



White Paper

Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager Issue 1.1

Abstract

This white paper documents the required steps pertaining to adding Avaya Aura® Media Servers (MS) to Communication Manager (CM). Additional sections cover adding announcements using Media Server, configuring Media Server High Availability as well as some maintenance activities. This is not intended to be comprehensive documentation on all aspects of CM or Media Server operation and management.

Issue 1.1 adds content on how to do “Stream Provisioning” on the media-server and how to access these streams on CM via a “Live Stream Source” announcement.

© 2018 Avaya Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <http://support.avaya.com> or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means a 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 IF YOU PURCHASE A 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, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://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. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

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

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

software virtual machine ("VM") or similar deployment.

License type(s)

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

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

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

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

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

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

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

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

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: <http://support.avaya.com/Copyright> or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

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

Note to Service Provider

The product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <http://support.avaya.com> or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

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, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website:

<http://support.avaya.com>, or such successor site as designated by Avaya.

Contact Avaya Support

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

Introduction

This quick start guide describes all the configuration steps that are needed in order to have CM operate with Media Server. Configuration steps are presented in the order they should be done and include required administration on CM, Media Server and System Manager.

Contents

Introduction	7
Required Releases	9
Media Server Licenses and WebLM configuration on Media Server	10
Media Server Channel Licenses and CM license file	12
CM and Media Server Configuration Settings	13
CM node-names administration	13
CM signaling-group administration	13
Media Server Configuration of SIP trusted nodes	15
CM media-server administration.....	16
Announcement Provisioning	18
Enrolling Media Server into System Manager	18
Communication Manager administration of Media Server announcements	26
Placing announcements onto Media Server.....	27
Provisioning Announcements using System Manager	28
Viewing Announcement Status from Communication Manager	34
Viewing Announcement Status from Media-Server Element Manager	35
Provisioning a Music-on-Hold Stream Source	37
Provisioning a Stream Source on CM	37
Provisioning a Stream Source on the Media Server	38
Monitoring a Stream Source via the Media Server Element Manager	39
Configuring Communication Manager Survivable Servers in a Media Server environment	40
Communication Manager maintenance commands for Media Server	41
Status media-server.....	41
List media-server	41
Media-server traffic reports	43
Collecting debug logs from Media Server	44
Communication Manager MST traces with Media Server	46
Collecting the MST trace.....	46
Interpreting the MST trace	47
Analyzing Communication Manager/Media Server SIP Messages	48
SIP/SDP media establishment messages.....	48
Associating Media Server SIP media establishment sessions with a specific user.....	49
SIP INFO messages and MSML commands.....	51
Media Server configuration for High Availability Operation	52
Media Server configuration with Prognosis for RTCP monitoring	56
Media Server Element Manager System Monitoring	57
Media Server Element Manager Element Status	62

Required Releases

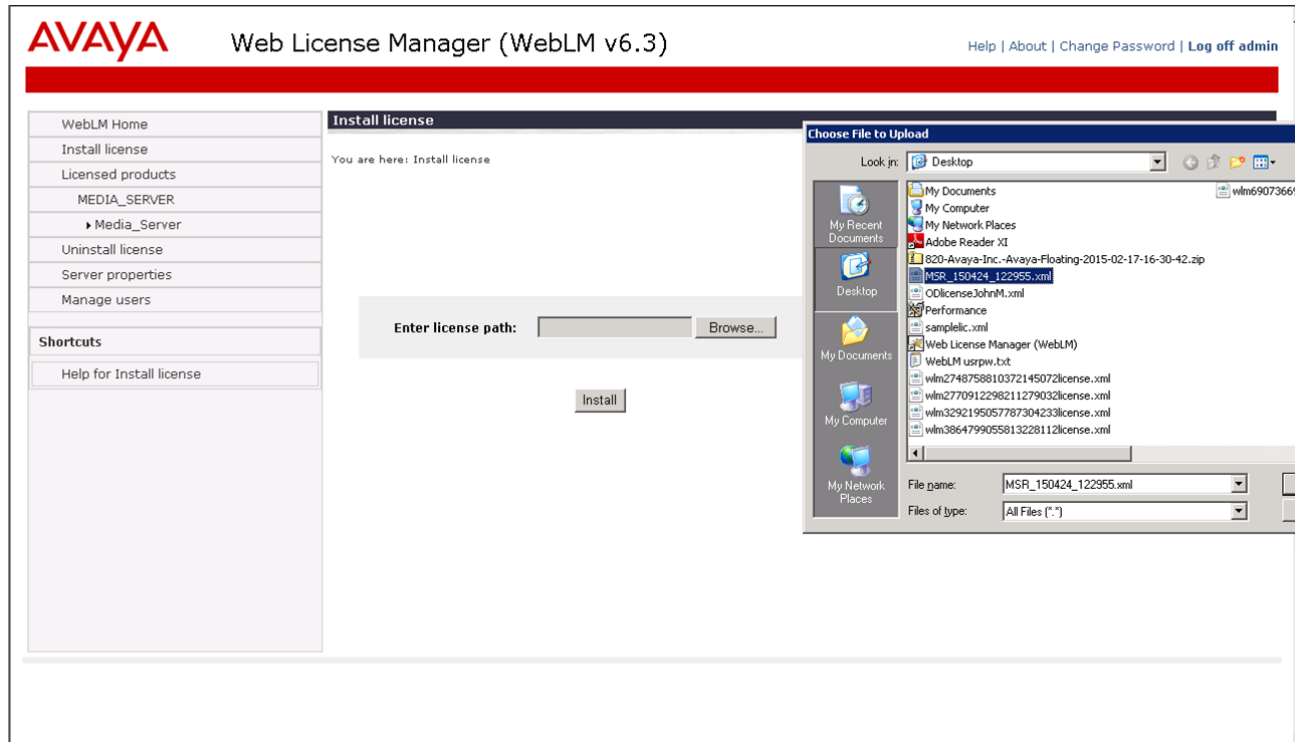
In order for Communication Manager to use Media Server, Communication Manager must be release 7.0 or newer and the Media Server must be release 7.7 or newer.

This whitepaper assumes CM and any Media Servers have already been loaded with the correct software releases.

Media Server Licenses and WebLM configuration on Media Server

Each Media Server instance in a deployment must obtain a server instance license from a WebLM server. This applies to each physical or virtual Media Server. The WebLM license server must contain a license instance or count for every Media Server deployed.

On the WebLM server, install the license by going **'Install License'**, clicking the **'Browse'** button, and select the file that contains the Media Server license.



Once a media server license is installed successfully on the WebLM server it should look like the screen shot below. The capacity of VALUE_MSR_SERVER_INSTANCES should at least match the number of Media Servers in your network.



WebLM Home	Media Server - Release: 7 - SID: 82	Standard License file								
Install license	You are here: Licensed Products > Media_Server > View License Capacity									
Licensed products	License installed on: July 14, 2015 1:35:28 PM -05:00									
MEDIA_SERVER	License Owner: Test 1234 TEST LN TEST KRW SALT LAKE CITY UT 84101 United States License Host: 00-0C-29-49-7A-78 Notes: This production license file is for use on a production license host. License File Host IDs: 00-0C-29-49-7A-78									
Media_Server	Licensed Features 2 Items Show ALL <table border="1"> <thead> <tr> <th>Feature (License Keyword)</th> <th>Expiration date</th> <th>Licensed capacity</th> <th>Currently Used</th> </tr> </thead> <tbody> <tr> <td>Maximum Media Server Instances VALUE_MSR_SERVER_INSTANCES</td> <td>permanent</td> <td>50</td> <td>50</td> </tr> </tbody> </table>		Feature (License Keyword)	Expiration date	Licensed capacity	Currently Used	Maximum Media Server Instances VALUE_MSR_SERVER_INSTANCES	permanent	50	50
Feature (License Keyword)	Expiration date	Licensed capacity	Currently Used							
Maximum Media Server Instances VALUE_MSR_SERVER_INSTANCES	permanent	50	50							
View license capacity										
View peak usage										
Uninstall license										
Server properties										
Manage users										
Shortcuts										
Help for Installed Product										

Each Media Server must be configured to point to the WebLM server.

1. Using the Media Server Element Manager, navigate to **Home >> Licensing >> General Settings**
2. Select '**WebLM Server**' from the '**Licensing**' drop down menu then enter the appropriate data for the WebLM server.
3. Click "**Save**".

Avaya Aura® Media Server
[Help](#) | [Sign Out](#) **cust**

Managing: b31h-asm1.avaya.com, 10.129.130.136
[Home](#) » [Licensing](#) » General Settings

General Settings

Licensing : **WebLM Server**

Server Host Name or IP Address:

Server Port:

URL Suffix:

If a Media Server is unable to initially obtain a server instance license, it shall not accept service requests from Communication Manager. If a Media Server is unable to renew its server instance license, it will enter license error mode and continue to operate normally for a grace period of 30 days.

Media Server Channel Licenses and CM license file

A standard CM license file must be obtained by CM from a WebLM server.

The CM license file must enable “Avaya Media Server VoIP Channels” via inclusion of the feature keyword “**VALUE_CM_AMS_VOIP_CHLS**” with an associated number. This determines the total number of simultaneous AAMS channels that CM may establish across all media-servers and corresponds to the number of AAMS channel licenses purchased.

The number of “**Avaya Media Server VoIP Channels**” may be displayed via the CM command “**display capacity**” and is visible on page 10.

display capacity		Page 10 of 14		
SYSTEM CAPACITY				
TOTAL LICENSED CAPACITY		Used Available		License Limit

Survivable Processor Capacity:		0	313	313
Avaya Media Server VoIP Channels:		0	40000	40000

The “**License Limit**” column represents the number of Media Server channel licenses purchased. The “**Used**” column represents the number of Media Server channels currently established and “**Available**” represents the number of channel licenses that are available for additional channels.

CM and Media Server Configuration Settings

This section describes the administration or configuration settings that must be used on both CM and Media Server in order for CM to make requests of Media Server and have Media Server satisfy those requests. These steps should be done in the order presented for each Media Server to be deployed.

CM node-names administration

Begin by adding a node-name entry for the specific Media Server on the node-names form. Enter “**change node-names ip**” and enter the IP address of each Media Server.

change node-names ip		Page 2 of 2
IP NODE NAMES		
Name	IP Address	
sst1-ams1	172.31.0.241	
sst1-ams2	172.31.0.242	
sst1-ams3	172.31.0.243	

CM signaling-group administration

Each Media Server requires administration of a separate SIP signaling-group.

For use with Media Server the signaling-group must use

- **Group type:** sip
- **Transport Method:** tcp or tls (Note: **tls** is the preferred method. If using **tls**, the default staging certificates should be replaced with customer provided certificates.)
- **Peer Detection Enabled?** n
- **Peer Server:** AMS
- The **Near-end Node Name:** is not administrable and will be set to “**procr**”.
- The **Far-end Node Name:** This is one of the node-name entries added onto the node-names form. Setting the Far-end Node Name shall cause the Far-end Domain: to be set to the associated IP address.
- The **Near-end Listen Port:** and **Far-end Listen Port:** will default to values depending on the selection of **tcp** or **tls** for the Transport Method. These ports may be changed to other values if desired.
- The **Far-end Network Region:** defines where this Media Server resides within the ip-network-region topology representation of the customer network and must be populated with a value between 1 and 250.

```
display signaling-group 501
```

Page 1 of 2

SIGNALING GROUP

Group Number: 501 Group Type: sip
 Transport Method: tls

Peer Detection Enabled? n Peer Server: AMS

Near-end Node Name: procr	Far-end Node Name: sst1-ams1
Near-end Listen Port: 9061	Far-end Listen Port: 5061
	Far-end Network Region: 5

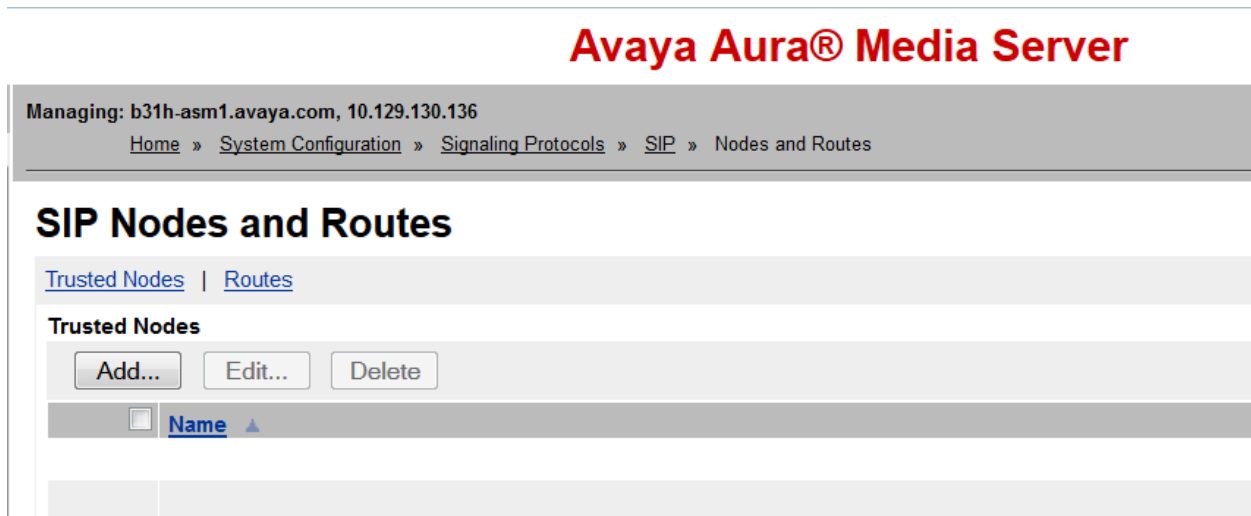
Far-end Domain: 172.31.0.241

Media Server Configuration of SIP trusted nodes

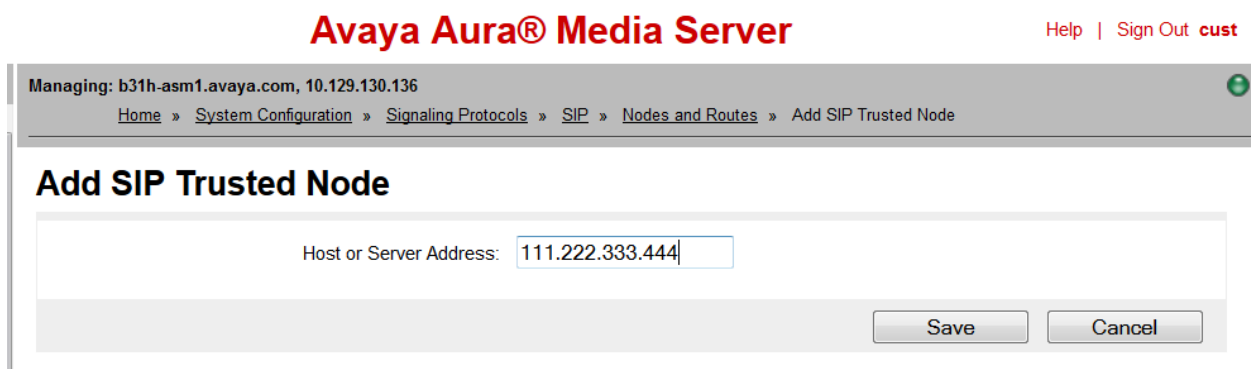
If the associated CM Media Server SIP signaling group administered in the previous step uses the Transport Method: **tcp**, then the configuration of SIP trusted nodes on Media Server is **required**. This step is must be skipped if the transport method **tls** is used.

Configuring a SIP trusted node on Media Server is done using the Media Server element manager.

1. Using the Media Server element manager, navigate to **Home >> System Configuration >> Signaling Protocols >> SIP >> Node and Routes**
2. Click **“Add”**.



3. Enter the CM **procr** interface IP address in the **‘Host or Server Address’** field and click **‘Save’**.



NOTE: If AMS SIP signaling groups use **tcp** and if the customer deployment has backup survivable CM servers, then the procr interface IP address of each survivable server must be added as a SIP trusted note in order for the survivable to access this specific Media Server. This is yet another reason to prefer use of **tls**.

CM media-server administration

After an Media Server specific SIP signaling-group has been created, an individual Media Server is added to CM using the “**add media-server X**” command.

```
display media-server 1
```

MEDIA SERVER	
Media Server ID:	1
Signaling Group:	501
Voip Channel License Limit:	
Dedicated Voip Channel Licenses:	
Node Name:	sst1-ams1
Network Region:	5
Location:	1
Announcement Storage Area:	

This form maps an individual Media Server to an individual SIP signaling-group and defines how CM communicates to a specific Media Server.

The media-server id (1-250) is entered as the last parameter of the “add media-server” command. On the media-server form:

- The **Signaling Group**: must be set to the signaling-group number created with the Far-End Node Name/IP address of the new media-server. In this example we used signaling-group 501 to communicate with media-server 1.
- The **Voip Channel License Limit**: is an optional field which can be used to limit the number of simultaneous channels established on this specific media-server.
- The **Dedicated Voip Channel Licenses**: is an optional field which can be used to reserve or dedicate some number of Media Server channel licenses to this specific media-server.

The remaining fields on the media-server form are not customer administrable.

- The **Node Name**: and **Network Region**: fields are taken from the associated signaling-group form.
- The **Location**: value is taken from the location field specified on the associated ip-network-region form.
- The **Announcement Storage Area**: field exists only if announcements have been administered to reside on this Media Server and is described in the section on **CM administration of AMS announcements**

No additional configuration is required on Media Server or CM. Media Server and CM should now

be able to communicate and Media Server may be used by CM to terminate IP audio calls. Many additional configuration screens are accessible on Media Server via the element manager. However no other configuration is required on Media Server. Of specific note are the “Media Processing” pages. Modification to these pages has no impact on CM/ Media Server operation. In general these parameters are controlled by CM’s ip-codec-set settings and are negotiated on a call by call basis.

Adding or removing **codecs** from

- **Home»System Configuration»Media Processing»Audio Codecs**

will not impact the audio codecs available to CM when establishing Media Server media sessions.

Adding or removing **Digit Relay** modes from

- **Home»System Configuration»Media Processing»Digit Relay(DTMF)**

will not change which DTMF transmission modes CM may use.

Changing the **Security Policy** or checking/unchecking **Crypto Suites** from

- **Home»System Configuration»Media Processing»Media Security**

will not change which media encryption options CM may use.

In order to remove a media-server you must first busyout the associated Media Server SIP signaling group. Then the “**remove media-server**” command may be executed.

Announcement Provisioning

Enrolling Media Server into System Manager

Each Media Server needs to be enrolled with System Manager so that CM announcements may be provisioned via System Manager.

- Note: If this is a Media Server High Availability configuration then HA cluster configuration should be performed prior to doing the enrollment. See the section on “**Media Server configuration for High Availability Operation**”.

Enrollment consists of the following steps:

- On each primary Media Server perform the enrollment process for each 1+1 HA cluster or standalone Media Server.
- Application cluster assignment on System Manager.

Note: System Manager refers to Media Server using cluster nomenclature. In Release 7.0, Communication Manager only supports clusters of standalone Media Server servers or High Availability 1+1 clusters. Media Server documentation will also refer to N+1 clusters and master clusters. These cluster configurations are not supported in Communication Manager Release 7.0 and should not be used when configuring Media Server to work with Communication Manager.

After enrollment is completed System Manager Role Based Access Controls and Single Sign On features will be enabled. Enrollment is initiated by accessing

- **Security>>System Manager>>Enrollment**

and clicking the ‘**Begin Enrollment**’ button (shown below). Note you need to ensure that both the Media Server and System Manager FQDN are resolvable to an IP address prior to starting the enrollment process.

The screenshot displays the Avaya Aura Media Server web interface. The top header includes the Avaya logo, the title "Avaya Aura® Media Server", and links for "Help", "Sign Out", and "root". Below the header, a breadcrumb trail shows the navigation path: "Home » Security » System Manager » Enrollment". The left sidebar contains a navigation menu with categories like "Session Detail Records", "Content Store", "Logging Settings", "Debug Tracing", "Engineering Parameters", "Element Manager Settings", "Licensing", "Tools", "Security", and "Account Management". The main content area is titled "System Manager Enrollment" and contains the following text:

Enroll this media server and media server cluster peers with System Manager by using this enrollment task to perform the following steps:

1. Enter the administrative names and descriptions of the media servers in the cluster.
2. Enter the required System Manager parameters.
3. Enter the data for a System Manager-signed certificate.
4. Verify the entered information and complete the enrollment.

Ensure that the following data are available before starting the System Manager enrollment process:

- System Manager server Fully Qualified Domain Name (FQDN).
- System Manager server port.
- A valid System Manager administrative account username and password.
- System Manager Trust Management enrollment password.

At the bottom of the main content area, there are two buttons: "Begin Enrollment..." and "Cancel".

As shown below you need to specify an **Administrative name** and **Administrative description** of each cluster and its media servers being enrolled. Please note that the administrative name for both the media server and cluster must be unique among all clusters/media servers currently enrolled with System Manager.

Once this is done click the **'Next'** button to proceed to step 2 of the enrollment.

Avaya Aura® Media Server

Help | Sign Out root

Managing: server5088-vm06.richlab.avaya.com, 135.60.77.221

Home » Security » System Manager » Enrollment

System Manager Enrollment

Step 1 of 4: Enter the cluster and element administrative information for the media server cluster.
The administrator defines the administrative names and descriptions of the media servers and the cluster. This information helps identify the media servers in a complex environment.

Cluster

Administrative name: (maximum: 128 characters)

Administrative description: (maximum: 1024 characters)

Servers

Server Name	Server Role	Element Administrative Name	Element Administrative Description
server5088-vm06	Primary	aams1	Primary AAMS for the east cluster. x

Reenroll

Warning: Reenrollment replaces existing node and cluster configuration on the configured System Manager.

Reenroll the media server cluster: ☐

Next Cancel

Copyright 2010-2015 Avaya Inc. All Rights Reserved

As shown below in the **'Server Configuration'** specifies the System Manager FQDN and its port. If this System Manager provides Geographic Redundancy, you must specify the FQDN of the secondary System Manager.

In the **'Administrative Account'** section specify the System Manager administrative account credentials that will be used to register the media server's with System Manager.

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.

Once all the information is entered click the **'Test Connection'** button to verify connection to System Manager. If the connection is successfully established the **'Next'** button will be activated. Click the **'Next'** button to proceed to step 3.



Avaya Aura® Media Server

[Help](#) | [Sign Out](#) [root](#)

- + Monitoring
- Applications
 - Operational State
 - Signalling Translations
- Cluster Configuration
 - High Availability
 - Server Designation
 - Replication Settings
 - Load Balancing
 - Advanced Settings
- System Configuration
 - + Server Profile
 - + Network Settings
 - + Signalling Protocols
 - + Media Processing
 - + Application Interpreters
 - + Monitoring Settings
 - + Session Detail Records
 - + Content Store
 - + Logging Settings
 - + Debug Tracing
 - + Engineering Parameters
 - + Element Manager Settings
- Licensing
 - General Settings
 - Monitoring
 - Server Status
 - [Utilization Threshold](#)
 - Advanced Settings
- Tools
 - + Manage Software
 - PVI Results
 - + Backup and Restore
 - Media Management
 - Session Detail Record Browser
 - Log Capture
- Security
 - General Settings
 - + Certificate Management
 - System Manager
 - Enrollment
 - Advanced Settings
- Account Management
 - Administrators
 - Roles
 - Policies

Managing: server5088-vm06.richlab.avaya.com, 135.60.77.221
[Home](#) » [Security](#) » [System Manager](#) » [Enrollment](#)

System Manager Enrollment

Step 2 of 4: Enter System Manager parameters. Click Test Connection to verify System Manager server and account configuration and to continue the enrollment process.

Server Configuration

Provide the information required by the media server to connect to the System Manager server.

Fully qualified domain name (FQDN) of System Manager server:

System Manager server port: (0 - 65535)

Fully qualified domain name (FQDN) of Secondary System Manager server:

Secondary System Manager server port: (0 - 65535)

Use Secondary System Manager server: ☐

Administrative Account

Provide the System Manager administrative account that the media server must use to send data to the System Manager.

System Manager registration username: (maximum: 32 characters)

System Manager registration password: (maximum: 32 characters)

Confirm password: (maximum: 32 characters)

Trust Management

Provide the enrollment password that the media server must use to acquire a System Manager-signed certificate from System Manager Trust Management.

System Manager trust management enrollment password:

Confirm password:

Verification

Click Test Connection to verify the entered System Manager server and account configuration.

Copyright 2010-2015 Avaya Inc. All Rights Reserved

In step 3 (shown below) specify information about the SMGR signed certificate that will be generated. Click the **'Next'** button to proceed to step 4.



Avaya Aura® Media Server

[Help](#) | [Sign Out](#) root

Managing: server5088-vm06.richlab.avaya.com, 135.60.77.221
[Home](#) » [Security](#) » [System Manager](#) » [Enrollment](#)

- + Monitoring
- Applications
 - Operational State
 - Signaling Translations
- Cluster Configuration
 - High Availability
 - Server Designation
 - Replication Settings
 - Load Balancing
 - Advanced Settings
- System Configuration
 - + Server Profile
 - + Network Settings
 - + Signaling Protocols
 - + Media Processing
 - + Application Interpreters
 - + Monitoring Settings
 - + Session Detail Records
 - + Content Store
 - + Logging Settings
 - + Debug Tracing
 - + Engineering Parameters
 - + Element Manager Settings
- Licensing
 - General Settings
 - Monitoring
 - Server Status
 - Utilization Threshold
 - Advanced Settings
- Tools
 - + Manage Software
 - + PVI Results
 - + Backup and Restore
 - + Media Management
 - + Session Detail Record Browser
 - + Log Capture
- Security
 - General Settings
 - + Certificate Management
 - System Manager
 - Enrollment
 - Advanced Settings
- Account Management
 - Administrators
 - Roles
 - Policies

System Manager Enrollment

Step 3 of 4: Enter the field data for the certificate signed by the configured System Manager.

Certificate friendly name: server5088-vm06_server4925smgrSigned

Key bit length:

Signature algorithm:

Organization:

Organization unit:

Common name: server5088-vm06.richlab.avaya.com

Country (ISO 3166):

State/Province (full name):

City/Locality:

Copyright 2010-2015 Avaya Inc. All Rights Reserved

In step 4 (shown below) all information related to the enrollment will be displayed. Verify that it is correct and then press the **'Next'** button to enroll. Click the **'Previous'** button to go back and update any information that is not correct.

The Element Manager displays a spinner during the enrollment process. After the enrollment completes, the system restarts the media server management related services (including the EM service). Close the EM browser window or tab. You can sign in again to EM after the EM service restart completes.



Managing: server5088-vm06.richlab.avaya.com, 135.60.77.221
[Home](#) » [Security](#) » [System Manager](#) » [Enrollment](#)

System Manager Enrollment

Step 4 of 4: Verify the System Manager enrollment information.

Cluster and Elements

The administrative names and descriptions of the media server cluster and elements.

Cluster administrative name: AAMS East Cluster
 Cluster administrative description: Media server cluster located in the east wing.

Server Name	Server Role	Element Administrative Name	Element Administrative Description
server5088-vm06	Primary	aams1	Primary AAMS for the east cluster.

System Manager Configuration

Fully qualified domain name (FQDN) of System Manager server: server4925smgr.richlab.avaya.com
 System Manager server port: 443
 System Manager registration username: admin
 System Manager registration password: *****
 System Manager trust management enrollment password: *****

Certificate Setup

Certificate friendly name: server5088-vm06_server4925smgrSigned
 Key bit length: 2048
 Signature algorithm: SHA256
 Organization: Avaya
 Organization unit: Development
 Common name: server5088-vm06.richlab.avaya.com
 Country (ISO 3166): US
 State/Province (full name): Texas
 City/Locality: Coppell

Summary

Previous Enroll Cancel

Copyright 2010-2015 Avaya Inc. All Rights Reserved

AVAYA

Avaya Aura® Media Server

Help | Sign Out root

Managing: server5088-vm06.richlab.avaya.com, 135.60.77.221

Home » Security » System Manager » Enrollment

- + Monitoring
- Applications
 - Operational State
 - Signaling Translations
- Cluster Configuration
 - High Availability
 - Server Designation
 - Replication Settings
 - Load Balancing
 - Advanced Settings
- System Configuration
 - + Server Profile
 - + Network Settings
 - + Signaling Protocols
 - + Media Processing
 - + Application Interpreters
 - + Monitoring Settings
 - + Session Detail Records
 - + Content Store
 - Logging Settings
 - + Debug Tracing
 - Engineering Parameters
 - Element Manager Settings
- Licensing
 - General Settings
 - Monitoring
 - Server Status
 - Utilization Threshold
 - Advanced Settings
- Tools
 - + Manage Software
 - PVI Results
 - + Backup and Restore
 - Media Management
 - Session Detail Record Browser
 - Log Capture
- Security
 - General Settings
 - + Certificate Management
 - System Manager
 - Enrollment
 - Advanced Settings
- Account Management
 - Administrators
 - Roles
 - Policies

Enrollment Complete

The System Manager enrollment is complete.

All Element Manager sessions will end momentarily. You must close your Element Manager browser window or tab. You can connect to Element Manager again in about three minutes.

Copyright 2010-2015 Avaya Inc. All Rights Reserved

Once the Media Servers are reenrolled you need to specify the clusters that will be used by Communication Manager. This assignment is done in System Manager under **Home/Elements/Media Server/Application Assignment**.

AVAYA

Aura® System Manager 7.0

Cluster Admini...

Last Logged on at April 22, 2015 9:37 AM

Log off admin

HomeMedia Server

Media Server

Cluster Administration

Server Administration

Application Assignment

Home / Elements / Media Server / Application Assignment

Application Assignment

Manage applications and media server clusters.

CommitCancel

Cluster Name	Communication Manager	Engagement Development Platform
AAMS East Cluster	☐	☐

CommitCancel

Communication Manager administration of Media Server announcements

Administration of announcements sourced by Media Server use the same Communication Manager “announcement” and “audio-group” forms as legacy TN2501 VAL boards and media gateway announcements. A Media Server-sourced announcement is entered on these forms as M1 through M250 (for media-server 1 through media-server 250). Unlike media-gateway announcements, media-servers do not require an “enable announcement-board” command to enable them; media-servers are enabled automatically after the first announcement is administered. Media Servers may source announcements that can be used by Communication Manager for the same features as legacy VAL sources. This includes announcements as music sources for music-on-hold, or announcements used in vectors.

```
display announcement 33335
```

ANNOUNCEMENTS/AUDIO SOURCES

```

Extension: 33335          COR: 1
Annc Name: Sale-of-the-day  TN: 1
Annc Type: integrated     Queue? n
Source: M2
Protected? n

```

```
change audio-group 3
```

Page 1 of 5

AUDIO GROUP 3

Group Name: HQandBranchAnncSources

AUDIO SOURCE LOCATION

1: <u>01A10</u>	16: _____	31: _____	46: _____	61: _____	76: _____
2: <u>011V9</u>	17: _____	32: _____	47: _____	62: _____	77: _____
3: <u>012V9</u>	18: _____	33: _____	48: _____	63: _____	78: _____
4: <u>013V9</u>	19: _____	34: _____	49: _____	64: _____	79: _____
5: <u>M1</u>	20: _____	35: _____	50: _____	65: _____	80: _____
6: <u>M2</u>	21: _____	36: _____	51: _____	66: _____	81: _____
7: _____	22: _____	37: _____	52: _____	67: _____	82: _____
8: _____	23: _____	38: _____	53: _____	68: _____	83: _____
9: _____	24: _____	39: _____	54: _____	69: _____	84: _____
10: _____	25: _____	40: _____	55: _____	70: _____	85: _____
11: _____	26: _____	41: _____	56: _____	71: _____	86: _____
12: _____	27: _____	42: _____	57: _____	72: _____	87: _____
13: _____	28: _____	43: _____	58: _____	73: _____	88: _____
14: _____	29: _____	44: _____	59: _____	74: _____	89: _____
15: _____	30: _____	45: _____	60: _____	75: _____	90: 

Announcements may also be administered with System Manager. Refer to the section “Provisioning Announcements using System Manager”.

Placing announcements onto Media Server

Media Server supports a variety of file formats for announcements. For ease of management the same files that may exist on legacy VAL boards should be used on Media Server.

Because Media Server may possibly be shared by other Communication Managers, each Communication Manager's announcement files are placed in a different storage area on a shared Media Server. (On Media Server this storage area is referred to as a "content-group".) This storage area is a unique name created by Communication Manager when the first announcement using any Media Server is administered. This storage area identifier is permanent and becomes part of Communication Manager's translation. It is not customer configurable and is visible only for informational purposes. This identifier never needs to be referenced by a system administrator. The **Announcement Storage Area** assigned to the specific Communication Manager may be seen on any "media-server" form. An example is shown here:

```
display media-server 4
```

MEDIA SERVER	
Media Server ID:	4
Signaling Group:	303
Voip Channel License Limit:	
Dedicated Voip Channel Licenses:	
Node Name:	clchauVMams2
Network Region:	250
Location:	
Announcement Storage Area:	ANNC-00208f24-4f60-e401-0e00-545505bd0000

The announcement file must be placed onto Media Server. This may be done by recording the announcement from a station using the announcement recording feature-access-code or more generally via the System Manager VAL manager capabilities.

Provisioning Announcements using System Manager

System Manager supports centralized provisioning of announcements on Communication Manager. The announcements may be sourced on Media Server as well as legacy VAL boards and media gateways. The actions presented here apply to any Communication Manager announcement source.

Announcements on System Manager are available under

- **Home -> Elements-> Communication Manager -> Call Center-> Announcements.**

Having already selected the specific Communication Manager to manage, and click on the ‘**show list**’ button to list all announcements configured on Communication Manager on all announcement sources.

AVAYA
Aura® System Manager 7.0

Announcements * | Go... | Log off admin

Home | Inventory * | Communication Manager * | Licenses *

Home / Elements / Communication Manager / Call Center / Announcements

Search

Status

Announcements [Switch to Classic View]

Select device(s) from Communication Manager List

Show List

Announcement List

View Edit New Delete More Actions

Advanced Search

139 Items Show 15 Filter: Enable

	Name	Extension	Source	Type	Protected	Rate	COR	Tenant Number	Queue	Size	TimeStamp	System
☐	Test-1	31013	M1	integrated	n(o)		1	1	y(es)	2876	2015-07-22 06:21:56.0	CM-182.14
☐	Test-2	80024	M1	integrated	n(o)		1	1	y(es)	6548	2015-07-22 06:21:11.0	CM-182.14
☐	Test-3	8010003	001V9	integrated	n(o)	64	1	1	y(es)	18	2015-07-21 23:38:10.0	CM-182.14
☐	Test-5	8080002	001V9	integrated	n(o)	64	1	1	y(es)	102	2015-07-21 23:36:04.0	CM-182.14
☐	Test-4	8080004	001V9	integrated	n(o)	64	1	1	y(es)			CM-182.14
☐	Test-6	8080006	001V9	integrated	n(o)	64	1	1	y(es)			CM-182.14
☐	Test-7	8080027	M1	integrated	n(o)		1	1	y(es)			CM-182.14
☐	Test-8	80023	M19	integrated	n(o)		1	1	y(es)			CM-182.14
☐	Test-9	80021	M19	integrated	n(o)		1	1	y(es)			CM-182.14
☐	Test-11	80006	M7	integrated	n(o)		1	1	y(es)			CM-182.14
☐	Test-10	80007	M1	integrated	n(o)		1	1	y(es)	6548	2015-07-22 06:09:39.0	CM-182.14

Click '**New**' to configure a new announcement. Enter the name of announcement which should be the same as the audio file (.wav) being uploaded on to the Media Server or VAL or media-gateway. Select an available extension from the drop down and type of announcement.

In the **Basic Information** section, select the source which the announcement will be uploaded to. If uploading to a Media Server select the Media Server # (M1-M250). Specify any other required parameters such as **Protected**, **Class of Restriction (COR)**, **Tenant Number (TN)**, and **Queue**. In the **Audio File Information** section, select the audio file which is to be uploaded or select an already uploaded, unused file from the drop down so that it will get associated with the selected extension on Communication Manager.

AVAYA
Aura® System Manager 7.0

Home Inventory Communication Manager Licenses

Home / Elements / Communication Manager / Call Center / Announcements

Search

Status

New Announcement

Commit Schedule Clear Cancel

System CM-182.14

* Name Test-1

* Extension 31013

* Type Integrated

Basic Information | Audio File Information |
Expand All | Collapse All

Basic Information

* Source M1

Protected n(o)

* COR 1

* Tenant Number 1

Queue y(es)

Audio File Information

Use Unused wave file

Upload Audio File Browse Test-1.wav

Note: Audio File Name will override the Announcement Name.

From announcements page, other operations such as view, edit, delete may be executed. To edit more than one announcement at a time, select the announcement rows which are to be edited, this will allow editing of values inline. The **More Actions** -> **Save** button will save updated fields permanently on Communication Manager.

System Manager also supports backup of one or more announcements from any Communication Manager announcement source. From the **Announcements** page select **More Actions -> Backup**. To take a backup of all announcements configured on a specific Communication Manager, the Backup All option is used. These backup files can be downloaded on to a client machine (laptop/desktop) for future use.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left sidebar contains a navigation menu with options like Communication Manager, Call Center, Agents, Announcements, Audio Group, Best Service, Routing, Holiday Table, Media Server, Variables, Vector, Vector Directory, Number, Vector Routing, Table, Service Hours, Tables, Coverage, Element Cut-Through, Endpoints, Groups, Network, and Parameters. The main content area displays the 'Announcements' page. A modal dialog box titled 'Download Backed-up Announcement' is open, showing a table of backed-up announcements. The table has three columns: Announcement Name, Board Name, and Extension. The data rows are as follows:

Announcement Name	Board Name	Extension
Test-1.wav	M1	
Test-2.wav	M1	
Test-1	M1	31013
Test-2	M1	80024

The dialog also includes a search bar, a 'Download' button, and a 'Done' button. The background interface shows the 'Announcements' page with a search bar and a 'Status' indicator.

The **More Actions** -> **Restore** option, allows you to restore the announcements which have been backed up for Communication Manager. While restoring, you can select the backup file from System Manager or can upload the backup zip file from a client machine.

AVAYA
Aura® System Manager 7.0

Home | Inventory | **Communication Manager** | Licenses

Home / Elements / Communication Manager / Call Center / Announcements

Search

Status

Restore Announcement

Restore Schedule Cancel

Select a CM from the following list

1 Item Found Filter: Disable, Apply, Clear

Element Name	FQDN/IP Address	Last Sync Time	Sync Type	Sync Status	Location	Software Version
CM-182.14	148.147.182.14	Jul 22, 2015 11:15:51 AM +0530	Incremental	Completed		R017x.00.0.432.0

Select : None

Restore Options

☐ Restore Announcement Properties
☐ Restore Wave Files
☒ Restore Both (Announcement Properties with associated wave file)
☐ Restore From Client

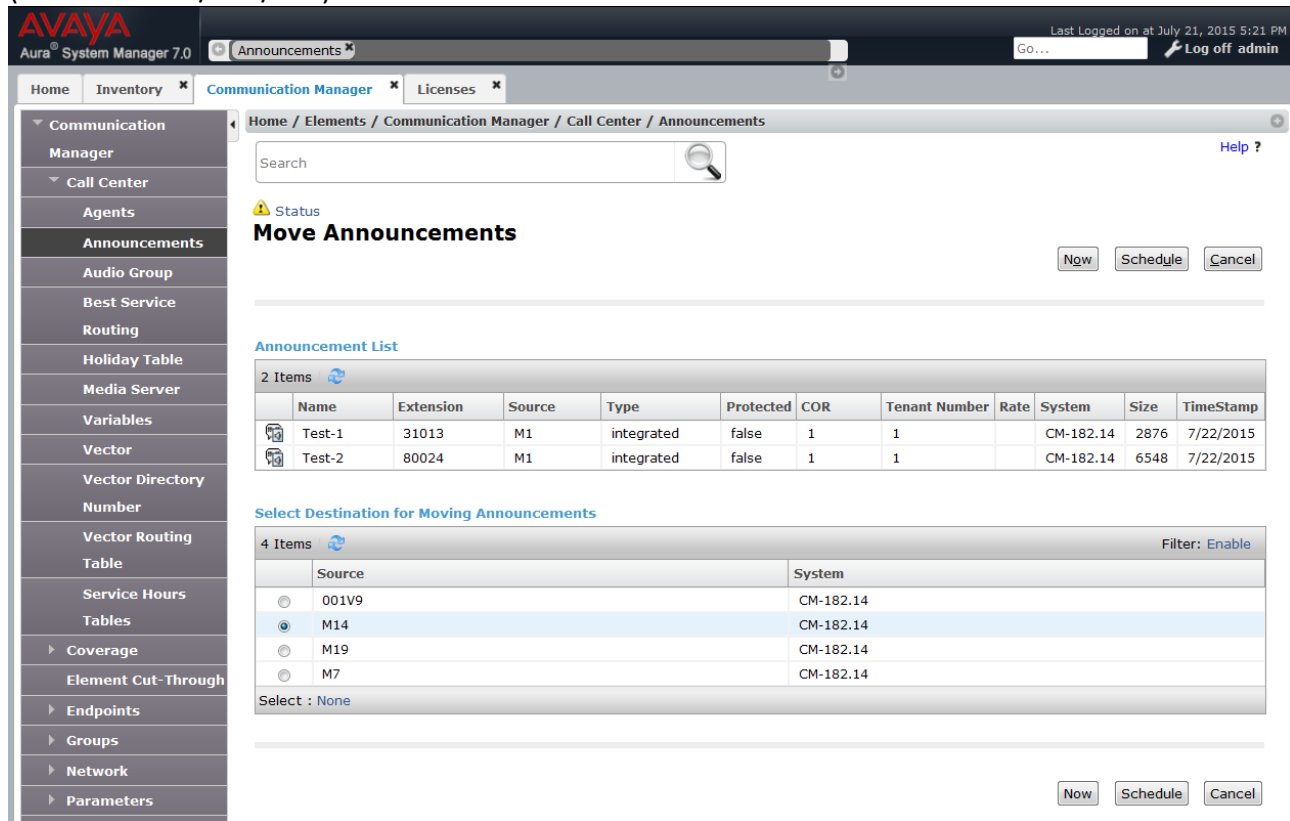
Backed-up Announcement List

2 Items Filter: Enable

File Name	File Size	Path	Backup Time	Backup Mode
Backup_Both_CM-182.14_22_07_2015_11_18_19	4689796	/opt/Avaya/IPTCM/7.0.9/Announcement/backup/CM-182.14	July 22, 2015 11:18:20 AM +05:30	BackupBoth
Backup_Both_CM-182.14_14_07_2015_11_26_10	84080	/opt/Avaya/IPTCM/7.0.9/Announcement/backup/CM-182.14	July 14, 2015 11:26:10 AM +05:30	BackupBoth

Select : None

More Actions -> Move may be used to move an announcement from one Communication Manager to another Communication Manager and the configured audio file from one source (Media Server /VAL/MG) to another source.



Avaya Aura® System Manager 7.0

Home | Inventory | Communication Manager | Licenses

Home / Elements / Communication Manager / Call Center / Announcements

Search

Status

Move Announcements

Now Schedule Cancel

Announcement List

2 Items

	Name	Extension	Source	Type	Protected	COR	Tenant Number	Rate	System	Size	TimeStamp
	Test-1	31013	M1	integrated	false	1	1		CM-182.14	2876	7/22/2015
	Test-2	80024	M1	integrated	false	1	1		CM-182.14	6548	7/22/2015

Select Destination for Moving Announcements

4 Items Filter: Enable

	Source	System
☐	001V9	CM-182.14
☒	M14	CM-182.14
☐	M19	CM-182.14
☐	M7	CM-182.14

Select : None

Now Schedule Cancel

More Actions -> Broadcast may be used to upload one or more audio files on to one or more sources (Media Server /VAL/MG).

Avaya Aura® System Manager 7.0

Home | Inventory | **Communication Manager** | Licenses

Home / Elements / Communication Manager / Call Center / Announcements

Search

Broadcast Announcements

Now Schedule Cancel

Only Audio Files are Broadcasted.

List Announcements:

Name	Extension	Source	Type	Protected	COR	Tenant Number	Rate	System	Size	TimeStamp
Test-1	31013	M1	integrated	false	1	1		CM-182.14	2876	7/22/2015
Test-2	80024	M1	integrated	false	1	1		CM-182.14	6548	7/22/2015

Select Destination for Broadcasting Announcements

Source	System
☒ M7	CM-182.14
☒ M19	CM-182.14
☒ M14	CM-182.14
☐ M1	CM-182.14
☒ 001V9	CM-182.14
☐ M9	CM-182.22
☐ M10	CM-182.22

Select : All, None

Viewing Announcement Status from Communication Manager

Existing Communication Manager administration commands such as “list integrated-annc-boards” or “list directory source m1” can be used to find out what Communication Manager believes exists in the Media Server announcement storage area.

list integrated-annc-boards						Page 2
Source: M2 INTEGRATED ANNOUNCEMENTS Time Remaining at 64Kbps: NA						
Internal Number	Group Number	Announcement Extension	Name	Length (Sec)	Size (Kb)	
NA		33335	AMS2-test	8	61	
NA		10005	Early-Closing	0	0	
NA		10008	panther	112	899	

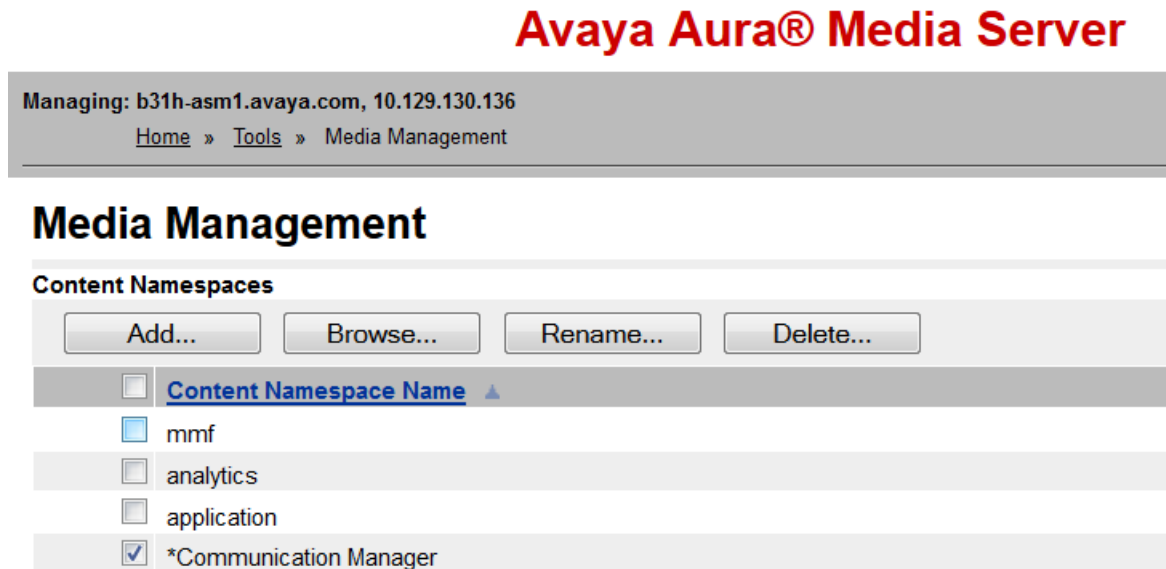
list directory source M2					
LIST DIRECTORY					
Source	File/Directory Name	Creation Date	Time	Size Kb	Pro- tect
M2	panther	2015-01-16	21:57:42	920	n
M2	AMS2-test	2015-05-04	17:38:09	62	n

Note that the file sizes shown on these forms assume an encoding of 64Kbps. If the files are encoded using a different bitrate, the file size will be accurate, but the duration in seconds may not reflect the correct length.

Viewing Announcement Status from Media-Server Element Manager

The Media Server Element Manager can also be used to navigate to a specific storage area on Media Server and view the announcement files present.

1. Navigate to **Home >> Tools >> Media Management**
2. Select **“Communication Manager”**, and then check **“Browse”**.



The next page displayed is titled **“Provision Media (Communication Manager)”**.

3. Expand the Communication Manager directory on the left panel and then look for the ANNC storage area matching that shown on the display media-server form. If the Media Server is not shared there should be only one ANNC area under Communication Manager. Select the desired ANNC storage area and all files present in that area are displayed on the right hand pane.

Avaya Aura® Media Server

Managing: b31h-asm2.avaya.com, 10.129.130.137

[Home](#) » [Tools](#) » [Media Management](#) » Provision Media

Provision Media (*Communication Manager)

Right click an item to see more options.

Add Content Group Add Media Delete... More Actions				
 Communication Manager - ANNC-00208f24-4f60-e401-0e00-545505bd0000 - ANNC-80627c0e-4560-e401-3800-5454f4d20000 - ANNC-008ab142-12a2-e401-0100-54c35a660000	Name ▲	Content Type	Size	Created(MDT)
	AMS2-test	audio/x-wav	62138	2015-05-04 11:38:09
	panther	audio/basic	920316	2015-01-16 14:57:42

Provisioning a Music-on-Hold Stream Source

The Media Server can access a music stream and make this stream available to Communication Manager. The stream source can be an internet streaming service or it can be a remote server hosting media files. Setting up a stream source requires configuration on CM and on the Media Server.

Provisioning a Stream Source on CM

On CM a stream source is administered as an integ-mus or integ-rep announcement with the “Live Stream Source” field enabled.

```
display announcement 10009
```

ANNOUNCEMENTS/AUDIO SOURCES

Extension:	10009	COR:	1
Annc Name:	80smusic	TN:	1
Annc Type:	integ-mus	Queue?	b
Source:	M1	Live Stream Source?	y

The **Annc Name** on the announcement form will need to exactly match the name of the stream source provisioned on the Media Server. The **Source** field can be a single media server or can be an audio-group comprised of only media servers. **Live Stream Source** must be set to **y**.

Provisioning a Stream Source on the Media Server

1. Navigate to **Home >> System Configuration >> Media Processing >> Music >> Stream Provisioning**

The screenshot shows the 'Avaya Aura® Media Server' interface. At the top, there's a header with 'Help | Sign Out cust'. Below it, a breadcrumb trail reads: 'Home » System Configuration » Media Processing » Music » Stream Provisioning'. The main heading is 'Stream Provisioning' with the subtext 'Manage streaming music sources.' Below this is a table with columns: 'Type', 'Stream Key', 'Primary URL', 'Backup URL', and 'State'. The table is currently empty, with only the header row visible. Above the table are buttons for 'Add...', 'Edit...', 'Delete', and a 'More Actions...' dropdown menu.

2. Select **Add**

The screenshot shows the 'Avaya Aura® Media Server' interface for adding a music source. The breadcrumb trail is: 'Home » System Configuration » Media Processing » Music » Stream Provisioning » Add Music Source'. The main heading is 'Add Music Source' with the subtext 'Add a new music source.' Below this is a form with the following fields: 'Stream Type' (a dropdown menu currently set to 'RSS Feed'), 'Name' (a text input field), 'Domain' (a text input field), 'Primary URL' (a text input field), 'Backup URL' (a text input field), and 'Locked' (a checkbox). At the bottom right of the form are 'Save' and 'Cancel' buttons.

3. From the **Stream Type** drop down list select “**RSS Feed**, **HTTP/MP3 Stream** or **HTTP Live Stream**” depending on the stream provider.
4. Assign a **Name** to the stream. The name must match the name given on the CM announcement form.
5. Skip the **Domain** field. It is for future use.
6. Enter the **Primary URL** of the desired music content.
7. Enter a **Backup URL** if one is available.

Avaya Aura® Media Server

Help | Sign Out admin

Managing: amsccloudappliance.localdomain, 135.60.10.115
[Home](#) > [System Configuration](#) > [Media Processing](#) > [Music](#) > Stream Provisioning

Stream Provisioning

Manage streaming music sources.

Add...
Edit...
Delete
More Actions...

	Type	Stream Key	Primary URL	Backup URL	State
☐	HTTP Live Stream	bbcradio	http://as-hls-ww-live.bbcmt.vo.llnwd.net/pool_7/live/bbc_1audio%3d96000.m3u8?dvr_window_length=24		Unlocked
☐	HTTP/MP3 Stream	80smusic	http://yp.shoutcast.com/sbin/tunein-station.pls?id=750312		Unlocked

Monitoring a Stream Source via the Media Server Element Manager

1. Navigate to **Home >> System Status >> Monitoring >> Music Streams**

Avaya Aura® Media Server

Help | Sign Out admin

Managing: amsccloudappliance.localdomain, 135.60.10.115
[Home](#) > [System Status](#) > [Monitoring](#) > Music Streams

Music Streams

Refresh every: 15 seconds

Directory Streams

Type	Stream Key	Title	Artist	File Index	Codec
Local File System	Audio	Kalimba	Mr. Scruff	2/2 - 00:05:50	MP3 44100Hz Stereo (192 kbps)
Local File System	ElevatorMusic	CorporateEdge		1/2 - 00:00:59	L16 8000Hz Mono (128 kbps)

Live Streams

Type	Stream Key	Title	Artist	Station	Codec
HTTP Live Stream	bbcradio		no desc		(-)
HTTP/MP3 Stream	80smusic	Goody Two Shoes	Adam Ant	181.fm - Awesome 80's	MP3 44100Hz Stereo (128 kbps)

The status of each stream is indicated by the Stream Key highlight color. Green indicates the stream is in-service, Yellow indicates the stream is in-service but either on backup, local cache or pre-recorded playback. Red indicates the stream is out-of-service. This could indicate a problem with the stream provider or a misconfigured URL or stream type.

Note that the above screen shows both **Directory Streams** (local file system) and **Live Streams**. CM only has access to the Live Streams.

Configuring Communication Manager Survivable Servers in a Media Server environment

In an environment with backup Communication Manager survivable servers and Media Server, a subset of the Media Servers may be used to play a role in the activation and deactivation of the backup Communication Manager servers. This role is similar to the role played by media-gateways. Configuring Communication Manager to use Media Server in this role is beyond the scope of this quick start guide but is documented in this white paper.

<http://downloads.avaya.com/css/P8/documents/101013810>

Communication Manager maintenance commands for Media Server

Status media-server

The status media-server command displays comprehensive status for an individual media-server.

```
status media-server 10
```

```

                                MEDIA SERVER STATUS

Media Server Number: 10
                        State: in-service
        Signaling-group: 510
                        Node Name: sst1-ams10
                        IP Address: 172.31.0.250
        Network Region: 6
                        SW-Version: 7.7.0.228
Voip Channel License Limit:
Dedicated Voip Channel Licenses:
Voip Channel Licenses in-use: 1224
                        Load Factor: 34
Estimated Channel Capacity: 3750
Announcements Present: 0
```

Two fields of interest not found on any other forms are the **Load Factor** and **Estimated Channel Capacity**. The **Load Factor** is a usage metric calculated by Media Server which represents how “busy” the Media Server is. This is an aggregation of various Media Server internal resource metrics. The value ranges from 0 to 100. Communication Manager polls Media Server at a minimum of once every 10 seconds and more often as the load factor increases. It is also provided by Media Server via the proprietary SIP header: **Av-Media-Server-Perf** placed in all SIP/SDP messages sent to CM. CM uses the load factor to assist in load balancing between multiple Media Servers. The specific performance characteristics of the individual server or virtual machine will greatly affect the load factor seen. For the same traffic offered, a virtual machine Media Server will have a much higher load factor than a high performance bare metal server.

The **Estimated Channel Capacity** is also a metric calculated by Media Server. Media Server estimates the channel capacity based on the number of processors/cores/memory and speed of the server. This channel capacity is an estimate, not a hard limit. The estimate is for G711 channels. Other codecs costs more per call and will results in a lower channel capacity.

List media-server

The “list media-server” command may be used to display data about all media-servers simultaneously. This is useful to quickly see which media-servers may be in or out of service and relative usage between them. The column showing “**Licenses In-Use**” is a snapshot of channels established on each media-server.

list media-server								Page	1
MEDIA SERVERS REPORT									
Num	Sig-grp	Node-Name	License Limit	Dedicated Licenses	Licenses In-Use	NetRgn	Loc	State	
1	501	sst1-ams1			322	6		INS	
2	502	sst1-ams2			314	6		INS	
3	503	sst1-ams3			80	6		INS	
4	504	sst1-ams4			310	6		INS	
5	505	sst1-ams5			82	6		INS	
6	506	sst1-ams6			264	6		INS	
7	507	sst1-ams7			72	6		INS	
8	508	sst1-ams8			294	6		INS	
9	509	sst1-ams9			542	6		INS	
10	510	sst1-ams10			556	6		INS	
11	511	sst1-ams11			310	6		INS	

Both the status media-server form and the list media-server form have a **State** field which can display several different values.

- **“out-of-service - OOS”**: The Media Server s will be out of service when the associated SIP signaling-group is out-of-service. The Media Server cannot come into service until the signaling group first comes into service. An in-service signaling group is a necessary first condition but not a sufficient condition for the Media Server to be in in service.
- **“in-service - INS”**: Media Server is in service and should be able to satisfy Communication Manager service requests
- **“pending-service - PINS”**: Communication Manager is actively attempting to contact the Media Server and establish the needed control sessions. In a working environment the pending-service state should be very short lived. If the state remains pending-service for more than a few seconds the Media Server and or network should be examined for problems.
- **“pending-lock - PLOCK”**: The Media Server has reported that is in the **pending-lock** state. This state is entered when someone explicitly uses the Media Server Element Manager and navigates to **Home » System Status » Element Status** and selects **“Pending Lock”** from the **“More Actions”** drop down list. When in this state, Media Server allows existing calls to remain established, but blocks establishment of new sessions. When all established sessions terminate normally, the Media Server will enter the **“locked”** state. To exit this state, **“Unlock”** must be selected from the drop down list.
- **“locked - LOCK”**: The Media Server has reported that is in the **locked** state. This state is entered when someone explicitly uses the Media Server Element Manager and navigates to **Home » System Status » Element Status** and selects **“Lock”** from the **“More Actions”** drop down list. . When in this state Media Server immediately terminates all existing sessions. To exit this state, **“Unlock”** must be selected from the drop down list.

- **"no-license - NOLIC"**: The Media Server has reported that it is unable to acquire an instance license from the WebLM server.
- **"ad - AD"**: The Media Server is in an ip-network- region which has become "auto-region-disabled" and hence is not available to be used by the Communication Manager server (main or survivable) issuing the command.
- **"rd - RD"**: The Media Server is in an ip-network- region which has become "manually-disabled" and hence is not available to be used by the Communication Manager server (main or survivable) issuing the command.
- **"not-applicable - N/A"**: This state only exists with respect to Communication Manager survivable servers. It indicates the survivable server is intentionally not attempting to establish any contact with this Media Server.
 - An inactive Communication Manager survivable server only attempts to contact those Media Servers in its media-server reporting list.
 - An active Communication Manager survivable server only attempts to contact those Media Server in its media-server reporting list and all Media Servers in regions for which it is assigned as a backup survivable server.

Media-server traffic reports

CM ip-dsp related traffic reports will now include Media Server. Existing per network region reports will now aggregate data for relevant port networks, media-gateways and Media Server. A new media-server specific traffic report has been introduced similar to the pn and gw specific reports. Any report which includes Media Server data will indicate that the capacity is now an estimated capacity. See the column below titled "G711 Est Capty".

list measurements ip dsp-resource ms summary yest											Page 1
Switch Name:							Date: 7:58 am FRI JUL 10, 2015				
IP DSP RESOURCE MEDIA-SERVER SUMMARY REPORT											
G711 Equivalent DSP							Total		MS		
MS	Peak	Net	Est	Rsrc	Usage	IGC	DSP	IGC	Denied	%	% Out
Num	Hour	Reg	Capty	Peak	(Er1)	Usage	Pegs	Pegs	Pegs	Den	Of Srv
M1	1200	6	2050	468	21.2	0.0	468	0	0	0	0
M2	1200	6	2050	454	20.6	0.0	454	0	0	0	0
M3	1200	6	550	116	5.3	0.0	116	0	0	0	0
M4	1200	6	2050	468	21.2	0.0	468	0	0	0	0
M5	1200	6	550	138	6.3	0.0	138	0	0	0	0
M6	1200	6	1950	378	17.1	0.0	378	0	0	0	0
M7	1200	6	1300	124	5.6	0.0	124	0	0	0	0
M8	1200	6	1550	448	20.3	0.0	448	0	0	0	0
M9	1200	6	2950	688	31.2	0.0	688	0	0	0	0
M10	1200	6	3750	680	30.8	0.0	680	0	0	0	0
M11	1200	6	2050	474	21.5	0.0	474	0	0	0	0
M12	1200	6	2000	348	15.8	0.0	348	0	0	0	0

Collecting debug logs from Media Server

1. Using the Media Server Element Manager, navigate to **Home » System Configuration » Debug Tracing » General Settings**
2. Select “**Enabled**” from the **Debug Logging** menu and click “**Save**”.

Avaya Aura® Media Server

Managing: b31h-asm1.avaya.com, 10.129.130.136
[Home](#) » [System Configuration](#) » [Debug Tracing](#) » General Settings

General Settings

[Debug](#) | [System Diagnostic](#)

Debug

Debug Logging: **Enabled** ▼

Trace File History: (0 - 20 files)

Trace File Size: (100,000 - 100,000,000 bytes)

System Diagnostic

Enable System Diagnostic Mode: ☐

Warning: This may cause system performance degradation.

3. Execute the desired test. When possible, execution of a Communication Manager “list trace station/tac” command during the test helps to provide important internal cids and SIP cids which makes it easier to analyze both MST and Media Server debug logs.
4. Using the Media Server EM navigate to **Home » Tools » Log capture**
5. Check the “**Include trace logs**” box and click on the [download](#) link. A zip file will be downloaded to the PC hosting the EM browser session.

Avaya Aura® Media Server

Managing: b31h-asm1.avaya.com, 10.129.130.136
[Home](#) » [Tools](#) » [Log capture](#)

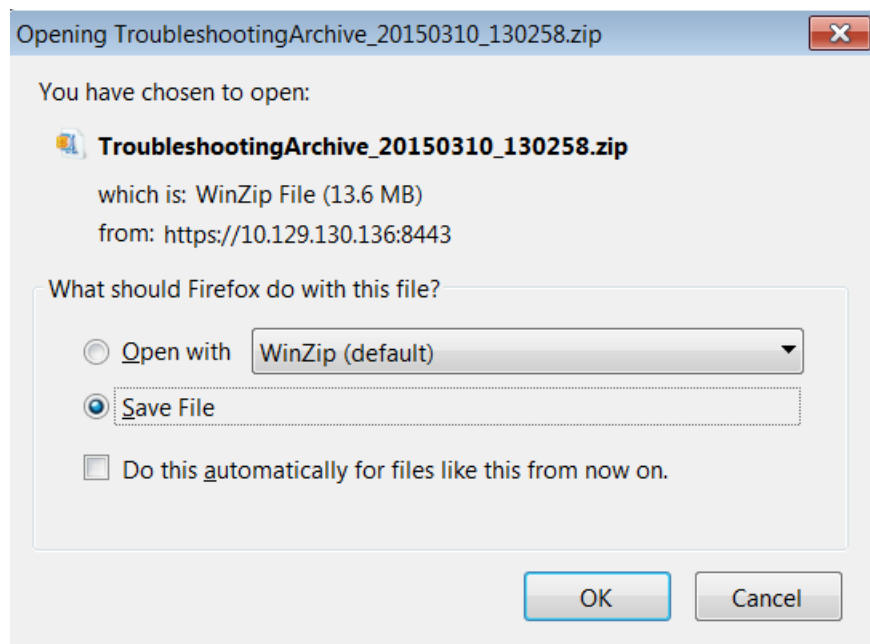
Log Capture

To capture logs for support, click [download](#)

Include trace logs: ☒

Include video capture: ☐

6. Save the file for the appropriate services organization.



Communication Manager MST traces with Media Server

Collecting the MST trace

Communication Manager communicates with each Media Server via a separate SIP signaling group. To include Media Server messaging in an MST trace, the MST trace needs to be enabled to capture “**SIP Trunks**” on page 1, and then on page 15 enter the signaling group number for the specific Media Server of interest or leave it blank for all SIP traffic to all signaling groups. On page 1 always set **Log Mst** and **Trace Analyzer** to “y”.

display mst Page 1 of 17

```

MESSAGE SEQUENCE TRACE

Run Time Limit: 99 days      Disable On Buffer Full? n  Generic Filters? n
Store Timestamp? y          Start Trigger? n          Log Mst? y
Message Storage: entire     Stop Trigger? n          Trace Analyzer? y
                             Stop Count:
                             Retrigger? n

X.25? n      GATEWAY? n      EWT? n  DEBUG BUTTON? n  HW ERROR LOG? n
ISDN-PRI? n   CCMS? n        SIP Trunks? y  PRECs? n  PROC ERRORS? n
ISDN-BRI? n   PACKET? n      CALL TRACE? n  BSR? n    IP? n
ASAI? n       VECTORS? n      CDR? n  DENIAL EVENTS? n  BASM? n
CMS? n  VECTOR EVENTS? n      PMS? n  FW ERROR LOG? n
IP Stations/LSPs/ESSs? n

X.25 Filter Data
Processor Channel: 1          Link Control: all
Application Data: none       Session Timers? y
Confirmations? n            Application Errors? y
Session Control: all         Unrecognized Messages? y
Processor Channel Control: all
  
```

display mst Page 15 of 17

```

MESSAGE SEQUENCE TRACE

SIP Filter Data

Signaling Group: 510
Message Bodies? y
Calling User:
Called User:
  
```

Interpreting the MST trace

All MST data is captured in log files located in /var/log/ecs.

The log files are of the form “yyyy-mmdd-hhmmss.log”

-rw-r--r-- 1 root root 1218 Jul 20 09:29 2015-0720-092746.log

```
cd /var/log/ecs
```

```
CM SAT> enable mst
```

```
# Run the test to collect data
```

```
CM SAT> disable mst
```

```
logc -t yyyymmdd:hhmm-YYYYMMDD:HHMM | logmst -c | mta > /tmp/xxx.m
```

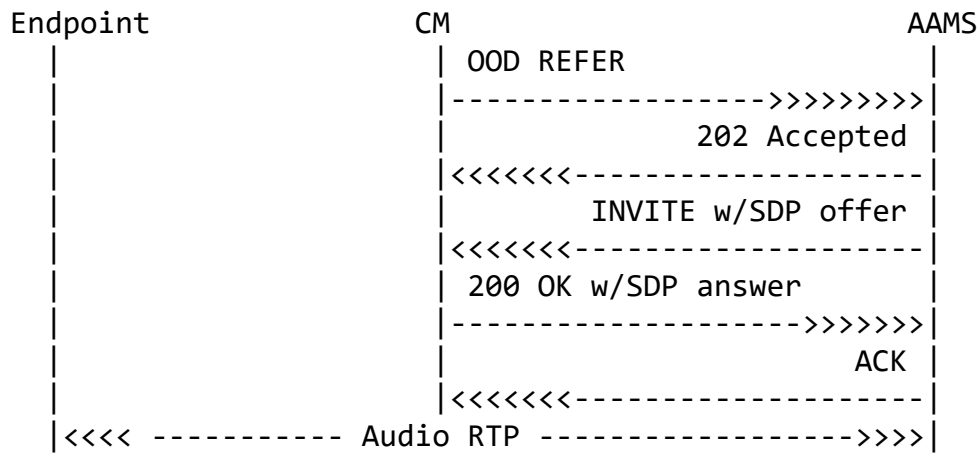
```
# Save/Send the /tmp/xxx.m file to the appropriate services/development contact.
```

Analyzing Communication Manager/Media Server SIP Messages

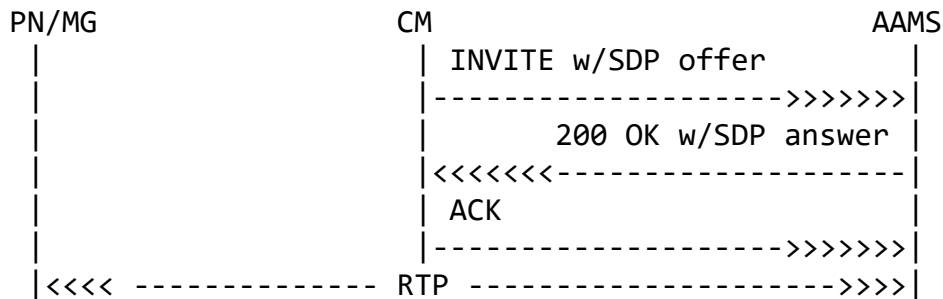
SIP messages between CM and Media Server are divided into two classes, SIP/SDP messages used to establish media sessions and SIP/INFO messages used to send Media Server Markup Language (MSML) requests to Media Server and receive MSML events from Media Server.

SIP/SDP media establishment messages

A typical CM/ Media Server SIP message exchange for establishing a media session between Media Server and an IP endpoint follows this flow. An SDP offer is elicited from Media Server by sending SIP/REFER to Media Server. The REFER includes “template” SDP which directs what Media Server should include in the SDP offer. Note: the Endpoint to CM signaling is not shown in this signaling chart.



A typical CM/ Media Server SIP message exchange for establishing a media session between Media Server and another Media Server or MG/PN for an IGC may follow the above flow or the flow below. If the other end of the IGC is a Media Server or MG with a non-cached ephemeral, the REFER sequence is used. If the other end of the IGC is an MG with a cached ephemeral or PN with Crossfire, the sequence below is used. An INVITE with an SDP is sent directly by Communication Manager to Media Server.



Associating Media Server SIP media establishment sessions with a specific user

Each SIP message involved in the SDP exchange will include a proprietary header “**av_cm_id**”. When part of an MST call trace, this header will identify which party this specific Media Server media stream is being established for. The format of this header is:

av_cm_id = ams_portid-igc/otherportid-cid-portid-uid-extension

Each parameter of this proprietary header is separated by a dash ('-'). The **igc/otherportid** parameter is only present if this media session is part of an IGC.

An example of the av_cm_id proprietary header for an IP station media session is shown here:

av_cm_id=6007142b-57a-7f000125-015e-2040208

- **6007142b** is an internal CM Media Server channel identifier
 - 60=channel type is Media Server
 - 07=AAMS#7
 - 142b=channel id on AMS#7
- **57a**=CM internal connection manager service id
- **7f000125**=CM internal UM/connection manager portid
- **01f3**=CM internal station UID
- **2040208**=station extension (not present for trunks or terminating SIP OPTIM stations)

An example of the av_cm_id proprietary header for an IGC media session between Media Server and another Media Server /MG/PN is shown here:

av_cm_id=60010b31-igc/4021-1d1a-40210134-2b62-1424438

- **60010b31** is an internal CM Media Server channel identifier
 - 60=channel type is Media Server
 - 01= Media Server #1
 - 0b31=channel id on Media Server #1
- **igc/4021** – identifies this media session as part of an IGC between Media Server #1 and MG # 0x21
 - **40** = MG, **60**=AAMS, **00**=Port Network
 - **21** = Media Server /MG/PN # (hex)
- **1d1a**=CM internal connection manager service id
- **40210134**=CM internal UM/connection manager portid
- **2b62**=CM internal station UID
- **1424438**=station extension (not present for trunks or terminating SIP OPTIM stations)

Here is a short fragment of an MST call trace along with the Media Server SIP/SIP messages. These are not complete SIP messages. Note the cid (469)/uid(9f3a)/portid(7f000125) in the SUSER/CONNMM messages and their presence in the SIP media establishment messages.

- SUSER STA_USER<0000**9f3a**> UM_ORIG(cid=0011**0469**)
- CONNM [0000**0469**] CM_PT_CONN(pt=(**7f000125**,(IP_STN,loss=?4e05?) tsopt=?fffe?))
- REFER sip:xxx; **av_cm_id**=60010000-**469-7f000125-9f3a**-2040208; SIP/2.0
- SIP/2.0 202 Accepted
 - o To: <sip:xxxx@10.33.6.101:5061;**av_cm_id**=60010000-**469-7f000125-9f3a**-2040208;
- INVITE (will contain SDP offer from AAMS)
 - o From: <sip:xxx@10.33.6.101:5061;**av_cm_id**=60010000-**469-7f000125-9f3a**-2040208;
- SIP/2.0 200 OK (will contain SDP answer from CM)
 - o From: <sip:xxxx@10.33.6.101;**av_cm_id**=60010000-**469-7f000125-9f3a**-2040208;>;
- ACK (from AAMS)
 - o From: <sip:xxxx-10.33.6.101:5061;**av_cm_id**=60010000-**469-7f000125-9f3a**-2040208;

SIP INFO messages and MSML commands

The “Media Server Markup Language” or MSML protocol is used to direct Media Server to apply actions to media streams established using SIP/SDP. Typical actions would be:

- Apply a tone to a stream
- Apply an announcement to a stream
- Collect digits from a stream
- Join (connect) one stream to another stream
- Join (connect) one stream to a conference

In all of these requests the MSML message must indicate which stream(s) the action should be applied to. An example of a MSML message applying dial tone is shown here.

INFO sip: *other stuff deleted*

```
<msml version="1.1">
  <dialogstart type="application/moml+xml"
    target="conn:648ba093-ae61-3751-8606-0c306e94648e"
    name="TONE_CM_DIALTONE_ID_1_SEQ_0_0x60010000" mark="1">
    <tonegen>
      <tone duration="1000s">
        <tone1 freq="350" atten="-10"/>
        <tone2 freq="440" atten="-10"/>
      </tone>
      <tonegenexit>
        <exit namelist="tonegen.end"/>
      </tonegenexit>
    </tonegen>
  </dialogstart>
</msml>
```

Note the **target** parameter “**conn:**”. The “**conn:**” field indicates the target of the tone application is a “connection” as opposed to a “conference”. The value of the conn: field is the **tag** provided previously by Media Server during the SDP establishment. This might be a **From** or **To** tag, depending on which side provided the SDP offer, but it is always the tag provided by the Media Server. The following INVITE was provided by Media Server hence it is a **From** tag. Communication Manager must provide this tag as the target in all MSML messages for the stream Communication Manager wishes to affect.

- INVITE sip:AMS_1610678272@10.33.2.4:9061;SIP/2.0
 - o From: tag=648ba093-ae61-3751-8606-0c306e94648e

Tip: when looking at Communication Manager MST traces it is easier to analyze these traces if each relevant tag string is globally replaced with a more easily identifiable string such as “ORIG-STATION”, etc.

**<join id1=ORIG_STATION; id2=TERM_STATION> will make more sense than
 <join id1=648ba093-ae61-3751-8606-0c306e94648e;
 id2=1287bc42-3214-76b5-128a-652bc5f329cd> .**

Media Server configuration for High Availability Operation

Media Server can be configured as a 1+1 High Availability (HA) cluster to ensure uninterrupted availability of media processing in the case where the media server fails. A 1+1 HA cluster consists of a primary server and backup server and only one server is active processing calls. The other server is inactive and will take over in the event a media server failure is detected.

In order to configure a 1+1 HA cluster you need to do the following:

- Configure the primary server
- Configure the backup server
- Enable 1+1 HA

Both servers need to have their clocks synchronized with the same Network Time Protocol (NTP) server and must be on the same subnet with Layer 2 network redundancy.

On the primary server (shown below) ensure the **'Role'** is set to primary, enable the replication account, and specify the username/password. The primary server UUID and IP address is needed during configuration of the backup server. This configuration is located under **Cluster Configuration >> Server Designation**.



Avaya Aura® Media Server

Help | Sign Out root

Managing: server5088-vm06.richlab.avaya.com, 135.60.77.221

Home » Cluster Configuration » Server Designation

- System Status
 - Element Status
 - Cluster Status
 - Alarms
 - Logs
 - Monitoring
- Applications
 - Operational State
 - Signaling Translations
- Cluster Configuration
 - High Availability
 - Server Designation
 - Replication Settings
 - Load Balancing
 - Advanced Settings
- System Configuration
 - Server Profile
 - Network Settings
 - Signaling Protocols
 - Media Processing
 - Application Interpreters
 - Monitoring Settings
 - Session Detail Records
 - Content Store
 - Logging Settings
 - Debug Tracing
 - Engineering Parameters
 - Element Manager Settings
- Licensing
 - General Settings
 - Monitoring
 - Server Status
 - Utilization Threshold
 - Advanced Settings
- Tools
 - Manage Software
 - PVI Results
 - Backup and Restore
 - Media Management
 - Session Detail Record Browser
 - Log Capture
- Security
 - General Settings
 - Certificate Management
 - System Manager
 - Enrollment

Server Designation

The administrator may designate each server's role within the cluster. A Primary server must always be configured.

[Local Server](#) | [Server Designation](#) | [Replication Account](#)

Local Server

Name: server5088-vm06

Address: 135.60.77.221

UUID: 662a3065-2991-11e5-9d34-000c29b17cb7

Role: Primary

Server Designation

Add
Remove

☐ Server Address	Server UUID	Role

Replication Account

Enable Replication Account: ☒

Username: (8-16 characters)

Password: (6-32 characters)

Confirm Password: (6-32 characters)

Save
Cancel

Copyright 2010-2015 Avaya Inc. All Rights Reserved

On the Backup server (below) ensure the **'Role'** is set to the backup, specify the primary server UUID, primary server IP address, enable replication account and specify the same username/password (must match primary server). This configuration is located under **Cluster Configuration >> Server Designation**.

If this was done correctly you should see both servers listed under **System Status>>Cluster Status** on both the primary and secondary server.



Avaya Aura® Media Server

[Help](#) | [Sign Out](#) [root](#)

Managing: server5088-vm07.richlab.avaya.com, 135.60.77.223
[Home](#) » [Cluster Configuration](#) » [Server Designation](#)

- System Status
 - Element Status
 - Cluster Status
 - Alarms
 - Logs
 - Monitoring
- Applications
 - Operational State
 - Signaling Translations
- Cluster Configuration
 - High Availability
 - Server Designation
 - Replication Settings
 - Load Balancing
 - Advanced Settings
- System Configuration
 - Server Profile
 - Network Settings
 - Signaling Protocols
 - Media Processing
 - Application Interpreters
 - Monitoring Settings
 - Session Detail Records
 - Content Store
 - Logging Settings
 - Debug Tracing
 - Engineering Parameters
 - Element Manager Settings
- Licensing
 - General Settings
 - Monitoring
 - Server Status
 - Utilization Threshold
 - Advanced Settings
- Tools
 - Manage Software
 - PVI Results
 - Backup and Restore
 - Media Management
 - Session Detail Record Browser
 - Log Capture
- Security
 - General Settings
 - Certificate Management
 - System Manager
- Account Management

Server Designation

The administrator may designate each server's role within the cluster. A Primary server must always be configured.

[Local Server](#) | [Server Designation](#) | [Replication Account](#)

Local Server

Name: server5088-vm07

Address: 135.60.77.223

UUID: b2eec9a6-2991-11e5-97f5-000c29738fca

Role: Backup

Server Designation

Primary Server UUID: 11e5-9d34-000c29b17cb7

Primary Server Address: 135.60.77.221

Replication Account

Enable Replication Account: ☒

Username: platrepluser (8-16 characters)

Password: ●●●●●●●● (6-32 characters)

Confirm Password: ●●●●●●●● (6-32 characters)

Save
Cancel

Copyright 2010-2015 Avaya Inc. All Rights Reserved

On both the primary and backup server HA needs to be enabled, which is configured under **Cluster Configuration>>High Availability**. Ensure that **'Enable High Availability'** is checked then specify the service IP address and mask.

The service IP address is shared by both the primary and backup server. It is used to send signaling and media to the server that is currently active.



Managing: server5088-vm06.richlab.avaya.com, 135.60.77.221

[Home](#) » [Cluster Configuration](#) » [High Availability](#)

System Status

Element Status

Cluster Status

Alarms

Logs

Monitoring

Active Sessions

Performance

Operational Measurements

Protocol Connections

Advanced

Applications

Operational State

Signaling Translations

Cluster Configuration

High Availability

Server Designation

Replication Settings

Load Balancing

Advanced Settings

System Configuration

Server Profile

Network Settings

Signaling Protocols

Media Processing

Application Interpreters

Monitoring Settings

Session Detail Records

Content Store

Logging Settings

Debug Tracing

Engineering Parameters

Element Manager Settings

Licensing

General Settings

Monitoring

Server Status

Utilization Threshold

Advanced Settings

Tools

Manage Software

PVI Results

Backup and Restore

Media Management

Session Detail Record Browser

Log Capture

High Availability

This task allows administrators to configure High Availability within the cluster.

[General Settings](#) | [Failure Notification List](#)

General Settings

Enable High Availability: ☒

Service IP Address:

(Service IP Address)

Service IP Address Mask:

(Service IP Address Mask)

Local High Availability State Lock: ☐

Failure Notification List

Add

Remove

☐ Protocol	Server Address	Server Port

Save

Cancel

Copyright 2010-2015 Avaya Inc. All Rights Reserved

Media Server configuration with Prognosis for RTCP monitoring

To enable Prognosis RTCP monitoring you need to enable **'Dual Unicast Monitoring'** and specify the Prognosis server IP address/port. This is configured under **System Configuration>>Media Processing>>General Settings>>Dual Unicast Monitoring** and is shown in the screenshot below.



Avaya Aura® Media Server

[Help](#) | [Sign Out root](#)

Managing: server5088-vm06.richlab.avaya.com, 135.60.77.221

[Home](#) > [System Configuration](#) > [Media Processing](#) > [General Settings](#)

Original Navigation

- Cluster Configuration
 - High Availability
 - Server Designation
 - Replication Settings
 - Load Balancing
 - Advanced Settings
- System Configuration
 - Server Profile
 - Network Settings
 - General Settings
 - IP Interface Assignment
 - Advanced Settings
 - Media Port Ranges
 - Port Assignments
 - TLS Ciphers
 - Signaling Protocols
 - SIP
 - General Settings
 - Domains and Accounts
 - Nodes and Routes
 - MRCPP
 - General Settings
 - Servers
 - Pools
 - [Custom Vendors](#)
 - REST
 - General Settings
 - Media Processing
 - General Settings
 - Audio Codecs
 - Video Codecs
 - Digit Relay (DTMF)
 - Media Security
 - Advanced Settings
 - Application Interpreters
 - Monitoring Settings
 - Session Detail Records
 - Content Store
 - Logging Settings
 - Debug Tracing
 - Engineering Parameters
 - Element Manager Settings
 - Licensing
 - General Settings
 - Monitoring

General Settings

This task allows administrators to view and modify media general settings.

[QOS Monitoring](#) | [QOS Streaming](#) | [Media Audits](#) | [Network Address Translation](#) | [Continuous Streaming Sources](#) | [Aurix Speech Search Engine](#) | [Dual Unicast Monitoring](#)

Audio RSS URL:  (maximum: 1024 characters)

Audio Volume (dB):   (-24 - 24)

Audio RSS Channel Key:   (maximum: 48 characters)

SHOUTCast Channel Key:   (maximum: 48 characters)

SHOUTCast Backup URL:  (maximum: 1024 characters)

SHOUTCast Primary URL:  (maximum: 1024 characters)

SHOUTCast HTTP Proxy Host:  (maximum: 255 characters)

SHOUTCast HTTP Proxy Port:  (1 - 65535)

Allow one item per RSS channel: ☐  

Aurix Speech Search Engine

Enable AURIX SSE Real-time Interfaces: ☐  

Enable AURIX SSE Web Service Interfaces: ☐  

Dual Unicast Monitoring

Dual Unicast Monitoring: ☒  

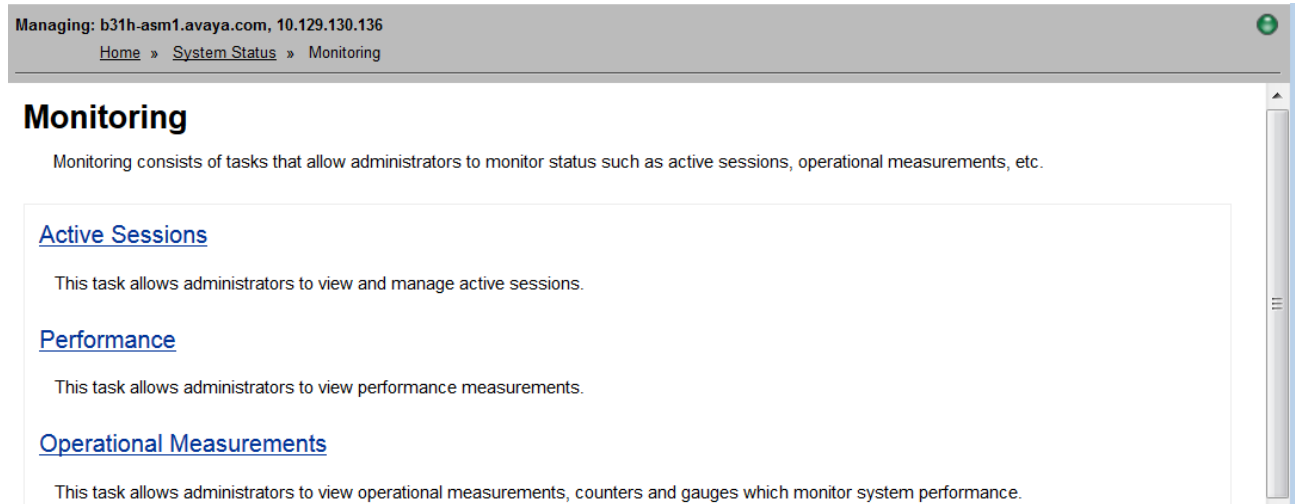
Monitoring Server IP:    (1 - 256 characters)

Monitoring Server Port:   (0 - 65535)

Copyright 2010-2015 Avaya Inc. All Rights Reserved

Media Server Element Manager System Monitoring

You can use Media Server System Monitoring to view active sessions, performance measurements and various operational measurements (OM).



The **'Active Sessions'** monitor will list all active SIP sessions on the Media Server providing multiple filter and searching capabilities. In addition, it displays the following Key Performance Indicators (KPI):

- Active Sessions
- Key Resource Usage
- Session Information
- CPU load

You may monitor details of a session by selecting a specific session or the next new session that matches the specified criteria. When monitoring a session you may switch views between dashboard, session detail record (SDR) and SIP protocol trace.

Avaya Aura® Media Server

Help | Sign Out cust

- System Status
 - Element Status
 - Cluster Status
 - Alarms
 - Logs
 - Monitoring
 - Active Sessions
 - Performance
 - Operational Measurements
 - Protocol Connections
 - Advanced
- Applications
 - General Settings
 - Operational State
 - Signaling Translations
 - Custom Applications
 - Default Handlers
- Cluster Configuration
 - High Availability
 - Server Designation
 - Replication Settings
 - Load Balancing
 - Advanced Settings
- System Configuration
 - Server Profile
 - Network Settings
 - Signaling Protocols
 - Media Processing
 - Application Interpreters
 - Monitoring Settings
 - Session Detail Records
 - Content Store
 - Logging Settings
 - Debug Tracing
- Licensing
 - General Settings
 - Monitoring
 - Server Status

Managing: sst1-ams1.dr.avaya.com, 172.31.0.241

Home » System Status » Monitoring » Active Sessions

Active Sessions

(Cluster)

Active Sessions: 1134	Conference Resources: 0	Session Attempts/Interval: 953
IVR Resources: 1122	MRCP Resources: 0	CPU Load (%): 39

Filter: None

Criteria: None

Sessions Listed: 1136
Filtered Sessions: 0

Remote Party	Start Timestamp	Application Name	Endpoint	QOS R-Factor	QOS Round Trip Delay(msec)	QOS
< sip:AMS_1610678329@172.31.0.211:	7/15/2015 12:17:27 PM	379bf905-cm	No Information	No Information	0	0
< sip:AMS_1610678322@172.31.0.211:	7/15/2015 12:17:27 PM	379bf905-cm	No Information	No Information	0	0
No Information	7/15/2015 12:17:27 PM	379bf905-cm	No Information	No Information	0	0
No Information	7/15/2015 12:17:27 PM	379bf905-cm	No Information	No Information	0	0
< sip:AMS_1610678327@172.31.0.211:	7/15/2015 12:17:27 PM	379bf905-cm	No Information	No Information	0	0
< sip:AMS_1610678325@172.31.0.211:	7/15/2015 12:17:27 PM	379bf905-cm	No Information	No Information	0	0
< sip:AMS_1610679326@172.31.0.211:	7/15/2015 12:17:27 PM	379bf905-cm	No Information	No Information	0	0

Copyright 2010-2015 Avaya Inc. All Rights Reserved

The session dashboard view (shown below) is updated in real-time and will display several voice quality statistics, information about audio/video packets transmitted/received and packet loss.

Avaya Aura® Media Server

Help | Sign Out cust

- System Status
 - Element Status
 - Cluster Status
 - Alarms
 - Logs
 - Monitoring
 - Active Sessions
 - Performance
 - Operational Measurements
 - Protocol Connections
 - Advanced
- Applications
 - General Settings
 - Operational State
 - Signaling Translations
 - Custom Applications
 - Default Handlers
- Cluster Configuration
 - High Availability
 - Server Designation
 - Replication Settings
 - Load Balancing
 - Advanced Settings
- System Configuration
 - Server Profile
 - Network Settings
 - Signaling Protocols
 - Media Processing
 - Application Interpreters
 - Monitoring Settings
 - Session Detail Records
 - Content Store
 - Logging Settings
 - Debug Tracing
- Licensing
 - General Settings
 - Monitoring
 - Server Status

Managing: sst1-ams12.dr.avaya.com, 172.31.0.252

Home » System Status » Monitoring » Active Sessions

Active Sessions

Viewing Session Dashboard

Filter: None

Gslid: 2174be37-9b7d-3536-848d-09e102bf9bb0

Records Listed: 53
Filtered Records: 0

Select Viewing Options... Stop Monitoring

Summary

R-Factor 82

Jitter 0 (ms)

Delay 0 (ms)

SNR 71

Audio

Codec		G729
Packet Time (ms)		20
Receive (pkts/s)		0
Transmit (pkts/s)		28
Packet Loss Last 5 Sec (%)		0
Packet Loss Last 30 Sec (%)		0
Packet Loss Last 60 Sec (%)		0
Speech Level (dbm0)		0
Noise Level (dbm0)		-71
Total Level (dbm0)		0
Activity Factor		0

Video

Codec		
Profile Level		
Packet Mode		
Negotiated Bandwidth		
Frame Rate (fps)		0
Receive (pkts/s)		0
Transmit (pkts/s)		0
Packet Loss Last 5 Sec (%)		0
Packet Loss Last 30 Sec (%)		0
Packet Loss Last 60 Sec (%)		0

Copyright 2010-2015 Avaya Inc. All Rights Reserved

A session detail record (SDR) is created for every Media Server SIP session and information about this session is written to the SDR. The SDR view (shown below) allows you to view the SIP trace and the SDR as it gets updated in real-time.

AVAYA

Avaya Aura® Media Server

Help | Sign Out cust

Managing: sst1-ams12.dr.avaya.com, 172.31.0.252

Home » System Status » Monitoring » Active Sessions

Active Sessions

Filter: None

Viewing Session Detail Records

Records Listed: 64

Gslid: 2174be37-9b7d-3536-848d-09e102bf9bb0

Filtered Records: 0

Select Viewing Options...

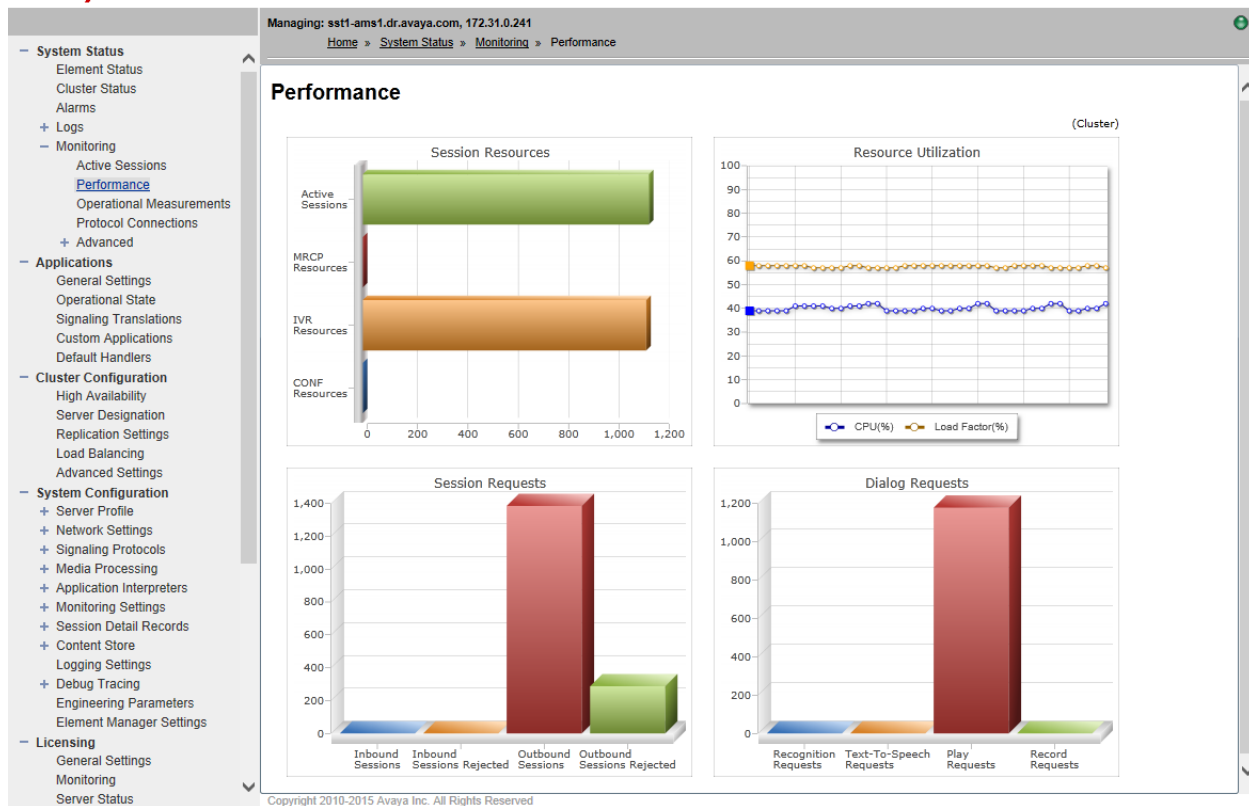
Stop Monitoring

Field	Value	Timestamp
Start Timestamp	2015-07-15 16:38:59	7/15/2015 12:38:59 PM
Global Session Id	2174be37-9b7d-3536-848d-09e102bf9bb0	7/15/2015 12:38:59 PM
SIP Trace	ENG(192-A) <idle> Incoming SIP Message: REFER sip:379bf905-da2f-11e0-882c-e36c7400a53b@172.31.0.252:5061 REFER sip:379bf905-da2f-11e0-882c-e36c7400a53b@172.31.0.252:5061;transport=tl;av_cm_id=600c00f8-15f3-7f4029c1-529c1;clock=all From: <sip:ACM@172.31.0.211>;tag=fe3f39802bf41e5841d05056b6ea3 To: <sip:379bf905-da2f-11e0-882c-e36c7400a53b@172.31.0.252:5061>;av_cm_id=600c00f8-15f3-7f4029c1-529c1;clock=allow> Call-ID: fe3f39942bf41e5841d05056b6ea3 CSeq: 1 REFER Max-Forwards: 70 User-Agent: Avaya CM/R017x.00.0.441.0 x-rt-gslid: 2174be37-9b7d-3536-848d-09e102bf9bb0 Via: SIP/2.0/TLS 172.31.0.211:9061;branch=z9hG4bKfe3f39802bf41e5841d05056b6ea3 Contact: <sip:ACM@172.31.0.211:9061>;transport=tl;sr Route: <sip:172.31.0.252:5061>;transport=tl;sr Refer-To: <sip:AMS_1611399416@172.31.0.211:9061>;transport=tl;sr Content-Type: application/sdp Content-Length: 491 v=0 o=- 1436978339 1 IN IP4 172.31.0.211 s=- c=IN IP4 255.255.255.255 t=0 0 a=templatecrtv1.audio,asme,drpyl,crya,stick,samek,audpl m=audio 0 RTP/SAVP 9 0 8 96 18 127 98 a=sendrecv a=rtcpmap 9 G722/8000	7/15/2015 12:38:59.478001 PM

Copyright 2010-2015 Avaya Inc. All Rights Reserved

The **‘Performance’** monitor (shown below) allows you to monitor Media Server resources, dialog requests, session requests, CPU load and load factor in real-time.

Media Server provides overload controls based on a load factor, which is an aggregated value between 0-100 that is calculated using various measurements like CPU and session count. Once the load factor reaches 100%, Media Server will raise alarm indicating it is overloaded and will reject any new calls with a 503 response so it could continue processing existing calls.



Media Server contains hundreds of OM that can be viewed using **'Operational Measurements'** monitor (shown below). There are 2 types of OM: Counter and Gauges. A counter is always incremented (i.e., total session requests) and are reset to zero at the end of every interval (default is 15 minutes). A gauge value will increase or decrease over time (that is, number of active sessions).



Managing: sst1-ams1.dr.avaya.com, 172.31.0.241

[Home](#) » [System Status](#) » [Monitoring](#) » [Operational Measurements](#)

System Status

Element Status

Cluster Status

Alarms

Logs

Monitoring

Active Sessions

Performance

Operational Measurements

Protocol Connections

Advanced

Applications

General Settings

Operational State

Signaling Translations

Custom Applications

Default Handlers

Cluster Configuration

High Availability

Server Designation

Replication Settings

Load Balancing

Advanced Settings

System Configuration

Server Profile

Network Settings

Signaling Protocols

Media Processing

Application Interpreters

Monitoring Settings

Session Detail Records

Content Store

Logging Settings

Debug Tracing

Engineering Parameters

Element Manager Settings

Licensing

General Settings

Monitoring

Server Status

Operational Measurements

Category: Resource Manager

To search within a category enter a search term.

Active Sessions

Average First Prompt Latency

CPD::AUTH Licenses Available

CPD::AUTH Licenses Total

Connections

Controller Calls Rejected

Add

Select All

Remove

Refresh every 30 seconds

☐ Category	Name	Current Value	Previous Value	Previous Interval Low Water Mark	Previous Interval High Water Mark
☐ Resource Manager	MSML Active Conferences	0	0	0	9
☐ Resource Manager	MSML Active Request	0	0	0	0
☐ Resource Manager	MSML Active Sessions	1142	1157	8	1170
☐ Resource Manager	MSML Request Attempt	0	0	0	0
☐ Resource Manager	MSML Request Failed	0	0	0	0
☐ Resource Manager	MSML Request Success	0	0	0	0
☐ Resource Manager	MSML Session Attempt	1997	1831	0	2131
☐ Resource Manager	MSML Session Failed	413	374	0	399

0 of 8 items selected

Selected Operational Measurement Details

Copyright 2010-2015 Avaya Inc. All Rights Reserved

Media Server Element Manager Element Status

The '**Element Status**' can be used to view or change (start, stop, restart) the media server service status. If any alarms are raised it will display the alarm with the highest severity. The operational state can be viewed or change and Media Server contains the following operational states:

- **Unlocked:** This is the normal operational state of Media Server.
- **Pending Locked:** In this mode Media Server will gracefully reject any new session requests and allow any existing sessions to remain up until they end normally. Typically Media Server will be placed in this state by a services technician prior to starting a maintenance period.
- **Locked:** In this mode any sessions on Media Server will be terminated immediately and any new session requests will be gracefully rejected.

Managing: b31h-asm1.avaya.com, 10.129.130.136

[Home](#) » [System Status](#) » Element Status

Element Status

Click the element name to display the alarm viewer for this element.

Start

Stop

Restart

More Actions

More Actions

Lock

Pending Lock

Refresh every: 5 seconds

Element Name: [b31h-asm1.avaya.com](#)

UUID: d92efde0-afc8-11e4-81ca-e41f13b3430c

Server Address: 10.129.130.136

Operating System: Linux

Service Status: Started

Operational State: Unlocked

Element Status: **Normal**

Alarm Description: No Alarm