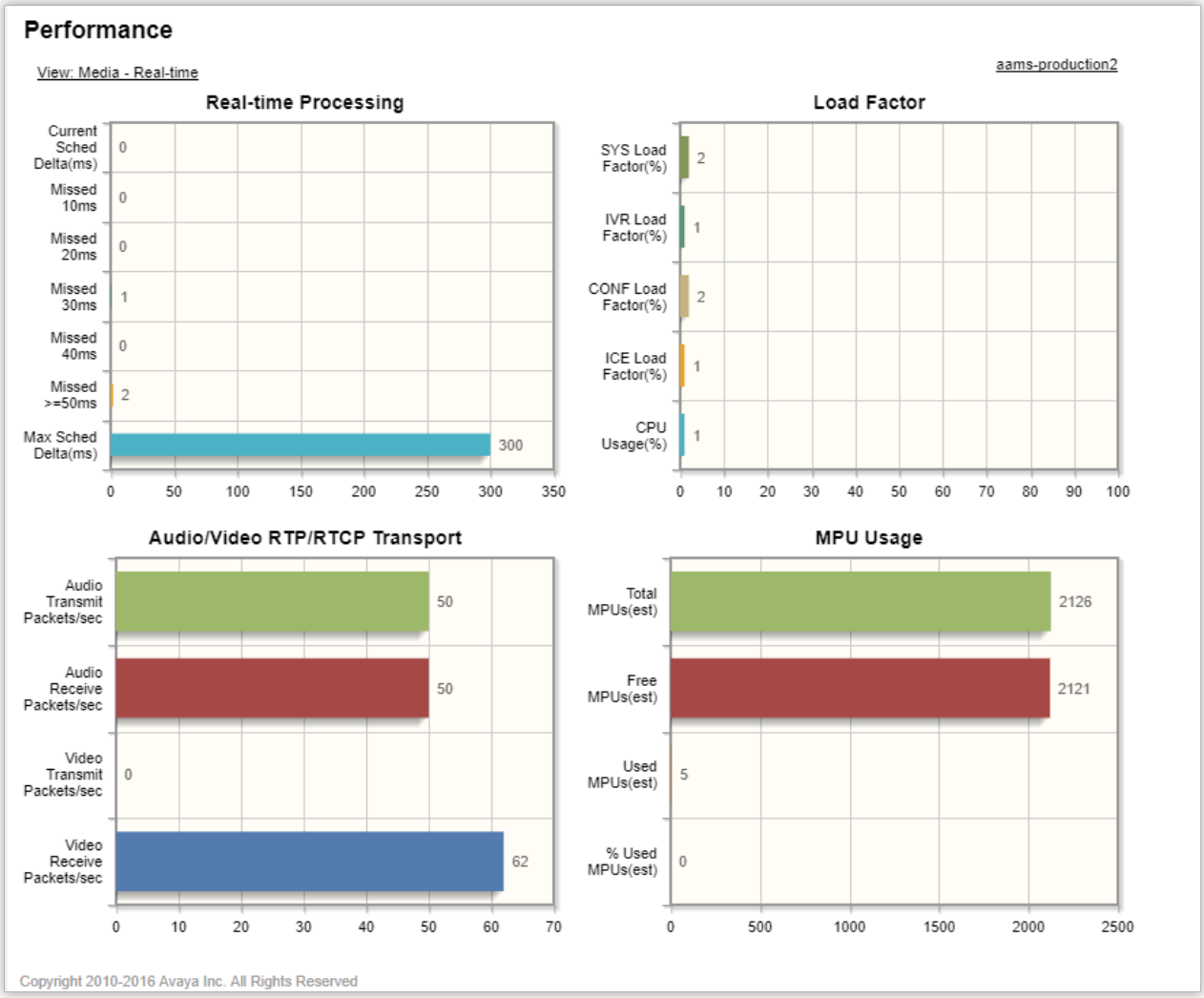


Figure 7: Example Performance page: Media — Real-time view.

Measurement	Type	Description
Current Sched Delta (ms)	Gauge	The current real-time scheduling delta in msec. This value should stay at 0 on healthy systems.
Missed 10ms	Gauge	The number of scheduling deadline intervals missed by 10ms.
Missed 20ms	Gauge	The number of scheduling deadline intervals missed by 20ms.
Missed 30ms	Gauge	The number of scheduling deadline intervals missed by 30ms.
Missed 40ms	Gauge	The number of scheduling deadline intervals missed by 40ms.

Table continues…

Measurement	Type	Description
Missed 50ms	Gauge	The number of scheduling deadline intervals missed by 50ms or more.
Max Sched Delta (ms)	Gauge	The maximum scheduling delta recorded on the server since the last restart.
SYS Load Factor (%)	Gauge	The total system load factor as reported to external application servers. This load factor includes all the individual load factors.
IVR Load Factor (%)	Gauge	The load factor specific to IVR resources.
CONF Load Factor (%)	Gauge	The load factor specific to conference resources.
ICE Load Factor (%)	Gauge	The load factor specific to ICE and WebRTC resources.
CPU Usage (%)	Gauge	The CPU usage on the system in percent.
Audio Transmit Packets/sec	Gauge	The current number of audio RTP/RTCP packets transmitted per second.
Audio Receive Packets/sec	Gauge	The current number of audio RTP/RTCP packets received per second.
Video Transmit Packets/sec	Gauge	The current number of video RTP/RTCP packets transmitted per second.
Video Receive Packets/sec	Gauge	The current number of video RTP/RTCP packets received per second.
Total MPUs(est)	Gauge	An estimate of the total MPUs (media processing units) available on this system when idle. Also known as the MPU rating.
Free MPUs(est)	Gauge	An estimate of the free MPUs (media processing units) available on this system.
Used MPUs(est)	Gauge	An estimate of the used MPUs (media processing units) on this system.
% Used MPUs(est)	Gauge	An estimate of the %used MPUs (media processing units) on this system.

Procedure

1. Navigate to **EM** > **System Status** > **Monitoring** > **Performance**.

   You must use a browser that supports HTML5/JavaScript like Chrome, Firefox, or Safari.

2. To switch between displays, click on the current view link located on the top left of the screen.
3. To switch between cluster and nodal displays, click on the node name or **(Cluster)** link, located on the top right of the page.

   The **(Cluster)** option is available only if you have configured a cluster.

Reports

Viewing the Traffic Summary report

About this task

You can view a report of the previous four weeks that summarize critical media server statistics like active sessions, load factors and CPU usage.

Procedure

To view the Traffic Summary report, navigate to **EM** > **System Status** > **Monitoring** > **Reports** > **Traffic Summary**.

OM monitoring

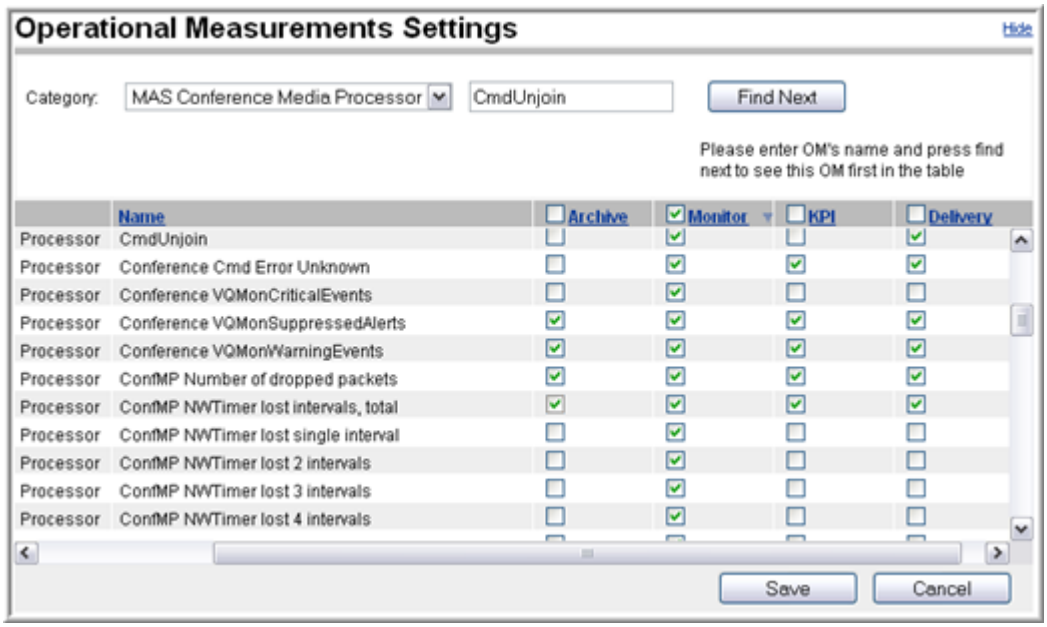
Configuring OM settings

About this task

Perform the following procedure to choose the Operational Measurements (OMs) that are available for Archiving, Monitoring, Delivery and the OM that are used as Key Performance Indicators (KPI):

Procedure

1. Navigate to **EM** > **System Configuration** > **Monitoring Settings** > **Operational Measurements** > **Settings**.



Tip:

- You can sort the columns by clicking on the column name.
- You can filter the displayed OMs by selecting a category from the **Category** drop-down menu.
- If you know the name of the OM to configure, type the name in the field to the left of the **Find Next** button. Then press `Enter` or click **Find Next**.
- You can use the check box next to the column title to select or deselect all OMs listed in that column.

2. On the Operational Measurement Settings page, select the check box in the **Archive** column next to each OM to archive.
3. Select check boxes in the **Monitor** column next to each OM that you want to monitor.
4. Select the check boxes in the **KPI** column next to each OM that you want to appear in **System Performance Summary**. The **System Performance Summary** is located at **EM** > **System Status** > **Cluster Status**.
5. Select the check box next to the OM in the **Delivery** column to indicate which OMs to deliver as periodic comma-separated values (CSV) reports.
6. Click **Save**.

Configuring OM delivery

About this task

Perform the following procedure to configure how the system delivers OM reports using FTP (File Transfer Protocol) or SFTP (Secure FTP):

Procedure

1. Navigate to **EM** > **System Configuration** > **Monitoring Settings** > **Operational Measurements** > **Delivery**.
2. Select **Periodic Performance Report Delivery** to enable performance report delivery for FTP or SFTP.
3. Select **Report ZIP Compression** to create a .zip file of the OM reports.
4. Select **FTP Report Delivery** to deliver reports using FTP.
5. Enter the address of the destination FTP server you want to send the reports to, in the **FTP Server Network Address field**.
6. In the **FTP Remote Directory** field, enter the address of an optional remote directory to change to before uploading the report.
7. In the **FTP Account Username** field, enter the FTP user name to use at the destination FTP server.
8. In the **FTP Account Password** field, enter the FTP password to use at the destination FTP server.

9. (Optional) Select the **Secure FTP (SFTP)** check box and then configure the SFTP options:
    a. In the **Secure FTP Remote Server Fingerprint** field, enter the fingerprint of the remote server.
    b. In the **Secure FTP Key File Name** field, enter the file name to use as the optional SFTP key file.
10. Click **Save**.
11. Restart Avaya Aura® MS for the changes to take effect.

Configuring OM archiving

About this task

Perform the following procedure to archive OMs and to configure OM retention options:

Procedure

1. Navigate to **EM** > **System Configuration** > **Logging Settings** > **OMs**.
2. Select **Archive Operational Measurements** to enable OM archiving.
3. In the **Operational Measurement Archive Minimum Record Age** field, specify the number of days after which the system needs to archive OMs.

   When the system initiates a cleanup, it removes all archived OMs older than the specified days.
4. In the **Operational Measurement Archive Cleanup Threshold Size** field, enter the maximum space in bytes for OMs to use before the system initiates a cleanup.
5. In the **Operational Measurements Reset Interval** field, set the interval in minutes at which the system archives and resets OMs.
6. Click **Save**.
7. Click **Confirm**.
8. Restart Avaya Aura® MS for the changes to take effect.

Monitoring protocol connections

About this task

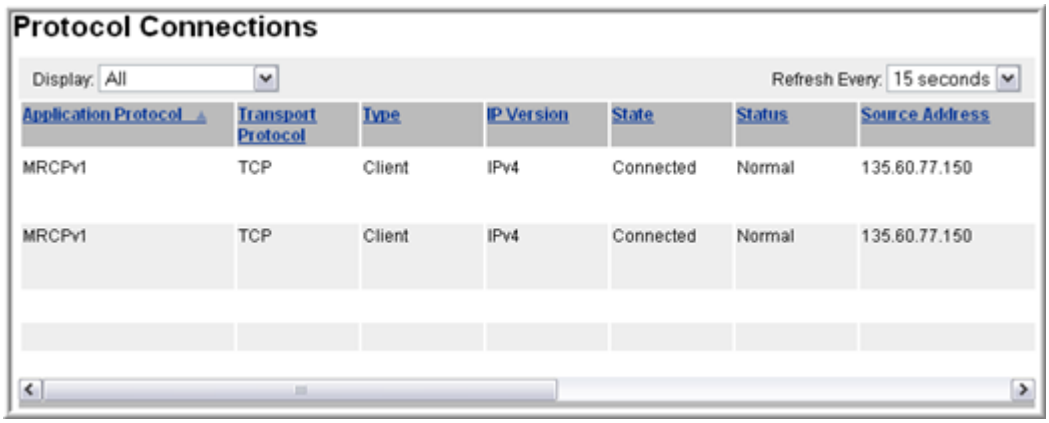
Perform the following procedure to view operational information about installed protocols:

Procedure

1. Navigate to **EM** > **System Status** > **Monitoring** > **Protocol Connections**.
2. To set the protocol connection data refresh interval, use the **Refresh every** drop-down menu.

View the information for the installed protocols using the vertical and horizontal scroll bars. You can change the order of the connection list by clicking the title of any column.

There are no actions that can be performed. The display is informational only.



Monitoring music streams

About this task

You can use EM to monitor the status of the following types of music source providers:

Live streams

- Real Siimple Syndication (RSS) provider
- HTTP/MP3 provider
- HTTP Live Streaming (HLS) provider

Directory streams

- Local File System provider
- Content Store provider

Note:

The **Local File System provider** and **Content Store provider** are configured as part of an adopting product. See adopting product documentation.

Perform the following procedure to monitor the status of configured music streams.

Procedure

1. Navigate to **EM** > **System Status** > **Monitoring** > **Music Streams**.
2. To see the status text of a music source, move the mouse over the **Stream Key** name.
3. To set the refresh interval, use the **Refresh every** drop-down menu.

Related links

Music streaming configuration on page 124

Streaming music troubleshooting on page 254

Advanced system monitoring

Viewing component status

About this task

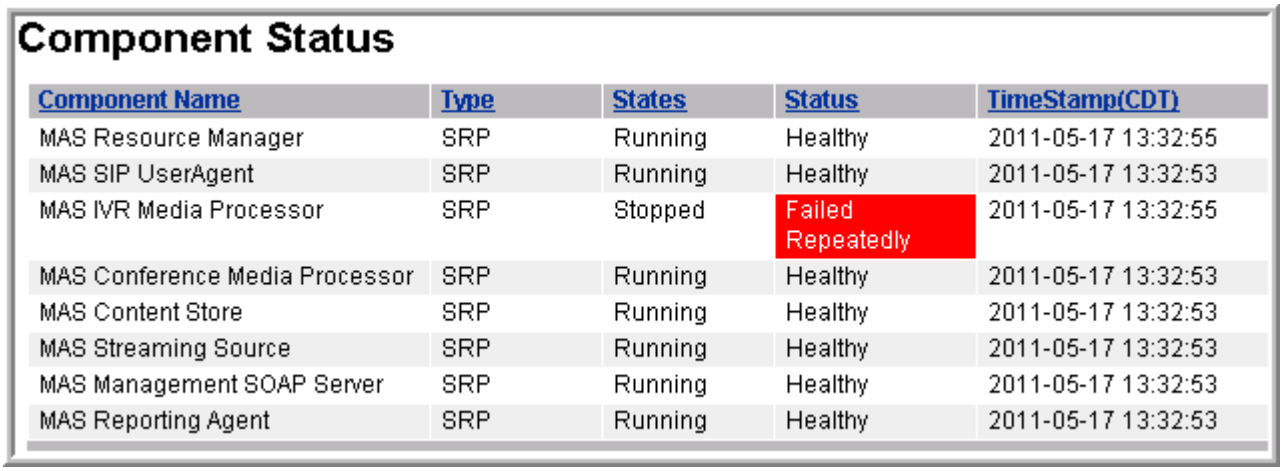
Perform the following procedure to view the operational state of individual Avaya Aura® MS components:

Procedure

Navigate to **EM** > **System Status** > **Monitoring** > **Advanced** > **Component Status**.

In the content pane of EM, the Component Status page displays information about the operational state of individual components of Avaya Aura® MS.

You cannot perform any actions on the listed components. The information is useful for diagnosing and isolating system problems when working with Avaya support.



Component Status

Component Name	Type	States	Status	TimeStamp(CDT)
MAS Resource Manager	SRP	Running	Healthy	2011-05-17 13:32:55
MAS SIP UserAgent	SRP	Running	Healthy	2011-05-17 13:32:53
MAS IVR Media Processor	SRP	Stopped	Failed Repeatedly	2011-05-17 13:32:55
MAS Conference Media Processor	SRP	Running	Healthy	2011-05-17 13:32:53
MAS Content Store	SRP	Running	Healthy	2011-05-17 13:32:53
MAS Streaming Source	SRP	Running	Healthy	2011-05-17 13:32:53
MAS Management SOAP Server	SRP	Running	Healthy	2011-05-17 13:32:53
MAS Reporting Agent	SRP	Running	Healthy	2011-05-17 13:32:53

Viewing advanced protocols

About this task

Perform the following procedure to view the status of various media server protocol interfaces:

Procedure

1. Navigate to **EM** > **System Status** > **Monitoring** > **Advanced** > **All Protocol Connections**.

   The system displays information about the operational state of protocols on Avaya Aura® MS.

2. To set the protocol connection data refresh interval, use the **Refresh every** drop-down menu.
3. Select the desired protocol from the **Display** drop-down list to restrict the display to certain protocols.

   You cannot perform any actions on this page. The information is useful for diagnosing and isolating system problems when working with Avaya support.

SDR monitoring

Avaya Aura® MS sessions generate Session Detail Records (SDRs) which contain detailed information about each session. EM provides an SDR Browser which you can use to review the details of any session processed by the media server.

Perform the following procedures to filter and review SDRs, generate graphical reports of sessions for traffic pattern analysis, and view peak Avaya Aura® MS traffic:

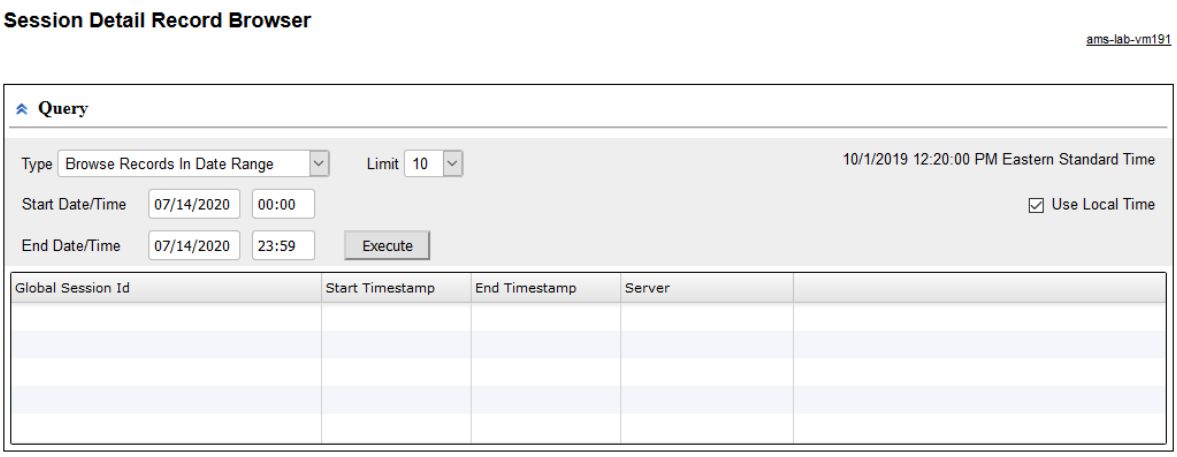
Reviewing SDRs

About this task

Perform the following procedure to filter and review the details of any sessions archived by the media server:

Procedure

1. Navigate to **EM** > **Tools** > **Session Detail Record Browser**.

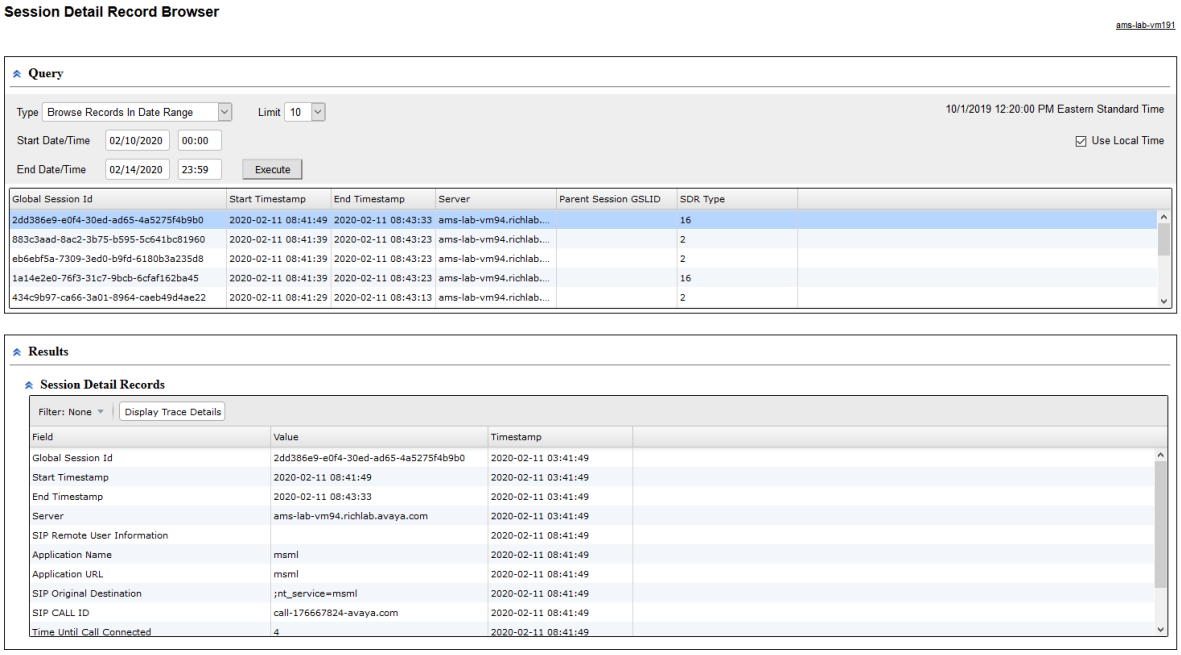


2. Select **Browse Records In Date Range** query type from the **Type** drop-down menu.
3. To define a time range for the query, use the **Start** and the **End** options in the **Query** panel.
4. Enter the maximum number of results in the **Limit** field.

5. Click **Execute** to run the query.

   The system displays the list of sessions.

6. Click one of the rows in the list of sessions.
7. Scroll down to review the details of that session in the **Session Detail Records** panel.



Determining peak session traffic

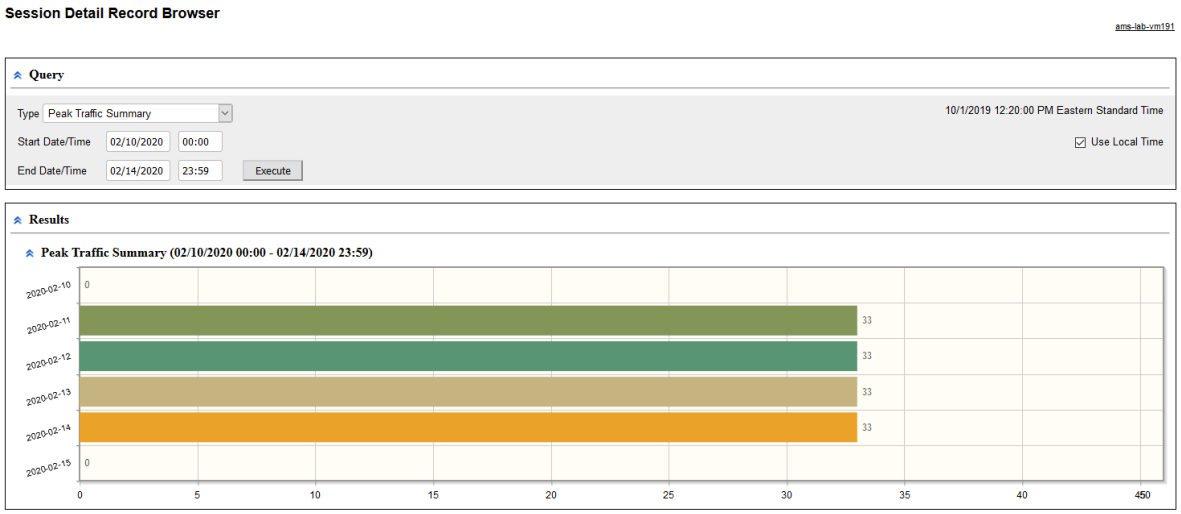
About this task

Perform the following procedure to generate a graphical report representing the peak number of sessions processed by the Avaya Aura® MS each day:

Procedure

1. Navigate to **EM** > **Tools** > **Session Detail Record Browser**.
2. To run a query which reports the peak number of sessions processed each day, select **Peak Traffic Summary** from the **Type** drop-down menu.
3. Use the **Start** and the **End** options in the **Query** panel to define a time range for the query.
4. Click **Execute** to run the new query and generate a graphical Peak Traffic Summary.

   Move your cursor over any bar graph element to see the peak number of sessions for each day.



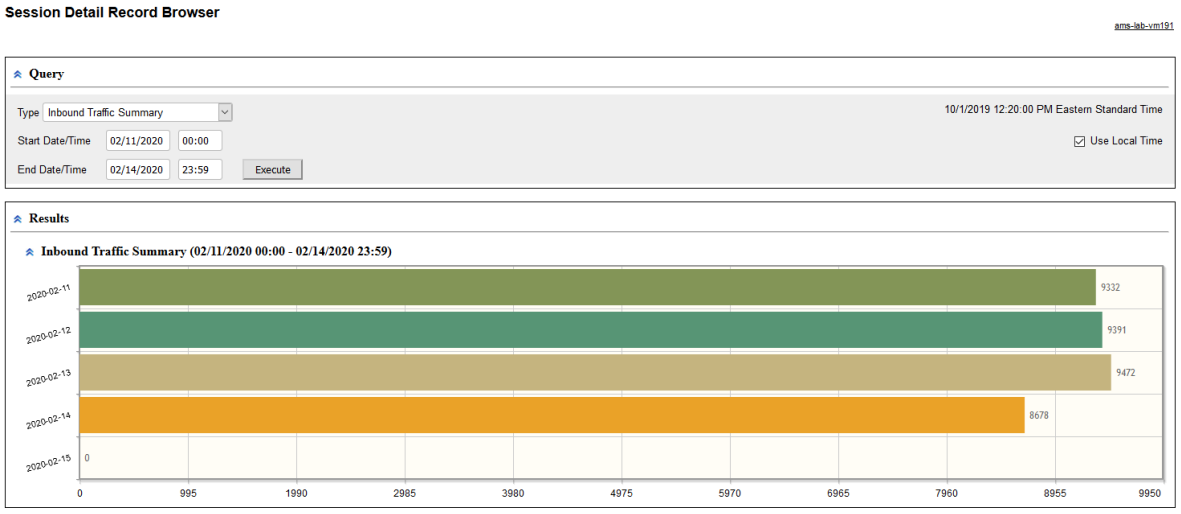
Summarizing daily inbound traffic

About this task

Perform the following procedure to generate graphical reports which summarize daily inbound traffic processed by the Avaya Aura® MS:

Procedure

1. Navigate to **EM** > **Tools** > **Session Detail Record Browser**.
2. To run a query which reports the total number of sessions processed for each day, select **Inbound Traffic Summary** from the **Type** drop-down menu.
3. To define a time range for the query, use the **Start** and the **End** options in the **Query** panel.
4. Click **Execute** to run the new query and generate a graphical Inbound Traffic Summary. Move your cursor over any bar graph element to see the total number of sessions handled for each day.



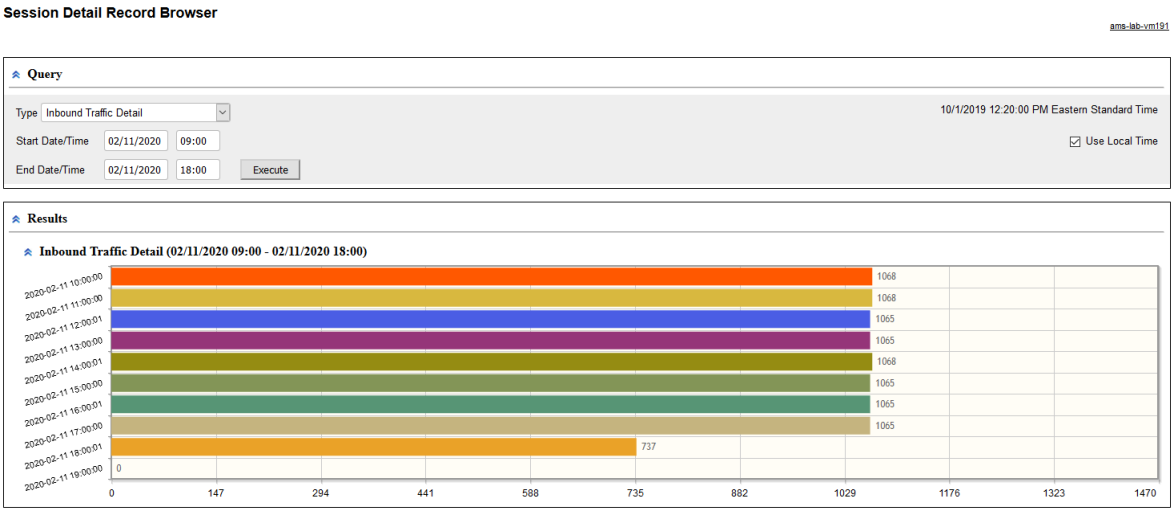
Analyzing hourly inbound traffic details

About this task

Perform the following procedure to generate graphical reports for determination of hourly traffic processed by the Avaya Aura® MS:

Procedure

1. Navigate to **EM** > **Tools** > **Session Detail Record Browser**.
2. To run a query which details the total number of inbound sessions processed each hour, select **Inbound Traffic Detail** from the **Type** drop-down menu.
3. To define a time range for the query, use the **Start** and the **End** options in the **Query** panel.
4. Click **Execute** to run the new query and generate a graph showing hourly inbound session totals. Move your cursor over any bar graph element to see the number of sessions recorded for that hour.



Reviewing a monitored SDR

About this task

A session which is traced using the session monitoring procedure produces a more detailed SDR. The SDR browser shows additional information for these monitored sessions which includes:

- Detailed SIP and application log records.
- Operational measurement graphs specific to the session.
- A graphical SIP message flow.

Perform the following procedure to review the detailed SDR of a monitored session.

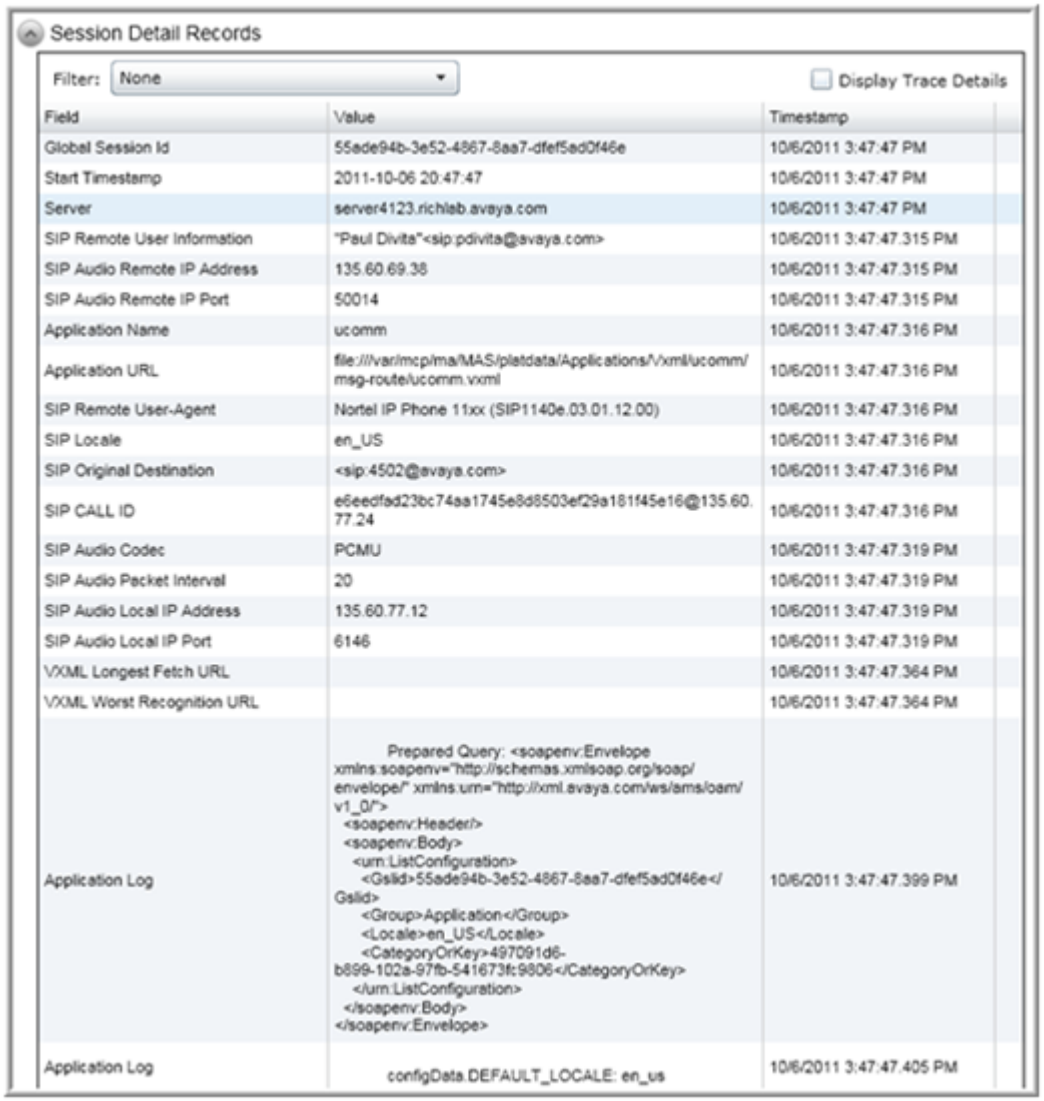
Before you begin

See Viewing details for a specific session on page 196 to add a detailed SDR to the archive and then perform the following procedure:

Procedure

1. Navigate to **EM** > **Tools** > **Session Detail Record Browser**.
2. Select **Browse Records In Date Range** as the query type, from the **Type** drop-down menu.
3. Use the **Start** and the **End** options in the **Query** panel to define a narrow time range for the query which includes the monitored session.
4. In the **Limit** field, enter the maximum number of results that you want to view.
5. Click **Execute** to run the query.

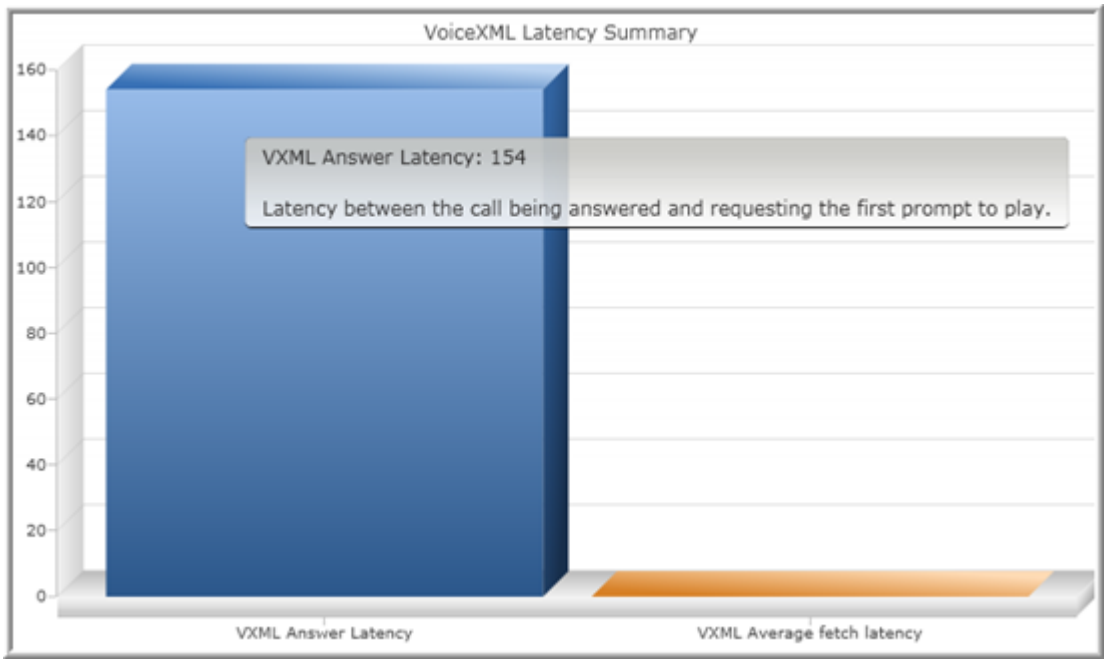
   The system displays the list of sessions corresponding to the monitored session.
6. Click the result row in the list of sessions.
7. Scroll down to review the details of the session as shown in the following examples.

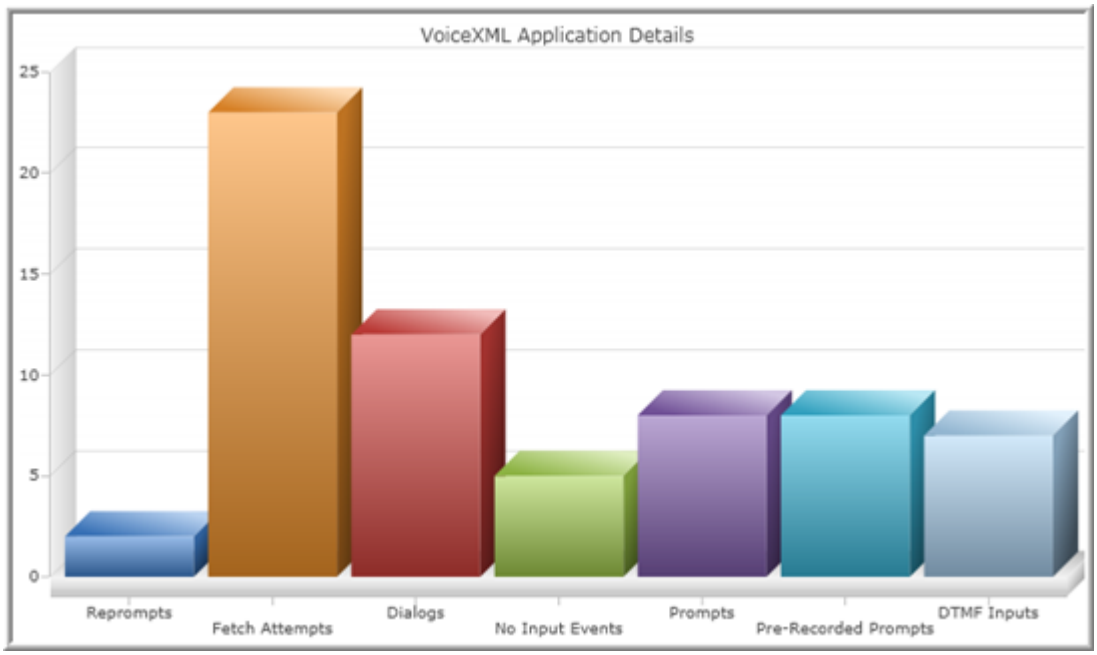


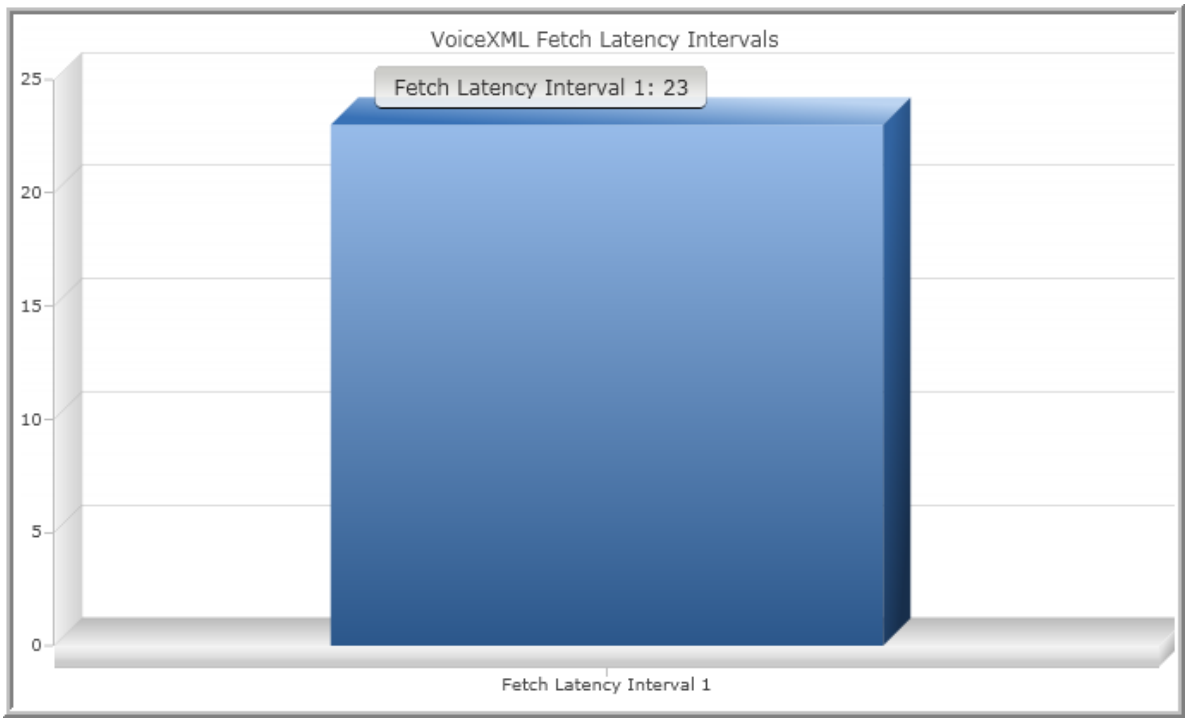
Session Detail Records

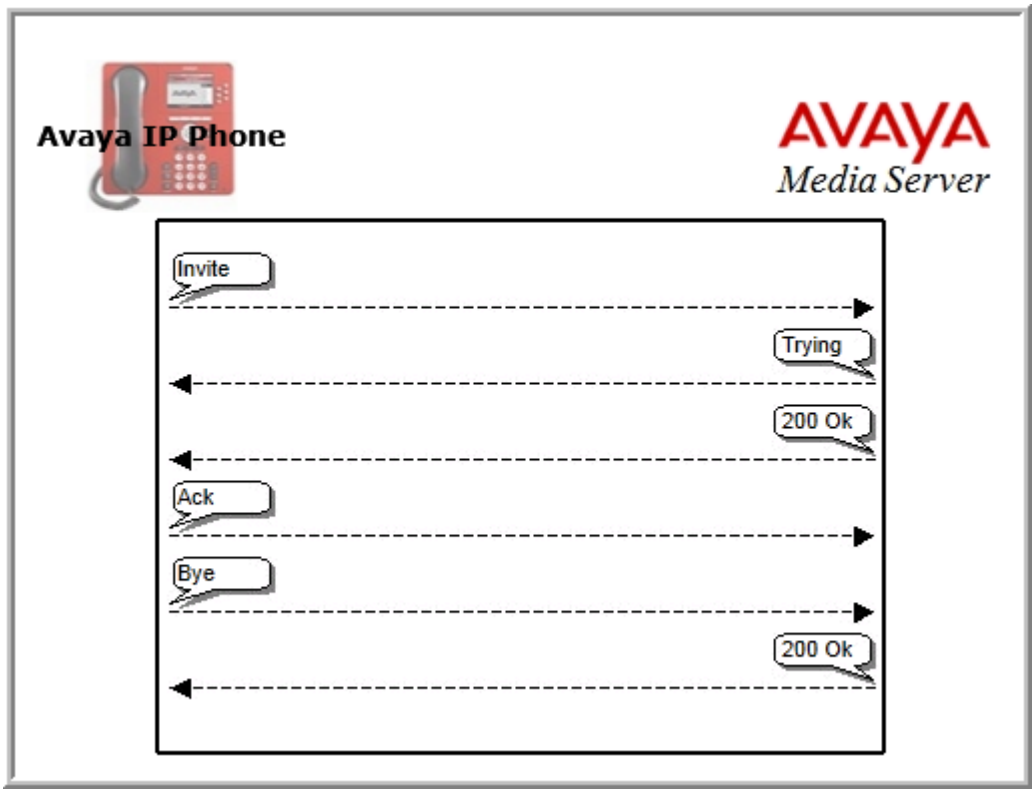
Filter: None — Display Trace Details

Field	Value	Timestamp
Global Session Id	55ade94b-3e52-4867-8aa7-dfef5ad0f46e	10/6/2011 3:47:47 PM
Start Timestamp	2011-10-06 20:47:47	10/6/2011 3:47:47 PM
Server	server4123.richlab.avaya.com	10/6/2011 3:47:47 PM
SIP Remote User Information	"Paul Divita"<sip:pdivita@avaya.com>	10/6/2011 3:47:47.315 PM
SIP Audio Remote IP Address	135.60.69.38	10/6/2011 3:47:47.315 PM
SIP Audio Remote IP Port	50014	10/6/2011 3:47:47.315 PM
Application Name	ucomm	10/6/2011 3:47:47.316 PM
Application URL	file:///var/mcp/ma/MAS/platdata/Applications/Vxml/ucomm/msg-route/ucomm.vxml	10/6/2011 3:47:47.316 PM
SIP Remote User-Agent	Nortel IP Phone 11xx (SIP1140e.03.01.12.00)	10/6/2011 3:47:47.316 PM
SIP Locale	en_US	10/6/2011 3:47:47.316 PM
SIP Original Destination	<sip:4502@avaya.com>	10/6/2011 3:47:47.316 PM
SIP CALL ID	e6eedfad23bc74aa1745e8d8503ef29a181f45e16@135.60.77.24	10/6/2011 3:47:47.316 PM
SIP Audio Codec	PCMU	10/6/2011 3:47:47.319 PM
SIP Audio Packet Interval	20	10/6/2011 3:47:47.319 PM
SIP Audio Local IP Address	135.60.77.12	10/6/2011 3:47:47.319 PM
SIP Audio Local IP Port	6146	10/6/2011 3:47:47.319 PM
VXML Longest Fetch URL		10/6/2011 3:47:47.364 PM
VXML Worst Recognition URL		10/6/2011 3:47:47.364 PM
Application Log	Prepared Query: <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:urn="http://xml.avaya.com/ws/ams/loam/v1_0/"> <soapenv:Header/> <soapenv:Body> <urn:ListConfiguration> <Gslid>55ade94b-3e52-4867-8aa7-dfef5ad0f46e</Gslid> <Group>Application</Group> <Locale>en_US</Locale> <CategoryOrKey>497091d6-b899-102a-97fb-541673fc9806</CategoryOrKey> </urn:ListConfiguration> </soapenv:Body> </soapenv:Envelope>	10/6/2011 3:47:47.399 PM
Application Log	configData.DEFAULT_LOCALE: en_us	10/6/2011 3:47:47.405 PM


VoiceXML Latency Summary
160
140
120
100
80
60
40
20
0
VXML Answer Latency: 154
Latency between the call being answered and requesting the first prompt to play.
VXML Answer Latency
VXML Average fetch latency


VoiceXML Application Details
25
20
15
10
5
0
Reprompts
Fetch Attempts
Dialogs
No Input Events
Prompts
Pre-Recorded Prompts
DTMF Inputs


VoiceXML Fetch Latency Intervals
Fetch Latency Interval 1: 23
25
20
15
10
5
0
Fetch Latency Interval 1


Avaya IP Phone
AVAYA
Media Server
Invite
Trying
200 Ok
Ack
Bye
200 Ok

Configuring SDR archiving

About this task

The system creates SDRs for each session. You can review the archived SDRs using an SDR browser. You can also clear all the records in the current archive.

Perform the following procedure to enable the archiving of SDRs, configure the retention options, and clear all the records in the current archive:

Procedure

1. Navigate to **EM** > **System Configuration** > **Logging Settings** > **Session Logging**.
2. Select **Session Detail Record Archiving** to enable SDR archiving.
3. In the **Session Detail Record Archive Minimum Record Age** field, specify the number of days after which the system archives SDRs.

   When the system initiates a clean-up, the system removes SDRs older than the configured number of days.
4. In the **Session Detail Record Archive Cleanup Threshold Size** field, enter the maximum space, in bytes, for SDRs to use before the system initiates a cleanup.
5. (Optional) Click **Clear** to delete all currently archived records.
6. Click **Save**.
7. Click **Confirm**.
8. Restart Avaya Aura® MS for the changes to take effect.

Configuring Field Promotion for SDR reports

About this task

Perform the following procedure to select the fields to include in SDRs:

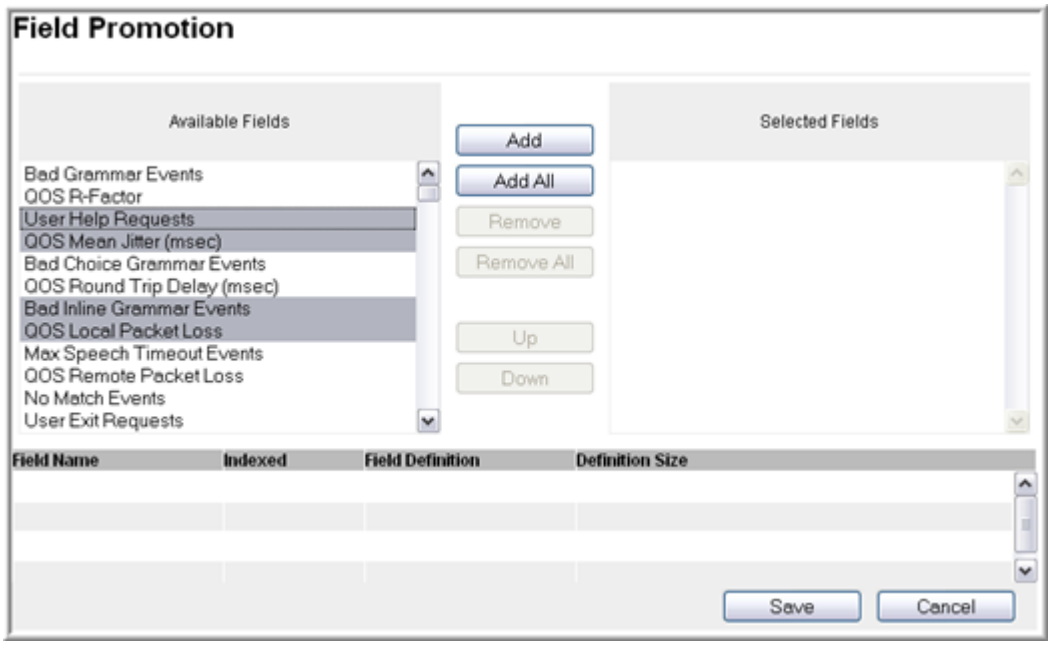
Procedure

1. Navigate to **EM** > **Element Status** and select **Lock** from the **More Actions** drop-down menu and click **Confirm** to lock the system.

   For more information on locking your system, see Setting the operational state.

   Important:

   When you lock the media server, the system ends existing sessions and does not accept new requests. The system redirects new traffic to other nodes in the cluster.
2. Navigate to **EM** > **System Configuration** > **Session Detail Records** > **Field Promotion**.

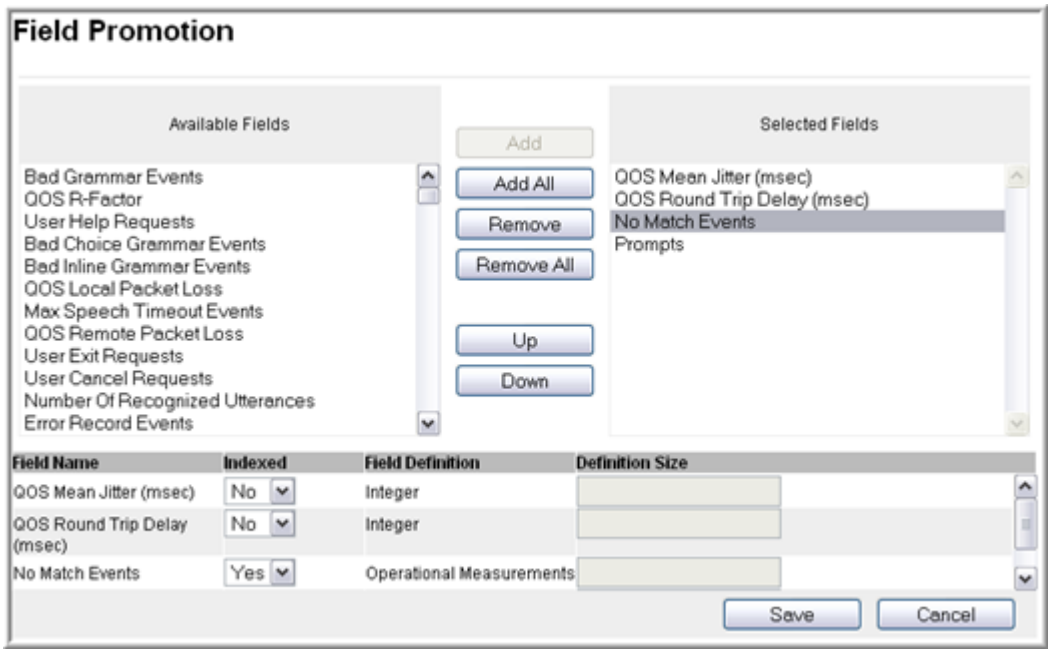


3. Select the required fields from the **Available Fields** column and then click **Add**.

   The system displays the selected fields in the **Selected Fields** column and in the table on the lower part of the page.

Tip:

To select multiple items, press and hold down either the `Shift` key, for multiple selections which are grouped together, or the `Control` key, for multiple selections which are separated.



4. To reorder the fields in **Selected Fields**, select a field and then click **Up** or **Down**.
5. In the **Indexed** column, select **Yes** or **No** as required.
6. If you want to remove any selected field, click on the field in the **Selected Fields** column and then click **Remove**.

Related links

Setting the operational state on page 23

Enabling enhanced SDRs for troubleshooting

About this task

You can enhance SDRs to capture additional detail to aid in system troubleshooting. When you select **Enable System Diagnostic Mode**, the system adds additional fields and full SIP message traces to the SDRs. The EM Active Sessions viewer and SDR browser display these additional details. Additional tracing is useful during trials and system commissioning.

Important:

The collection of additional SDR data impacts system performance. Do not select **Enable System Diagnostic Mode** on live systems processing traffic. Ensure you clear **Enable System Diagnostic Mode** when you have finished troubleshooting.

Perform the following procedure to enable enhanced SDR tracing:

Procedure

1. Navigate to **EM** > **System Configuration** > **Debug Tracing** > **General Settings** > **System Diagnostic**.
2. Select **Enable System Diagnostic Mode**.
3. Click **Save**.
4. Click **Confirm**.
5. Restart Avaya Aura® MS for the changes to take effect.

   To view an enhanced trace of sessions that Avaya Aura® MS processes after the restart, use the SDR browser as described in Reviewing session detail records. Alternatively, use the Active Sessions viewer as described in Viewing current active sessions.

Related links

Viewing current active sessions on page 195

Chapter 11: Account management

Account management overview

Avaya Aura® MS Element Manager (EM) supports several account management policies that you can customize for the required EM administrator authentication and authorization. You can configure the system to use Avaya Aura® MS based authentication or the centralized Avaya Aura® System Manager authentication.

Avaya Aura® MS also supports Role Based Access Control (RBAC) to manage the level of access that the system grants to the authorized administrators. RBAC simplifies permission management by assigning permissions to reusable roles instead of individual administrators.

Account management policies

Avaya Aura® MS provides several options for validating EM administrator login credentials. You can choose one of the following authentication and authorization sources:

EM authentication and authorization sources	
Source	**Description**
Avaya Aura® Media Server	Default option for EM and emergency login. When you use the Avaya Aura® Media Server option, you enable the Avaya Aura® MS RBAC feature. Configuration for administrators and roles is stored locally on Avaya Aura® MS. Single Sign-On (SSO) is not available with the Avaya Aura® Media Server option.
Avaya Aura® System Manager	When you use the Avaya Aura® System Manager option, you enable the centralized Avaya Aura® System Manager RBAC feature. Configuration for administrators and roles is stored on Avaya Aura® System Manager. When you log in to Avaya Aura® MS EM, you see the System Manager login page. After successful login, you are redirected back to Avaya Aura® MS EM. The Avaya Aura® System Manager option provides Single Sign-On (SSO).

Configuring the operating system as the authentication and authorization source

About this task

Perform the following procedure to use the operating system administrator login credentials to access EM. The administrators which log in using this method have unrestricted EM permissions. RBAC is unavailable when the operating system is configured as the authentication and authorization source.

Procedure

1. Navigate to **EM** > **Account Management** > **Policies** > **Sign In**.
2. Select the **Operating System** from the **Authentication and authorization** source drop-down menu.
3. **(Optional)** Configure how long a user session can be idle before EM ends the user session. In the **Element Manager session timeout interval (m)** field, type the number of minutes the session can be idle.
4. Click **Save**.
5. Click **Confirm**.

   The system restarts EM to apply the change. EM login sessions are ended. There is no impact to media server processing of call sessions. You can log in using operating system administrator credentials after the EM restart completes.

Avaya Aura® MS RBAC configuration

You can use Avaya Aura® MS Role Based Access Control (RBAC) when you configure the account management policy to use Avaya Aura® Media Server as the authentication and authorization source.

Using RBAC requires that you create roles for each job function. Next, you define the permission level for each EM task in role. Finally, you can then assign roles that match the job function requirements of each administrator.

The system includes one default administrator with the name admin and with the default role of System Administrator. You cannot modify or delete the default role. You can change the password for the default administrator but you cannot delete the default administrator. The system does not disable the default administrator account after multiple failed login attempts. However, after the configured number of failed login attempts is exceeded, the system generates warning event logs for each default administrator login failure.

In an Avaya Aura® MS cluster, administrators, roles, and permissions are configurable on the Primary media server only. If configuration replication is enabled, changes made on the Primary

server are automatically replicated to the other servers in the cluster. You can view but not edit the configuration on the non-Primary servers of the cluster.

You must select **Avaya Media Server** as the authentication and authorization source to use Avaya Aura® MS RBAC and the procedures in this section.

Configuring Avaya Aura® MS as the authentication and authorization source

About this task

Perform the following procedure to enable Avaya Aura® Media Server based RBAC by configuring the system to use Avaya Aura® MS as the authentication and authorization source for EM login.

Before you begin

The default EM administrator must have a password before you can select Avaya Aura® Media Server as the authentication and authorization source. Follow the procedure for modifying administrator properties to add a password to the admin user.

Procedure

1. Navigate to **EM** > **Account Management** > **Policies** > **Sign In**.
2. Select **Avaya Aura® Media Server** from the **Authentication and authorization source** drop-down menu.
3. **(Optional)** Configure the number of login attempt failures that disable an administrator account by selecting **Number of login failures that locks the account** and typing the required number of failures in the field.

   A value of 0 means there is no failure attempt limit.
4. **(Optional)** Configure how long a user session can be idle before EM ends the user session. In the **Element Manager session timeout interval (m)** field, type the number of minutes the session can be idle.
5. Click **Save**.
6. Click **Confirm**.

   The system restarts EM to apply the change. EM login sessions are ended. There is no impact to media server processing of call sessions. You can log in using Avaya Aura® MS RBAC credentials after the EM restart completes.

Related links

Modifying administrator properties on page 234

Configuring Avaya Aura® MS RBAC password policy

About this task

Perform the following procedure to update administrator password policies when you enable Avaya Aura® Media Server based RBAC. This task is not available unless you configure the system to use Avaya Aura® MS as the authentication and authorization source for EM login.

Procedure

1. Navigate to **EM** > **Account Management** > **Policies** > **Password**.
2. Configure the minimum password length and minimum number of different characters required.
3. To restrict an administrator from reusing passwords, enter the number of previous password to track in the **Number of unique passwords in the password history** field.

   The system uses the password history to ensure that new administrator passwords are not the same as recently used passwords.
4. To configure the number of days after which an administrator password expires, select the **Password expiration interval (d)** field and type the required number of days in the field.

   Value 0 indicates the password never expires.
5. To configure the minimum number of days allowed between password changes, select **Minimum password age (d)** and type the required number of days in the field.

   A minimum password age prevents password recycling that could otherwise defeat the password history policy.

   Value 0 disables the minimum password age restriction.
6. Click **Save**.

Related links

Modifying administrator properties on page 234

Adding roles

About this task

You can create roles for each administrator job function on your system. For each role you assign permission levels that define which EM tasks an administrator with that role can perform.

After you add a role, the role is available to be assigned to an administrator.

Use the Definitions for role permission levels table as an aid when selecting the permissions for each task in the role.

Definitions for role permission levels	
Property	**Description**
Deny	The system blocks the administrator from viewing or modifying the task.
View	The system allows the administrator to only view the task.
Modify	The system allows the administrator to view and modify the task.

Perform the following procedure to add a new role to the system:

Procedure

1. Log in to EM by using an administrator account. The administrator account must have the permission to modify account management tasks.

2. Navigate to **EM** > **Account Management** > **Roles**.
3. Click **Add**.
4. Type a name for the new role in the **Role ID** field.
5. Type a description for the new role in the **Role Description** field.
6. Set the permissions for the role by clicking **Configure**.
7. Select the role permission level from the drop-down menu next to each of the listed tasks.
8. Click **Continue**.
9. Click **Save**.

Modifying role properties

Procedure

1. Log in to EM by using an administrator account. The administrator account must have the permission to modify account management tasks.
2. Navigate to **EM** > **Account Management** > **Roles**.
3. Select the role you want to modify from the list of roles.
4. Click **Edit**.

   The system displays a page with the role properties and a list of administrators currently assigned to the role. Changes to the role impact the administrators in the list.
5. Change the name of the role by typing a new name in the **Role ID** field.
6. Change the description of the role by typing a new description in the **Role Description** field.
7. Change the permissions for the role by clicking **Configure**.
8. Change the role permission level for each task by selecting the new permission level from the drop-down menu next to each of the listed tasks.
9. Click **Continue**.
10. Click **Save**.

Deleting roles

Procedure

1. Log in to EM by using an administrator account. The administrator account must have the permission to modify account management tasks.
2. Navigate to **EM** > **Account Management** > **Roles**.
3. Select the role you want to delete from the list of roles.

Tip:

You can see how many administrators are using each role by looking in the **Number of Administrators** column.

If you want to review a list of the administrators currently assigned to the role you are about to delete, perform the following steps:

a. Click **Edit**.

b. Review the list of administrators.

c. Click **Delete**.

The system deletes the role and removes the role from each administrator assigned the role.

Adding administrators

Before you begin

Ensure the roles that are required for the new administrator are created.

Procedure

1. Log in to EM by using an administrator account. The administrator account must have the permission to modify account management tasks.
2. Navigate to **EM** > **Account Management** > **Administrators**.
3. Click **Add**.
4. Type a unique user name for the new administrator in the **Administrator ID** field.
5. Type a description for the new administrator in the **Administrator Description** field.
6. Select the required authentication source from the **Authentication Source** drop-down menu.
7. Select the required status of the account from the **Status** drop-down menu.

   If you select **Disabled** then the account is suspend and cannot be used to access EM.
8. Type a password for the new administrator in the **Password** and **Confirm Password** fields.
9. If you want the administrator to enter a new password after the first login, then select **Password Change Required**.
10. Assign roles to the administrator by clicking **Edit** in the **Roles** section.
11. Select the required roles from the **Roles** list.
12. Click **Continue**.
13. Click **Save**.

Modifying administrator properties

Procedure

1. Log in to EM by using an administrator account. The administrator account must have the permission to modify account management tasks.
2. Navigate to **EM** > **Account Management** > **Administrators**.
3. Select the administrator you want to modify.
4. Click **Edit**.
5. Change the description of the administrator by typing a new description in the **Administrator Description** field.
6. Select the required status of the account from the **Status** drop-down menu.

   If you select **Disabled** then the account is suspend and cannot be used to access EM.
7. If you want to change the password, type a new password for the administrator in the **Password** and **Confirm Password** fields.
8. If you want the administrator to enter a new password after the next login, then select **Password Change Required**.
9. Change the roles assigned to the administrator by clicking **Edit** in the **Roles** section.
10. Select the required roles from the **Roles** list.
11. Click **Continue**.
12. Click **Save**.

Deleting administrators

Procedure

1. Log in to EM by using an administrator account. The administrator account must have the permission to modify account management tasks.
2. Navigate to **EM** > **Account Management** > **Administrators**.
3. Select the administrator you want to remove.
4. Click **Delete**.

   The administrator account is removed from the system and cannot be used to access EM.

Changing administrator passwords

About this task

RBAC administrators perform the following procedure to update their passwords when you enable Avaya Aura® Media Server based RBAC. This task is not available unless you configure the system to use Avaya Aura® Media Server as the authentication and authorization source for EM login.

Procedure

1. Log in to EM by using Avaya Aura® MS RBAC administrator credentials.
2. Navigate to **EM** > **Account Management** > **Administrator Password**.
3. Type a new password for the new administrator in the **Password** and **Confirm Password** fields.
4. Click **Save**.

Related links

Modifying administrator properties on page 234

Resetting EM default admin password

About this task

If the Element Manager (EM) default admin password is unavailable, the administrators can reset it to the default password `Admin123$` in a Linux® shell using the emtool command.

```
emtool resetadminpassword
```

Note:

This command is to reset the password for the Avaya Aura® Media Server default administrator account admin.

Resetting EM login source

About this task

When authentication and authorization with System Manager Single Sign-On is either not available or not working for Element Manager (EM), the administrators can reset the EM authentication and authorization source to default, that is Avaya Aura® Media Server in a Linux® shell using the emtool command.

```
emtool resetloginsource
```

After the reset, the administrators can use the Avaya Aura® Media Server administrator accounts to access the EM.

Avaya Aura® System Manager RBAC configuration

You can use Role Based Access Control (RBAC) when you configure the account management policy to use Avaya Aura® System Manager as the authentication and authorization source.

System Manager provides centralized RBAC to manage the level of access the system grants to authorized administrators. RBAC simplifies permission management by assigning permissions to reusable roles instead of individual administrators. The System Manager authentication supports Single Sign-On (SSO).

Using RBAC requires that you create roles for each job function. Next, you define the permission level for each EM task in role. Finally, you can then assign roles that match the job function requirements of each administrator.

System Manager includes one default administrator with the name `admin`, and with the default role of System Administrator. The default administrator has full access to all levels of Avaya Aura® MS EM tasks. When using System Manager for authentication and authorization, administrators, roles, and permissions are configurable only on System Manager.

If you want to use System Manager with Avaya Aura® MS, you must set up a mutual authentication between the servers. After you setup mutual authentication, you must select the Avaya Aura® System Manager option as the authentication and authorization source to use System Manager RBAC and SSO.

Perform the procedures in this section to configure Avaya Aura® MS to use System Manager RBAC and SSO.

For information about configuring administrators and roles when using System Manager for centralized RBAC, see *Administering Avaya Aura® System Manager*.

Configuring Avaya Aura® MS to use System Manager

About this task

To configure the media server to use System manager, see System Manager enrollment on page 140.

Configuring System Manager as the authentication and authorization source

About this task

Perform the following procedure to enable System Manager based RBAC and SSO by configuring the system to use Avaya Aura® System Manager as the authentication and authorization source for EM login.

Before you begin

Ensure Avaya Aura® MS is configured to use System Manager.

Procedure

1. Navigate to **EM** > **Account Management** > **Policies** > **Sign In**.
2. Select the Avaya Aura® System Manager from the **Authentication and authorization source** drop-down menu.
3. Click **Save**.
4. Click **Confirm**.

   The system restarts EM to apply the change. EM login sessions are ended. There is no impact to media server processing of call sessions. You can login using the System Manager credentials after the EM restart completes.

Accessing Avaya Aura® MS EM when System Manager is not available

About this task

When System Manager is configured and enabled as the authentication and authorization source for EM login, but System Manager is unavailable, you can use the login credentials of the Avaya Aura® MS based authentication administrator to access Avaya Aura® MS EM.

Procedure

1. Use the following URL in a web browser for emergency access to Avaya Aura® MS EM:

   `https://AvayaMSFQDN:8443/emlogin`

2. If geo-redundant System Managers are available refer to the procedure to switch between primary and secondary System Manager.

Configuring security policies

Procedure

1. Gain access to System Manager that is configured to manage Avaya Aura® MS.

   If you are already logged in to Avaya Aura® MS EM, you can click on **Network** in the upper-left of EM to access System Manager.

2. Click **Administrators**.
3. Navigate to **Security** > **Policies**.

   For detailed steps on configuring policies in System Manager, see *Administering Avaya Aura® System Manager*.

Configuring roles

Procedure

1. Gain access to System Manager that is configured to manage Avaya Aura® MS.

   If you are already logged in to Avaya Aura® MS EM, you can click on **Network** in the upper-left of EM to access System Manager.

2. Click **Administrators**.
3. Navigate to **Security** > **Roles**.
4. Click the role you want to access from the list or click **Add** to create a new role.

   Use **Avaya Aura® Media Server** as the element or resource type when configuring roles.

   For detailed steps on adding, deleting or modifying roles in System Manager, see *Administering Avaya Aura® System Manager*.

Configuring administrators

Procedure

1. Gain access to System Manager that is configured to manage Avaya Aura® MS.

   If you are already logged in to Avaya Aura® MS EM, you can click on **Network** in the upper-left of EM to access System Manager.

2. Click **Administrators**.

   For detailed steps on adding, deleting, or modifying administrators in System Manager, see *Administering Avaya Aura System Manager*.

Switch from Primary SMGR to Secondary SMGR

About this task

If EM is using the primary System Manager and the primary is unavailable you can use this procedure to switch EM to use the secondary System Manager.

Procedure

1. Gain access to the Element Manager that is configured to manage the Primary node of the Avaya Aura® MS cluster by using the following emergency login URL:

   ```
   https://<AvayaMS_FQDN>:8443/emlogin
   ```

2. Navigate to **Security** > **System Manager** > **Advanced Settings** and ensure the following is configured.

   a. Specify the Secondary System Manager FQDN in the **Fully qualified domain name (FQDN) of Secondary System Manager server** field.

   b. Specify the Secondary System Manager port in the **Secondary System Manager server port** field.

   c. Ensure the field **Use Secondary System Manager server** field is checked.

3. Click **Save**.

4. To apply the change on each node of the cluster, access a Linux shell for each media server in the cluster and restart EM using the command:

   ```
   service avaya.em restart
   ```

Switch from Secondary SMGR to Primary SMGR

About this task

If EM is using the secondary System Manager and the secondary is unavailable you can use this procedure to switch EM to use the primary System Manager.

Procedure

1. Gain access to the Element Manager that is configured to manage the Primary node of the Avaya Aura® MS cluster by using the following emergency login URL: `https://<AvayaMS_FQDN>:8443/emlogin`.
2. Navigate to **Security** > **System Manager** > **Advanced Settings** and ensure the field **Use Secondary System Manager server** field is unchecked
3. Click **Save**.
4. To apply the change on each node of the cluster, access a Linux shell for each media server in the cluster and restart EM using the command: **`service avaya.em restart`**.

Updating the System Manager FQDN

About this task

To maintain uninterrupted service with the System Manager, the FQDN must be updated. Use this procedure to update the System Manager FQDN for a media server cluster, only if the System Manager FQDN has been changed and not the IP address or any other related configuration.

Procedure

1. Access the Element Manager (EM) that is configured to manage the Primary node of the Avaya Aura® MS cluster by using the following emergency login URL:

   https://AvayaMSFQDN:8443/emlogin
2. Navigate to **Security** > **System Manager** > **Advanced Settings** and update **Fully qualified domain name (FQDN) of System Manager server** with the new System Manager FQDN.
3. Click **Save**.
4. To apply the change on each node of the cluster, access a Linux shell for each media server in the cluster and restart the EM using the command:

   ```
   service avaya.em restart
   ```

   Important:

   Restart the EM service on every media server in the cluster.

Resetting EM login source

About this task

When authentication and authorization with System Manager Single Sign-On is either not available or not working for Element Manager (EM), the administrators can reset the EM authentication and authorization source to default, that is Avaya Aura® Media Server in a Linux® shell using the emtool command.

```
emtool resetloginsource
```

After the reset, the administrators can use the Avaya Aura® Media Server administrator accounts to access the EM.

Chapter 12: Troubleshooting

Element Manager troubleshooting

Note:

Element Manager (EM) works with recent versions of Chrome, Firefox, and Edge.

Cannot log into EM when using Avaya Aura® System Manager for authentication and authorization

You cannot gain access to EM when using Avaya Aura® System Manager for authentication and authorization.

A possible cause is that the FQDNs (Fully Qualified Domain Names) of System Manager and Avaya Aura® MS cannot be resolved from your computer.

Proposed Solution 1

Ensure that the FQDNs of System Manager and Avaya Aura® MS can be resolved through either DNS or the local hosts file.

Proposed Solution 2

If the FQDNs cannot be resolved using DNS or the local hosts file, then use the Avaya Aura® MS IP address to access the following specific URL for EM emergency login:

https://mediaServerIP:8443/emlogin

Proposed Solution 3

When System Manager is used for authentication and authorization, you must use the local operation system login credentials for EM emergency login.

Unable to access EM due to a password issue

You are unable to access EM due to an expired or lost password when using Avaya Aura® Media Server as the EM authentication source.

Proposed Solutions

- Use **emtool** to reset the authentication source and the default password for the administrative account.
- To reset the **Element Manager** default admin password to the default of `Admin123$`, use the following command in a Linux shell:

  ```
  emtool resetadminpassword
  ```

- To reset the **Element Manager** login source to the default operating system authentication, use the following command in a Linux shell:

  ```
  emtool resetloginsource
  ```

EM cannot upload files larger than 2-GB

You encounter errors when using EM to upload large files because many browsers have a 2-GB limit on file upload.

Proposed Solutions

- Use the latest versions of Chrome or Firefox. These browsers support file uploads greater than 2-GB.
- Use an alternate upload procedure, such as using a tool like sftp or scp to transfer the file to the server. After the file is on the server, move it to the correct location. For example, a backup file must be placed in the backups folder, as follows:

  ```
  $MASHOME/platdata/EAM/Backups
  ```

EM displays a blank page after login when using IE

After logging on to EM with valid credentials, you see a blank page. IE can block access to servers that are not in the trusted sites list. If the server you are connecting to is not in the trusted sites list, the browser does not display the EM pages.

Proposed Solution

Perform the procedure to add the Avaya Aura® MS to the trusted sites list in IE so that EM can display the pages.

Certificate error seen on IE when using EM

You see a certificate error message next to the URL field when using IE to access EM.

Proposed Solutions

Creating a self-signed certificate for EM

Procedure

1. Navigate to **EM** > **Security** > **Certificate Management** > **Key Store**.
2. In the **Key Certificates** section, click **Create New**.
3. Select **Self-Signed** from the **Signing authority** drop-down menu.
4. Configure the certificate fields and ensure that you use Avaya Aura® MS FQDN as the **Common Name**.

   For example, `Server1.companyXYZ.com`
5. Click **Save**.
6. Close all browser connections to EM and log in after EM restarts.
7. Click on the certificate error displayed in IE next to the URL.

   IE displays the Certificate Error window.
8. Click **View certificates**.

   IE displays the Certificate window.
9. On the **General** tab, click **Install Certificate**.

   IE displays the Certificate Import Wizard window.
10. Click **Next**.

    IE displays a dialog window.
11. Click **Finish**.

    IE displays a security warning.
12. Click **Yes**.

    IE displays a message that the certificate import was successful.
13. Click **OK**.
14. Click **OK**.
15. Close IE.
16. Open IE and log in to EM to verify the certificate error is not present.

Importing a CA certificate to IE

About this task

Import a certificate for EM HTTPS connections and import the CA certificate that signs the EM certificate in to IE.

Before you begin

Ensure that the certificate to import is in the PKCS12 format. Ensure that it uses the FQDN of Avaya Aura® MS for the common name in the certificate.

Procedure

1. Navigate to **EM** > **Security** > **Certificate Management** > **Key Store**.
2. In the **Key Certificates** section, click **Import**.

   EM displays the Import Certificate page.
3. In the **Password for certificate import** field, enter the certificate password.
4. Click **Browse** to navigate the file system and select the certificate for import.
5. Click **Save**.
6. Click **Confirm**.
7. Close all browser connections to EM and log in after EM restarts.
8. Open IE.
9. Navigate to **Tools** > **Internet Options**.
10. Select the **Content** tab.
11. Click **Certificates**.

    IE displays the Certificates window.
12. Select the **Trusted Root Certificate Authority** tab.
13. Click **Import**.

    IE displays the Certificate Import Wizard window.
14. Click **Next**.
15. Click **Browse** and select the trust certificate of Certificate Authority. The certificate must be in PKCS12 format.
16. Click **Next**.
17. Type the password for the private key.
18. Click **Next**.
19. Select **Place all certificates in the following store**.
20. To set the Certificate store to **Trusted Root Certification Authorities**, click **Browse** .
21. Click **Next**.
22. Click **Finish**.

    IE displays a security warning.
23. Click **Yes**.

    IE displays a message that the certificate import was successful.

24. Click **OK**.
25. Close IE.
26. Open IE and log in to EM to verify the certificate error is not present.

    Ensure that you use an FQDN in the login URL. For example:

    `https://amsServer1.companyXYZ.com:8443/em`

Downloading a trust certificate revocation list fails

Condition

After clicking Download CRL on the **EM** > **Security** > **Certificate Management** > **Trust Store** page, you see an error that the system could not download the certificate revocation list (CRL) from the trust store.

Cause

Possible causes for this problem include:

- A connection failure because of incomplete mutual authentication configuration between Avaya Aura® MS EM and the server hosting the CRL
- An import failure has occurred after the CRL is downloaded. CRL formats other than DER are not supported and cannot be imported.

Proposed Solutions

Resolving a connection failure:

Ensure that there is correct mutual authentication configuration between Avaya Aura® MS EM and the server hosting the CRL by performing the following imports:

- Import the CA Certificate that signs the key certificate for the server hosting the CRL into the Avaya Aura® MS trust store.
- Import the CA Certificate that signs the key certificate for the AMS Clustering service into the trust store of the CRL server.

Resolving import failures:

Perform the following procedure to ensure that the CRL distribution point URI and CRL format are correct:

1. Determine the CRL distribution point URI in the CA certificate. You can do so by using the following OpenSSL command to view the certificate contents and obtain the URI:

   `openssl x509 -text -noout -in` *`certfilename`*

2. Copy the CRL distribution point URI from the certificate and paste it into the URL field of a browser.

   The CRL downloads if the CRL distribution point URI is valid. If the download fails, the CRL distribution point URI is invalid or obsolete.

3. If the CRL distribution point URI downloads, then verify the format of CRL. DER files are binary. PEM files are Base64 encoded.
4. Avaya Aura® MS supports the DER format. If the file is in PEM format, you can convert the PEM file to DER format by using the following OpenSSL command:

   ```
   openssl crl -in inputfile -outform DER -out outputfile
   ```

   For example:

   ```
   openssl crl -in crl.pem -outform DER -out crl.der
   ```

5. Perform the following procedure to manually import the DER formatted:
   a. Navigate to **EM** > **Security** > **Certificate Management** > **Trust Store**.
   b. Select the required trust store certificate authority from the list.
   c. Click **Import CRL**
   d. Click **Browse** and select a file to set the **Trust certification revocation list import file** field.
   e. Click **Save**.

VeriSign cannot sign a CSR generated by EM

Condition

VeriSign reports an error when you try to sign a certificate signing request (CSR) whichthat was generated by Avaya Aura® MS EM.

VeriSign rejects a CSR as improperly formatted when the CSR contains a Subject Alternative Name extension. VeriSign considers an included Subject Alternative Name extension as a separate certificate and requires fees to for each additional Subject Alternative Name extension included.

Proposed solutions

- If you do not require a Subject Alternative Name extension in the CSR, then generate the CSR in EM without specifying a Subject Alternative Name extension.
- If you require a Subject Alternative Name extension in the CSR, use the VeriSign website to add the Subject Alternative Name extensions required.

The EM Media Management tool is slow

You can experience slow system response times when browsing media using **EM** > **Tools** > **Media Management**.

A possible cause for this problem is that you have installed anti-virus software on the system and that Avaya Aura® MS related directories are not in the scan exclusion list.

Proposed solution

If you install anti-virus software, ensure that you exclude the following directories from the scans:

- Linux®:

  ```
  $MASHOME/avaya/ma/MAS/common/log
  ```

  ```
  $MASHOME/avaya/ma/MAS/platdata
  ```

Backup task running from EM failed

Condition

You see in **Tools** > **Backup and Restore** > **History Log** EM page that some backup task has failed during execution.

Possible causes for the backup failure are:

- Remote host name or IP address is incorrect or not accessible.
- User credentials for remote host are incorrect.
- Destination path does not exist or user has no rights to write data under it.
- Remote host fingerprint is incorrect or not the top priority.

Resolving backup failures

Perform the following steps to find the cause of failure:

1. Enable debug logs in EM.
2. Run failed backup task again.
3. Download troubleshooting archive.
4. Extract the archive and open ElementManagerDebug.txt from it, then scroll to time of task execution and find output of pscp_mod tool.

Analyzing output and resolving issue

Check if the output contains one of the following:

1. Network error: No route to host – ip address or hostname of remote host you use for backup is incorrect or it may be down. Check that the host is correctly configured and alive.
2. Is not a valid format for a manual host key specification – check that the fingerprint that you have entered in the backup destination is correct.
3. Host key did not appear in manually configured list – fingerprint you used in configuration is not supported by pscp_mod or not the top priority. Use another fingerprint according to description of backup destination configuration.
4. Access denied – credentials you have entered are incorrect. Check that user login and password for remote server are valid and reconfigure destination with it.
5. Unable to open <destination path>/<backup file> – destination path you have entered does not exist on remote server. Create it manually or change to another existing path.

6. Unable to open <destination path>/<backup file> : permission denied – destination path you have entered exists, but account you use for backup does not have write permissions. Change directory permissions for user or use another path.

Remove stale media server cluster and server data in System Manager

Condition

When the media servers are configured to work with System Manager, it may occur that the media server cluster and server data in System Manager becomes invalid or stale. This situation would occur when administrators make change to the media server cluster configuration before first disenrolling the media server cluster from System Manager.

Proposed Solutions

Use the utility script **`aamsdatautils.sh`** on System Manager to clean up the stale media server cluster and server data from System Manager database.

Important:

The script must be run as root.

Procedure

1. Get the cluster names, server names, and server IP addresses for cleanup.
2. SSH to the System Manager server. Change user to root. Change work directory to `/opt/Avaya/mediaserver/utils`.
3. Run the script.

   For example:

   ```
   ./aamsdatautils.sh --cleanup "cluster 1,cluster 2" "amsName 1,amsName 2" 10.100.200.1,10.100.200.2
   ```

   or

   ```
   ./aamsdatautils.sh --cleanup cluster1,cluster2 amsName1,amsName2 10.100.200.1,10.100.200.2
   ```

4. Log into System Manager web console. Navigate to the **Elements** > **Media Server** > **Cluster Administration** and **Elements** > **Media Server** > **Server Administration** to verify the media server cluster and server data has been properly cleaned up.

   Note:

   - Ensure to get the correct cluster names, media server names, and media server IP addresses for cleanup. Administrators can check the information through System Manager **Elements** > **Media Server** > **Cluster Administration** and **Elements** > **Media Server** > **Server Administration**.
   - If a cluster name or a server name contains a whitespace, use single or double quotes to enclose the whole cluster name or server name input.

- Multiple cluster names, server names, and server IP addresses are separated by a comma ‘,’.
- The utility script can only properly handle whitespaces in cluster and server names starting with System Manager future releases 8.1.3.8 and 10.1.3.1. For removing stale media server data with whitespaces in earlier System Manager releases, contact Avaya support for assistance.

Call completion troubleshooting

Avaya Aura® MS rejects incoming SIP sessions

Avaya Aura® MS rejects SIP sessions in the following manner:

- Avaya Aura® MS rejects incoming SIP sessions for one or more service types. Use the Log Viewer to identify attempts to launch an uninstalled or unlicensed service.
- Avaya Aura® MS rejects incoming SIP sessions. You see SIP failure responses such as 305 Use Proxy, or 403 Forbidden, in the message traces or logs.

Possible causes for these problems include:

- Calls to services on Avaya Aura® MS that are not licensed, receive a SIP final response indicating that the service is unavailable.
- The proxy configuration is incomplete.
- The target service application is not installed.
- Avaya Aura® MS is in the Pending Lock state.

Proposed solution

Checking the license

About this task

Perform the following procedure to ensure that the required licenses are configured:

Procedure

1. To check the number and variety of installed licenses, navigate to **EM** > **Licensing** > **General Settings** > **Licensing Details**.

   Ensure that the required licenses are installed and available.

   If you need to alter the license configuration, see License configuration on page 60.
2. Restart Avaya Aura® MS to activate any installed license.

Related links

License configuration on page 60

Checking proxy configuration

About this task

Perform the following procedure to verify whether the required SIP proxy nodes and routes are configured:

Procedure

1. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **SIP** > **Nodes and Routes**.
2. Ensure that you have configured the required **Trusted Nodes**.
3. Ensure that you have configured the required **SIP Routes**.

   If you need to add trusted SIP nodes or SIP routes, see the procedures for SIP configuration.

Related links

SIP configuration on page 87

Checking application installation

About this task

If you have not installed a required application then the requests for that application fail.

Perform the following procedure to ensure that you have installed and unlocked the required applications:

Procedure

1. Navigate to **EM** > **Applications** > **Packaged Applications**, and ensure that the target service is installed.

   If necessary, install the application using the application installer.
2. Navigate to **EM** > **Applications** > **Operational State** and ensure that the target service is unlocked.

   If necessary, unlock the application by selecting the check box next to the desired application and then click **Unlock**.

Checking if Avaya Aura® MS is in the Pending Lock state

About this task

Avaya Aura® MS in the Pending Lock state rejects new service requests. If this state is not required, then you can resolve the issue by unlocking Avaya Aura® MS as described in the following procedure:

Procedure

1. Navigate to **EM** > **System Status** > **Element Status** to check the state of Avaya Aura® MS.
2. Set the Avaya Aura® MS state to the Unlocked state by selecting **More Actions** > **Unlock**.

TLS connection issues

Clients using Transport Layer Security (TLS) are unable to connect to Avaya Aura® MS.

The possible causes for TLS connection issues include:

- The certificates on either side of the attempted connection have expired.
- The Trust Anchor configuration is incomplete.
- All the nodes in a cluster are not TLS enabled.
- The IP address of the server is changed.
- The configuration is incomplete or pending a restart.
- A backup file containing expired certificates or incorrect TLS configuration settings was restored.

Proposed solution

See proper security configuration documents and ensure that all settings are implemented correctly.

Some common solutions for these problems include:

- Ensure that certificates on either side of the attempted connection did not expire.
- Ensure that the Trust Anchor is in the Trust Store on all cluster nodes.
- Ensure that all nodes in a cluster are TLS enabled for every interface.
- When the IP address of a server changes, new certificates may be required if `subject alt name` is used.
- If a restoration, using a backup file containing expired certificates or outdated TLS configuration settings was used, then fix the TLS configuration.
- Some TLS changes require an Avaya Aura® MS restart for the changes to take effect.
- Confirm that the media security settings meet the requirements. For more detailed information, see Media security configuration.

Related links

Media security configuration on page 120

Digit collection issues

Users are unable to log in to Avaya Aura® MS services because of problems with digit connection.

The possible reasons for digit collection issues include:

- The client may connect to Avaya Aura® MS through a PSTN or other form of internet gateway device. In this case you must configure the gateway device to properly translate digits in a format that negotiates with Avaya Aura® MS. The following are the supported digit signaling formats:
  - In-band DTMF tones

  - RFC 2833 telephone events
  - SIP INFO digits
- To communicate digits, the client and the gateway device must use the same digit signaling formats.
- Some gateways that translate in-band digits into events, such as telephone-event or INFO digits, fail to completely clamp the received tones. These tones are heard by Avaya Aura® MS and can trigger unexpected behavior.
- If necessary, collect SIP messaging to resolve the nature of digit communication issue between the client, gateway, and Avaya Aura® MS.
- In some cases, such as conferencing, clients unintentionally send digits into the conference through their microphone. The system detects these digits as conference controls in the conference. For example, a person near a conference user dials a number on a speakerphone. The digits can carry in the conference over the microphone of the active user.
- When users report digit collection issues, ask about the client type and surroundings to identify the cause of any unexpected conference behaviors.

Proposed solutions

- Configure the mode of digit transport from the clients or gateways or both for your installation. Digit translating gateway devices might require adjustments in order to fully clamp in-band DTMF tones.
- Analyze traces to ensure that clients and gateways are properly communicating digits to Avaya Aura® MS.
- Advise users in noisy surroundings to ensure minimal background noise as the background noise might impact digit collection.

Quality of Service (QoS) Troubleshooting

Most networks experience periodic packet loss and congestion at some point, even if they are highly managed. Some codecs are more susceptible to packet loss than others due to their algorithmic design, but some basic rules can be followed to increase resiliency and quality. It is strongly recommended to use 20ms ptime for all codecs to help increase packet stream resiliency and lower latency. Using ptimes such as 30ms or 60ms increases end-to-end delay and reduces resiliency to packet loss, which in turn can impact QoS. Using higher ptimes for bandwidth savings is often not worth the tradeoff.

It is also important to note, some codecs suffer from excessive tandem encoding degradation even in perfect network conditions. This occurs when multiple media hops are present in the network, and a codec is decoded and encoded again at each hop before being sent on towards the remote endpoint. This degradation can be severe enough that just one tandem encode can reduce voice quality. G.729 is especially susceptible to tandem encoding degradation and should be used with caution when multiple media hops are present in the network.

Warning or Critical QoS alarms

Possible reasons for QoS alarms include:

- The endpoint client may be having difficulties in generating a good packet stream.
- The endpoint client NIC may be misconfigured or dropping packets
- Missing or incorrect DSCP setting in Avaya Aura® MS configuration
- Missing or incorrect DSCP settings or policies in network routers or switches
- The network routers and switches between the client and the Avaya Aura® MS may be overloaded, dropping packets
- The Codec selected by the client may not produce a quality audio experience at the network packet loss rate
- Avaya Aura® MS may have been installed on a virtual machine (VM) that is improperly configured
- Avaya Aura® MS NIC is dropping packets or incorrectly configured.

Proposed solutions

- Examine endpoint client to ensure it is producing a quality packet stream.
- Examine endpoint client NIC driver or configuration.
- Examine Avaya Aura® MS DSCP setting to ensure they match the network policy
- Examine client and network switch and routers settings to ensure they enforce the expected packet prioritization.
- Examine network configuration to ensure network is not causing unexpected loss due to congestion or other factors
- Choose higher quality Codecs compatible with network loss rate specification.
- If Avaya Aura® MS is installed on a Virtual Machine, improper VM resource allocation/ reservation can cause packets to be lost in the oncoming network drivers. Refer to “Deploying and Updating Avaya Aura® Media Server Appliance FP1” and follow all requirements and recommended best practices for VM configuration.
- Examine Avaya Aura® MS server NIC configuration.
- If the QoS alarms are determined to be due to Codec preference and network configuration decisions that cannot be changed, the options are:
  - Disable the QoS alarm, removing a useful warning of unexpected network problems.
  - Decrease thresholds for QoS warning or critical states such that normal observed levels of quality degradation do not trigger the alarms.
  - Increase numbers of sessions allowed in the warning or critical states before raising alarms.

Media playback troubleshooting

Unable to playback provisioned audio file

Proposed solution

Avaya recommends that audio to be played by Avaya Aura® Media Server be encoded as 16 bit, 8 kHz, single channel, PCM files. Codecs other than PCM or using higher sampling rates for higher quality recordings can be used, however, with reduced system performance. Multiple channels, like stereo, are not supported.

Streaming music troubleshooting

Problems with streaming music provider status

The EM page for monitoring music stream status indicates problems with a music provider. The color of the Stream Key for a music provider indicates the status of the provider. If the status is a color other than green and has a status other than **Stream is available**, then there is a potential problem with the stream.

Proposed solution

User the following table to identify solutions for each music provider error.

Status	Possible cause	Proposed solution
Stream staus is unknown	Stream is initializing after being configured.	Normal Condition. No action required.
Stream is available	The stream is providing audio.	Normal Condition. No action required
At least one configured URL is currently unreachable.	The primary or backup URL provider is unreachable.	Check connectivity to the configured URLs. Configure another provider if the provider cannot be reached. Configure an HTTP proxy for external music source access
Primary URL is not reachable, using backup URL.	The primary URL failed and the backup URL is being used. The media server does switch back to the primary URL until the media server is restarted or the backup URL fails.	Check that the primary URL can be reached. If it cannot then consider using a different primary provider URL. Configure an HTTP proxy for external music source access.

Table continues…

Status	Possible cause	Proposed solution
All streaming servers are unreachable, currently using a pre-recorded backup file.	The provider URLs are unreachable. Up to 15 minutes of audio recorded from the provider is being played in a loop. At least 30s of audio must have been previously captured from the provider to enable recorded audio playback as a backup.	Check the connection to the provider URLs and consider using a different provider if the connection cannot be established. Configure an HTTP proxy for external music source access.
Stream status is pending.	The stream has been initialized and the connection to the provider is being attempted.	Wait for a momentary status change indicating the result of the connection attempt.
The configured stream has no files provisioned.	There are no media files in the channel folder for the stream.	MP3 or WAV files need to be added to Local Directory or Content Store provider.
The connection to a streaming server was lost.	An active connection to the provider has failed.	Verify the configured URL is correct. Determine if the provider is reachable and returns playlist documents. A provider may have gone offline based on its daily schedule. Select providers that are always available.
The RSS document has no usable or valid files for synchronization.	The RSS provider has no useable media content that can be downloaded and played.	Select an RSS provider that has native MP3 or WAV content.
The RSS document is invalid.	The RSS provider XML document cannot be parsed.	Choose another RSS provider.
Configured proxy server unreachable.	The SHOUTcast provider HTTP proxy is unavailable.	Diagnose connectivity with the SHOUTCast HTTP proxy.
Streaming server playlist invalid or unreachable.	An HLS master playlist file contains an unreachable media playlist.	Diagnose the HLS provider master playlist for media playlists that are unreachable Resolve connection issues. Configure a different HLS provider. Configure an HTTP proxy for external music source access

For detailed steps for testing SHOUTCast and RSS connections, see Users do not hear streaming SHOUTCast audio on page 256 and Users do not hear streaming RSS audio on page 257.

Related links

Monitoring music streams on page 216

Configuring an HTTP proxy for external music source access on page 127
Users do not hear streaming RSS audio on page 257
Users do not hear streaming SHOUTCast audio on page 256

Users do not hear streaming SHOUTCast audio

Users do not hear audio form the configured SHOUTCast source or you see the following alarm:

Alarm ID 361: There is a problem communicating with the SHOUTCast providers.

The possible causes for the problem are:

- Improper configuration.
- The configured SHOUTCast URL is unavailable or unreachable.
- The RSS document is incorrectly formatted.
- The audio provided by the configured SHOUTCast URL is not in MP3 or WAV audio format.

Proposed solution

Check the SHOUTCast configuration:

- Ensure that the SHOUTCast URL and channel key are correct.
- Ensure that the SHOUTCast proxy server host and port configuration are correct.
- Ensure that the streaming source is in either MP3 or WAV audio format and that all of the other requirements are met. See Adding a streaming music source on page 127 for a complete list of requirements.
- Ensure that the SHOUTCast URL is reachable from the media server by attempting to resolve the URL from the media server. To do this, you can use wget or cURL with the configured SHOUTCast URL.

The following is a successful wget example:

```
wget http://yp.shoutcast.com/sbin/tunein-station.pls?id=227567
--2014-01-06 18:52:59--  http://yp.shoutcast.com/sbin/tunein-station.pls?id=227567
Resolving webproxy.avaya.com... 8.28.150.65
Connecting to webproxy.avaya.com |8.28.150.65|: 80... connected.
Proxy request sent, awaiting response... 200 OK
Length: 5080 (5.0K) [audio/x-scpls]
Saving to: `tunein-station.pls?id=227567.2'
2014-01-06 18:53:00 (157 KB/s) - `tunein-station.pls?id=227567.2'
saved [5080/5080]
```

The following is a successful cURL example:

```
curl http://yp.shoutcast.com/sbin/tunein-station.pls?id=227567
[playlist]
numberofentries=45
File1=http://95.141.24.96:80
Title1=(#1 - 44/1000) ChartHits.FM - Top 40 Radio - Mega Hot Music!
Length1=-1
File2=http://95.141.24.58:80
Title2=(#2 - 45/1000) ChartHits.FM - Top 40 Radio - Mega Hot Music!
Length2=-1
Version =2
```

Related links

Music streaming configuration on page 124

Users do not hear streaming RSS audio

The possible causes for this problem are:

- Improper configuration.
- The configured RSS URL is unavailable or unreachable.
- The audio files specified in the RSS document not in MP3 or WAV audio format.

Proposed Solution

Check the RSS configuration:

- Ensure that the RSS URL and channel key are correct.
- Ensure that the audio files specified in the RSS document are in either MP3 or WAV audio format and that all of the other requirements are met. See Adding a streaming music source on page 127 for a complete list of requirements.
- Ensure that the RSS document is formatted correctly. The following is an example of an RSS document with correct formatting:

```
<?xml version="1.0" encoding="UTF-8"?>
<rss version="2.0">
  <channel>
    <title>Relaxing Music</title>
    <description>Example RSS Music Playlist</description>
    <language>en-us</language>
    <ttl>15</ttl>
    <item>
      <title>Corporate Edge - A Clear Vision</title>
      <enclosure url="http://musicserver/Music/DavenportMusic-0.wav" type="audio/
wav"/>
      <guid>35942909-51f1-11e5-b4f5-00ffb0699410</guid>
      </item>
    <item>
      <title>Corporate Edge - First Impressions</title>
      <enclosure url="http://musicserver/Music/DavenportMusic-1.wav" type="audio/
wav"/>
      <guid>3edcc894-51f1-11e5-b4f5-00ffb0699410</guid>
      </item>
    <item>
      <title>Kaleidoscope - Shades of Blue</title>
      <enclosure url="http://musicserver/Music/DavenportMusic-2.wav" type="audio/
wav"/>
      <guid>47779c66-51f1-11e5-b4f5-00ffb0699410</guid>
      </item>
     <item>
      <title>Keynotes - Colors</title>
      <enclosure url="http://musicserver/Music/DavenportMusic-3.wav" type="audio/
wav"/>
      <guid>ea3dd092-51f1-11e5-b4f5-00ffb0699410</guid>
     </item>
     <item>
      <title>Kalimb<A/title>
      <enclosure url="http://musicserver/Music/Kalimba.mp3" type="audio/mpeg"/>
      <guid>3e789aa0-cb7b-11e5-b904-18a9051819e8</guid>
     </item>
```

```
   </channel>
</rss>
```

- Ensure the RSS URL is reachable from the media server by attempting to resolve the URL from the media server. To do this, you can use wget or cURL with the configured RSS URL.

  The following is a successful wget example:

```
wget http://xyz.com/audio/rss/feed.xml
--2014-01-06 18:39:24--  http://xyz.com/audio/rss/feed.xml
Resolving webproxy.avaya.com... 8.28.150.65
Connecting to webproxy.avaya.com|8.28.150.65|:80... connected.
Proxy request sent, awaiting response... 200 OK
Length: 1025790 (1002K) [text/xml]
Saving to: `feed.xml'
2014-01-06 18:39:27 (2.85 MB/s) - `feed.xml' saved [1025790/1025790]
```

The following is a successful cURL example:

```
curl http://xyz.com/audio/rss/feed.xml
BBB?xml version="1.0" encoding="UTF-8" ?>
BBBrss xmlns:itunes="http://www.itunes.com/DTDs/Podcast-1.0.dtd" version="2.0">
  BBBchannel>
   . . .
  BBB/channel>
BBB/rss>
```

Proposed solution

Check the RSS configuration:

- Ensure that the RSS URL and channel key are correct.
- Adjust the continuous streaming source volume level on the media server.
- Ensure that the audio files specified in the RSS document are in either MP3 or wav audio format.
- Ensure the RSS URL is reachable from the media server by attempting to resolve the URL from the media server. To do this, you can use wget or cURL with the configured RSS URL.

The following is a successful wget example:

```
wget http://xyz.com/audio/rss/feed.xml
--2014-01-06 18:39:24--  http://xyz.com/audio/rss/feed.xml
Resolving webproxy.avaya.com... 8.28.150.65
Connecting to webproxy.avaya.com|8.28.150.65|:80... connected.
Proxy request sent, awaiting response... 200 OK
Length: 1025790 (1002K) [text/xml]
Saving to: `feed.xml'
2014-01-06 18:39:27 (2.85 MB/s) - `feed.xml' saved [1025790/1025790]
```

The following is a successful cURL example:

```
curl http://xyz.com/audio/rss/feed.xml
<?xml version= "1.0" encoding= "UTF-8" ?>
<rss xmlns:itunes= "http://www.itunes.com/DTDs/Podcast-1.0.dtd"
version="2.0">
<channel>
...
<channel>
</rss>
```

High Availability troubleshooting

Cannot enable High Availability because it is disabled

When you navigate to **EM** > **Cluster Configuration** > **High Availability** > **General Settings**, you cannot select **Enable High Availability**.

You can select **Enable High Availability** only if the prerequisite High Availability configuration is complete, that is, a Primary and Backup server must be configured.

Proposed Solution

Perform the prerequisite High Availability configuration procedures in the correct order. For detailed information, see 1+1 High Availability cluster configuration on page 39.

Related links

1+1 High Availability cluster configuration on page 39

Protocol troubleshooting

SNMP Traps are not getting posted on Network Management Station (NMS)

SNMP Traps are not posting to the NMS.

The possible causes for this problem include:

- Network connectivity problems or firewall rules.
- SNMP configuration mismatch.
- SNMP Delivery is not enabled.
- An incorrect SNMP network manager address or port.

Proposed solution

Checking the network

About this task

Perform the following procedure to confirm there are no network problems between the monitoring system and Avaya Aura® MS:

Procedure

1. Verify that the monitoring system and Avaya Aura® MS can ping each other.
2. If the ping test fails, troubleshoot the network connection between the monitoring system and Avaya Aura® MS.

Checking the SNMP configuration

Procedure

Ensure that the configuration for the trap route (destination and user) matches the configuration defined on NMS.

Related links

Editing a SNMP User on page 77

Editing a SNMP Trap Destination on page 79

Editing a SNMP Trap Route on page 81

SNMP delivery is not enabled

Procedure

Ensure that SNMP delivery is enabled.

Incorrect SNMP network manager address

Procedure

Ensure that the destination address and port is correctly configured for the SNMP trap route.

SOAP connection is rejected

A provisioning or management system cannot connect to Avaya Aura® MS SOAP interface.

Possible causes for this problem include:

- The SOAP configuration is not complete.
- The remote server is not in the **SOAP Trusted Nodes** list when you enable the use of **Trusted SOAP Nodes** on Avaya Aura® MS.
- The SOAP server address or port used is incorrect or has changed in one of the endpoints.

Proposed solution

About this task

Perform the following procedure to verify SOAP configuration on Avaya Aura® MS and on the management system which is attempting to connect to Avaya Aura® MS.

Procedure

1. For basic SOAP configuration details, see Configuring SOAP on page 66 and then perform the following checks:
   a. Verify that each setting of the SOAP configuration on Avaya Aura® MS is compatible with the settings of the system which is attempting to connect to Avaya Aura® MS.
   b. Verify that the system which is attempting to connect to Avaya Aura® MS is in the **SOAP Trusted Nodes** list. This is required when you select **Enable Trusted SOAP Nodes**.

2. Check that the ports configured for SOAP on Avaya Aura® MS match the SOAP ports configured on the system which is attempting to connect to Avaya Aura® MS.
    a. Navigate to **EM** > **System Configuration** > **Network Settings** > **Advanced Settings** > **Port Assignments**.
    b. Scroll down to **Management SOAP Server**.
    c. Verify the **admin_soap_tls** port value.
    d. Verify the **admin_soap** port value.

Related links

Configuring SOAP on page 66

Chapter 13: Related resources

Media Server documentation

The following table lists the documents related to Media Server. Download the documents from the Avaya Support website at https://support.avaya.com.

Title	Description	Audience
Overview		
Avaya Aura® Media Server Overview and Specification	Describes the key features of Media Server	Customers and sales, services, and support personnel
Implementing and administering		
Deploying and Updating Avaya Aura® Media Server Appliance	Deploy, update, and troubleshoot Avaya Aura® Media Server appliances deployed in the VMware® virtualized environment or on Avaya Solutions Platform.	System administrators, implementation engineers, and support personnel
Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS	Install, upgrade, and patch software-only version of Avaya Aura® Media Server on customer provided hardware platform.	System administrators, implementation engineers, and support personnel
Implementing and Administering Avaya Aura® Media Server	Deploy update, upgrade and patch, non-appliance versions of Avaya Aura® Media Server deployed on Platform Vendor Independent (PVI) servers.	System administrators, implementation engineers, and support personnel
Performance Measurements Reference Avaya Aura® Media Server	Evaluate system performance metrics. Troubleshoot events and alarms.	System administrators, implementation engineers, and support personnel
Using		
Using Web Services on Avaya Aura® Media Server	Develop web services to provision and manage Avaya Aura® Media Server	Avaya Professional Services and application developers

Related links

Finding documents on the Avaya Support website on page 263
Accessing the port matrix document on page 263
Avaya Documentation Center navigation on page 264

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
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 only displays the documents for the selected category.
7. Click **Enter**.

Related links

Media Server documentation on page 262

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support by Product** > **Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or both the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

   The list displays the product-specific Port Matrix document.
7. Click **Enter**.

Related links

Media Server documentation on page 262

Avaya Documentation Center navigation

For some programs, the latest customer documentation is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

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

Using the Avaya Documentation Center, you can:

- Search for keywords.

  To filter by product, click **Filters** and select a product.

- Search for documents.

  From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.

- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** ( ).

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

  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.

- Add yourself as a watcher using the **Watch** icon ( ).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

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

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.

- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the website. The available functionality depends on your role.

Related links

Media Server documentation on page 262

Training

The following courses 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
20980W	What's New with Avaya Aura®
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components

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.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

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

Related links

Using the Avaya InSite Knowledge Base on page 266

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.

Related links

Support on page 266

Index

A

B

C

D

E

F

H

I

L

M

N

P

Q

R

S

T

U

V

W