



Implementing and Administering Avaya Media Server 7.5

Release 7.5
January 2014

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 generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by 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 Web sites 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 its Hardware and Software ("Product(s)"). 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 Web site: <http://support.avaya.com>. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](http://support.avaya.com/licenseinfo/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER; 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").

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation 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.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://support.avaya.com/Copyright>.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation 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 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, and "Linux" is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: <http://support.avaya.com>.

Contact Avaya Support

See the Avaya Support Web site: <http://support.avaya.com> for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support Web site: <http://support.avaya.com>, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Management interface	9
Introduction to Element Manager	9
EM installation	9
Web browser configuration	9
Enabling SSL file downloads in IE	10
Adding EM to the trusted sites list in IE	10
EM overview	11
EM interface	13
Setting the content pane refresh frequency	15
Advanced settings and engineering parameters	16
Chapter 2: Quick setup	17
Quick installation and configuration	17
Installing on Linux	17
Installing on Windows	18
Configuring Avaya MS using EM	19
Quick call testing, monitoring, and debugging	20
Making a test call and monitoring active sessions	21
Reviewing session detail records	23
Viewing call traces for debugging	24
Chapter 3: Basic management tasks	27
Logging in to and navigating in EM	27
Observing the current operational status using EM	27
Starting and stopping the media server	28
Setting the operational state	29
Managing the High Availability state	31
Viewing the software inventory	32
Reviewing the PVI Checker results	33
System configuration and trace logs	34
Enabling Debug Tracing	34
Downloading log capture	35
Obtaining the UUID of a media server	36
Changing users for EM login on Linux	36
Chapter 4: Configuration	39
Configuration overview	39
Cluster configuration	39
Configuring a Primary server for a cluster	40
Configuring a Secondary server for a cluster	41
Configuring a Standard server for a cluster	43
Configuring the replication settings for a cluster	44
Configuring replication of Content Store data between clusters	45
Disabling replication of Content Store data between clusters	46
Configuring SIP load balancing for a cluster	46
Replication of configuration settings in a cluster	47
High Availability configuration	48

High Availability synchronization overview.....	48
Restrictions and limitations of High Availability.....	49
Configuring the Primary server for High Availability.....	49
Configuring the Backup server for High Availability.....	51
Completing High Availability cluster configuration.....	52
Enabling High Availability.....	53
Reviewing High Availability configuration and status.....	54
Changing the Service IP Address for a High Availability configuration.....	56
Replication of configuration settings in a High Availability configuration.....	57
License configuration.....	58
Configuring License Server keys.....	58
Configuring License Server chunk size.....	60
Updating License Server keys.....	61
Configuring Nodal Licensing.....	61
Updating Nodal Licensing keys.....	62
Configuring WebLM Server licensing.....	63
License utilization alarm threshold configuration.....	65
Modifying predefined server profiles.....	66
Network settings configuration.....	66
Setting the SNTP source server.....	66
Enabling SNMP traps.....	67
Configuring the Avaya MS SNMP agent.....	68
Configuring SOAP.....	68
Configuring connection security options.....	69
Configuring transmit prioritization.....	70
Selecting IP interface assignments.....	71
Computer name and IP address modification.....	73
Changing the computer name on Linux.....	73
Changing the computer name on Windows.....	74
Changing the IP address on Linux.....	75
Changing the IP address on Windows.....	76
SIP configuration.....	77
Configuring SIP general settings.....	77
Adding SIP domains.....	80
Adding SIP accounts.....	81
Configuring SIP trusted nodes.....	81
Configuring SIP routes.....	82
Configuring SIP route properties.....	84
Editing a SIP domain or a SIP account.....	86
Changing the SIP account password.....	86
Deleting a SIP domain or a SIP account.....	87
Editing a SIP trusted node or a SIP route.....	87
Deleting a SIP trusted node or a SIP route.....	88
MRCP configuration.....	88
Configuring an MRCP general settings.....	88
Adding an MRCP server.....	90
Adding MRCP server resources.....	92

Adding an MRCP pool.....	94
Adding a server to an MRCP pool.....	96
Adding custom MRCP vendors.....	96
Editing custom MRCP vendors.....	97
Deleting custom MRCP vendors.....	98
Editing an MRCP server or server resources.....	98
Deleting an MRCP server.....	99
Deleting MRCP server resources.....	99
Editing an MRCP pool.....	100
Changing status of MRCP pools.....	100
Deleting an MRCP pool.....	101
Removing MRCP server from a pool.....	101
Media settings configuration.....	102
Configuring QoS monitoring settings.....	102
Configuring QoS streaming settings.....	103
Configuring silence suppression.....	104
Configuring continuous STOUTCast streaming.....	105
Configuring continuous RSS streaming.....	107
Enabling and configuring audio codec settings.....	108
Removing an audio codec.....	109
Enabling and configuring video codec settings.....	110
Removing a video codec.....	111
Enabling and configuring digit relay settings.....	111
Removing a digit relay method.....	112
Media security configuration.....	113
Security configuration.....	118
Configuring the System Manager settings.....	118
Creating a new certificate signed by System Manager in the Key Store.....	118
Creating a new certificate to be signed by other Certificate Authorities in the Key Store.....	119
Creating a new self-signed certificate in the Key Store.....	119
Processing a Certificate Signing Request Response in the Key Store.....	120
Creating a renewal Certificate Signing Request to be signed by the original signing Certificate Authority.....	120
Deleting a pending Certificate Signing Request (new or renew).....	121
Assigning a certificate for a Service Profile.....	121
Unassigning a certificate for a Service Profile.....	121
Importing a certificate for Service Profile.....	122
Exporting a Key Store certificate in PEM format.....	122
Exporting a Key Store certificate with a key.....	123
Importing a trust certificate to the Trust Store.....	123
Importing a Trust Certification Revocation List.....	123
Downloading a Certification Revocation List.....	124
Deleting Certificate Authorities from the Trust Store.....	124
Content Store configuration.....	124
Configuring Content Store location.....	124
EM preferences configuration.....	126
Configuring time zone preferences.....	126
Setting Login security warning text.....	126

Chapter 5: Media file provisioning.....	127
Media file format.....	127
Media storage in Avaya MS Content Store.....	127
Overview of the EM Media Management tool.....	128
Media Provisioning.....	129
Adding a content namespace.....	129
Renaming a content namespace.....	130
Deleting a content namespace.....	130
Viewing namespace content.....	131
Adding a content group.....	131
Adding media files on the server to a content group.....	132
Downloading media files to your computer.....	133
Renaming a content group.....	133
Deleting a content group.....	134
Batch provision media.....	135
Searching for a media file.....	136
Renaming a media file.....	137
Moving a media file.....	138
Copying a media file.....	138
Deleting a media file.....	139
Chapter 6: Application management.....	141
Enabling CCXML and VoiceXML applications.....	141
Adding CCXML and VoiceXML custom applications.....	141
Editing CCXML and VoiceXML custom applications.....	142
Application interpreter configuration.....	142
Configuring RFC5707 (MSML) interpreter.....	142
Configuring VoiceXML interpreter.....	143
Configuring CCXML interpreter.....	143
Viewing or changing application operational state.....	144
Viewing or changing custom application operational state.....	144
Configuring application signaling translations.....	145
Deleting application signaling translations.....	145
Deleting a custom application.....	146
Configuring packaged applications.....	146
Chapter 7: Backup and restore.....	147
Backup and restore overview.....	147
Configuring a backup task.....	147
Executing a backup task.....	150
Deleting a backup task.....	150
Editing a backup destination.....	151
Restoring from the local destination.....	151
Uploading a backup file for restore.....	152
Viewing the backup and restore history log.....	153
Configuring the history log.....	153
Using the command-line backup and restore tool.....	154
Chapter 8: Avaya MS monitoring.....	157
Avaya MS monitoring overview.....	157

Element status viewing.....	157
Viewing cluster status.....	157
Monitoring alarms.....	158
Monitor event logs.....	161
Viewing event logs.....	162
Configuring event log throttling.....	164
Configuring log filter settings.....	165
Viewing security logs.....	168
Configuring SysLog settings.....	169
Monitor active sessions.....	170
Viewing current active sessions.....	170
Viewing details for a specific session.....	172
Releasing one or more sessions.....	174
Muting and unmuting sessions.....	175
Monitoring system performance.....	176
OM monitoring.....	178
Configuring OM settings.....	178
Configuring OM delivery.....	179
Configuring OM archiving.....	181
Monitoring protocol connections.....	181
Advanced system monitoring.....	182
Viewing component status.....	182
Viewing advanced protocols.....	183
System license monitoring.....	183
Monitoring License Server status.....	183
SDR monitoring.....	184
Reviewing SDRs.....	184
Determining peak session traffic.....	186
Summarizing daily inbound traffic.....	187
Analyzing hourly inbound traffic details.....	188
Reviewing a monitored SDR.....	189
Configuring SDR archiving.....	193
Configuring Field Promotion for SDR reports.....	194
Enabling enhanced SDRs for troubleshooting.....	196
Chapter 9: Troubleshooting.....	199
Introduction to troubleshooting.....	199
Element Manager troubleshooting.....	199
Cannot log in to EM after installation on Linux.....	199
Cannot log in to EM after installation on Windows.....	201
Cannot log in to EM using a new user account on Windows.....	202
Cannot log in to EM using the EM desktop shortcut with IE.....	202
EM cannot download files when using IE.....	204
EM displays a blank page after login when using IE.....	204
The EM Media Management tool is slow.....	204
Call completion troubleshooting.....	205
Avaya MS rejects incoming SIP sessions.....	205
Unsupported codec response from Avaya MS.....	207

TLS connection issues.....	208
Digit collection issues.....	209
Media playback troubleshooting.....	210
Unable to playback provisioned audio file.....	210
RSS and SHOUTCast troubleshooting.....	210
Users do not hear streaming SHOUTCast audio.....	210
Users do not hear streaming RSS audio.....	211
High Availability troubleshooting.....	212
Cannot enable High Availability because it is disabled.....	212
Protocol troubleshooting.....	213
SNMP Traps are not getting posted on management consoles.....	213
SMTP mail delivery is not working.....	215
SOAP connection is rejected.....	215
Index.....	217

Chapter 1: Management interface

Introduction to Element Manager

Element Manager (EM) is an optional, Web-based administration tool that facilitates the operation, administration, and maintenance (OAM) of Avaya Media Server (MS).

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

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

EM installation

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

Install EM to configure Avaya MS if you do not have an alternate OAM management system. The installation procedures for Avaya MS cover the EM installation option in detail.

Web browser configuration

You can gain access to EM using a Web browser that you start locally on the server or remotely from another computer. EM works with Internet Explorer (IE) versions 6, 7, 8, and 9 and with Firefox versions 3.5 and later.

To use IE 9 with EM, configure IE 9 to:

- Download files from secure sites using SSL.
- Treat Avaya MS as a trusted site.

Perform the following procedures to configure IE 9 and later for EM.

Enabling SSL file downloads in IE

About this task

Configure IE to download files from secure sites using SSL so that you can upload and download files using EM.

Procedure

1. Open IE.
 2. From the IE menu bar, select **Tools > Internet Options**.
If the menu bar is not visible, press the **Alt** key.
 3. Click the **Advanced** tab.
 4. In the **Settings** section, scroll down to **Security**.
 5. Clear the **Do not save encrypted pages to disk** check box.
 6. Click **OK**.
 7. Close and reopen the IE browser.
-

Adding EM to the trusted sites list in IE

About this task

Configure IE to consider Avaya MS as a trusted site so that you can gain access to EM.

Procedure

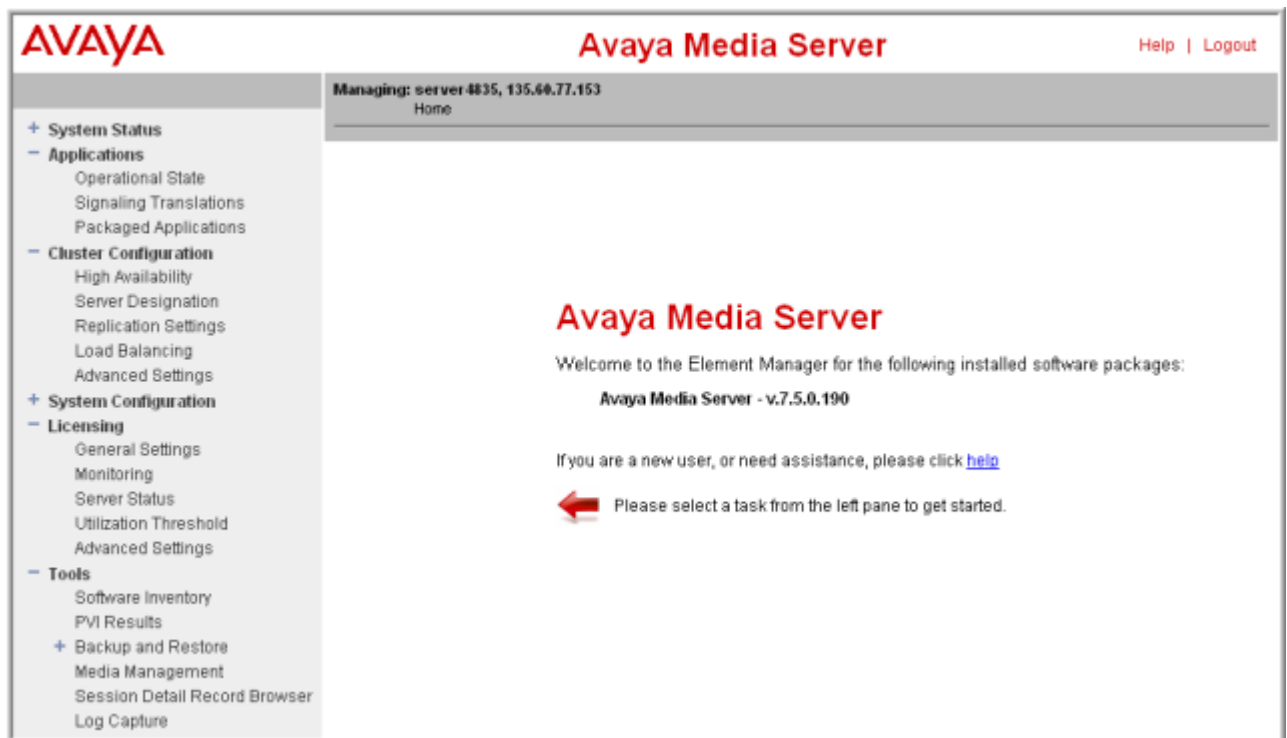
1. Open IE.
2. From the IE menu bar, select **Tools > Internet Options**.
If the menu bar is not visible, press the **Alt** key.
3. Click the **Security** tab.
4. Select the **Trusted sites** zone.
5. Click **Sites**.
6. Enter the address of Avaya MS in the **Add this website to the zone** field. For example:
`https://localhost`
`https://server123.companyABC.com`
7. Click **Add**.

8. Click **Close**.
9. Click **OK**.

EM overview

The EM layout includes a branding banner at the top, a task pane at the left, a content pane at the right for management activities, and a navigation bar at the top of the content pane. The upper-right corner of the EM page has **Help** and **Logout** links.

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



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

The screenshot displays the Avaya Media Server management interface. The top header includes the Avaya logo, the title 'Avaya Media Server', and links for 'Help' and 'Logout'. Below the header, a breadcrumb trail shows 'Home > System Status > Element Status'. The left sidebar contains a navigation menu with categories: System Status, Applications, Cluster Configuration, System Configuration, Licensing, and Tools. The main content area is titled 'Element Status' and includes a sub-header 'Click the element name to display the alarm viewer for this element.' Below this, there are buttons for 'Start', 'Stop', 'Restart', and 'More Actions', along with a 'Refresh every: 5 seconds' dropdown. The main content area displays the following information:

- Element Name: [server4835](#)
- UUID: 835c8aa4-6d0b-11e0-958e-001f296491ca
- Server Address: 135.60.77.153
- Operating System: Linux
- Service Status: Started
- Operational State: Unlocked
- Element Status: **Critical Alarm(s)**
- Alarm Description: MAS Instance is not licensed

Below the main content area, there is a section for 'Installed Software Packages' showing 'Avaya Media Server - v.7.5.0.190' with a description: 'A software based application platform that provides infrastructure for a diverse range of multimedia services.'

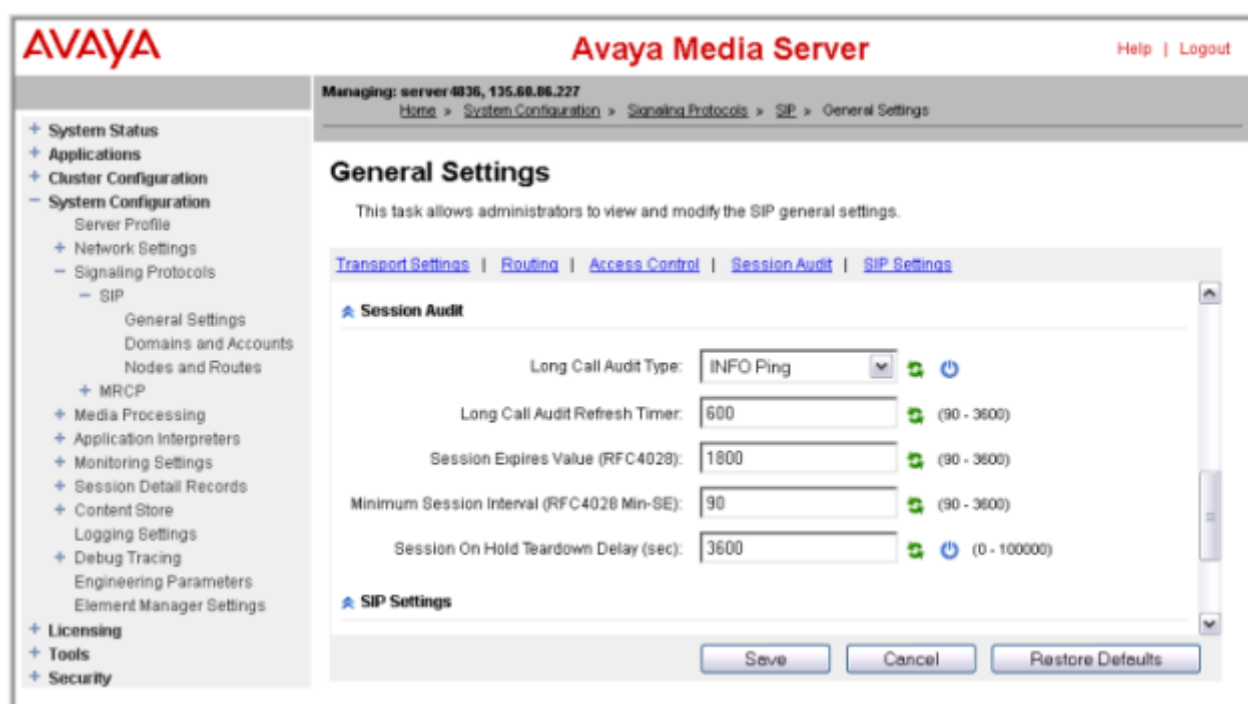
The tasks pane on the left lists all the actions that an administrator performs for Avaya MS OAM. The actions are grouped into categories as follows:

Actions	Description
System Status	Presents a view of the current and historical information pertaining to the status of the system. These tasks include element status, cluster status, alarm viewing, event log viewing, and monitoring. The monitoring task includes performance monitoring, operational measurements, and protocol monitoring of Avaya MS. Active session monitoring includes graphical SIP message flows and SIP traces showing details of the messages for a particular session.
Applications	Lists all installed applications, whether custom or packaged. Expanding an application displays all tasks specific to the operation, administration, and maintenance of that application.
Cluster Configuration	Provides tasks for server designation, replication settings, clustering and high availability configuration, and load balancing settings.

Actions	Description
System Configuration	Categories include server profiles, network settings, signaling protocols, media processing, application interpreters, monitoring settings, session detail records, engineering parameters, EM settings, and SIP routing. The administrator can view and modify Avaya MS platform configuration.
Licensing	Provides an interface to configure and monitor the licensing services.
Tools	Provides utilities to view which software versions are installed, perform a backup or restore of system and customer data, manage media, view session detail records, and collect logs.
Security	Provides an interface for Security related configuration.

EM interface

The following figure illustrates the features of the EM interface:



Task navigation

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

Click the minus sign (-) before the label to collapse expanded items. The subtasks remain expanded when you collapse the parent task.

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

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

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

Scroll bars

The system displays vertical scroll bars when the system cannot display the content in a window without vertical clipping. The system displays horizontal scroll bars when the system cannot display the content in a window without horizontal clipping. You can reduce horizontal clipping by using the vertical line separating the menu pane and the content areas to resize the menu pane horizontally.

Disabled items

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

Saving configuration changes

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

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

Undo changes

You can use the restore default icon button () next to the fields, to restore individual configuration items to the default value that Avaya provides. You can use the **Restore Default** button, located next to the **Save** and the **Cancel** button, to restore all the fields on the

current page to the default values. Click **Save** to apply the restored default values to the system.

System restarts

The system designates any field that needs a restart for the change to take effect with a restart icon (🔌). For these fields, saving the change only saves the change in the system database. Restart the system before the change is applied to any system processing.

Data validation

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

Help

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

Setting the content pane refresh frequency

About this task

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

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

Procedure

1. Navigate to **EM > System Status > Element Status** or to any task with the refresh option.
2. Click the **Refresh every** drop-down menu and select refresh interval.
The content you are viewing refreshes at the selected frequency.

Advanced settings and engineering parameters

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

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

Chapter 2: Quick setup

Quick setup describes the basic minimum procedures to quickly install and commission a stand-alone Avaya Media Server (MS). You also learn how to place RFC4240 calls to the server, monitor active calls, and review detailed records of the call sessions.

Quick installation and configuration

This simplified procedure for installing Avaya MS takes you through the following tasks:

- Installing Avaya MS software with Element Manager (EM)
- Licensing and minimally configuring the server
- Restarting the Avaya MS software
- Placing and monitoring an RFC4240 call

Follow the topics in this chapter sequentially for a quick installation and configuration of Avaya MS.

Before installing and configuring Avaya MS, make sure you have an acceptable platform with both hardware and operating system software which meet the minimum requirements and prerequisites for Avaya MS installation. For detailed system information, see Hardware and Software Requirements in *Installing, Upgrading, and Patching Avaya Media Server 7.5*. The document also includes additional installation methods beyond the ones outlined in the following procedures.

Installing on Linux

Procedure

1. Open a Linux shell on the target system.
2. Change to root user by running the following command:

```
su -
```
3. Download the installer to the server, or insert the Avaya MS installation DVD into the DVD drive of the server.
4. Change the current directory to the directory containing the downloaded installer or to the drive mount where the Avaya MS installation DVD resides.

The name of the installation file is in the following format:

`MediaServer_x.y.z.bbb_yyyy.mm.dd.bin`

For example: `MediaServer_7.5.0.231_2011.11.06.bin`.

5. Apply executable permissions to the installer file:

`chmod 755 <filename>`

6. Enter the following command to run the installer:

`./<filename>`

where `<filename>` is the Avaya MS installer.

7. Read the Introduction details and press `Enter`.
8. At the License Agreement prompt, press `Enter` to read through the pages of license agreement.
9. To accept the terms of the license agreement, enter `Y` and press `Enter`.
10. Accept the default option to install EM by pressing `Enter`.
The installer prompts you for a Linux group name to use for the EM login.
11. Press `Enter` to accept the default group, or type an existing Linux group and press `Enter`.

 Important:

The Linux group you specify must contain users that can successfully authenticate against Secure Shell (SSH).

12. To begin installation, choose the installation destination by specifying a location of your choice or accept the default location by pressing `Enter`.

Installing on Windows

Procedure

1. Download the installer to the server, or insert the Avaya MS installation DVD into the DVD drive of the server.
2. Using Windows Explorer, locate the downloaded installer or the drive where the Avaya MS installation DVD resides.
The name of the installation file is in the following format:
`MediaServer_x.y.z.bbb_yyyy.mm.dd.exe`
For example: `MediaServer_7.5.0.231_2011.11.06.exe`.
3. Double-click the installation file.

4. In the Overview window, click **Next**.
 5. In the License Agreement window, select **I accept the terms of the License Agreement**.
 6. Click **Next**.
 7. Select **Install Element Manager**.
 8. Click **Next**.
 9. In the Choose Install Folder window, click **Install** to install the software to the default folder or a folder you specify.
 10. Click **Next**.
 11. To restart the system, select **Restart** and then click **Done**.
-

Configuring Avaya MS using EM

About this task

Perform the following procedures using EM to configure items and tasks required to activate Avaya MS:

- Installing a license
- Enabling Trusted node access for SIP
- Restarting the Avaya MS software

Procedure

1. To gain access to EM, use a Web browser with this URL:
`http://<serverIP>:8080/em`, where `serverIP` is the address of your server.
 For example, `http://135.60.86.209:8080/em`.
2. Log in using the server admin or root user and password.
3. Specify whether you want to disable trusted node access for this Avaya MS, or add the SIP Nodes from which you get calls to the trusted nodes list.
 To disable trusted SIP node access:
 - a. Navigate to **EM > System Configuration > Signaling Protocols > SIP > General Settings > Access Control**.
 - b. Clear **Trusted Node Access Only**.
 - c. Click **Save**.
 To add trusted SIP nodes to the trusted nodes list:
 - a. Navigate to **EM > System Configuration > Signaling Protocols > SIP > Nodes and Routes > Trusted Nodes**.

- b. Click **Add...**
 - c. Enter the IP of the SIP node from where you will get the test call.
 - d. Click **Save**.
4. To add the license to the media server, navigate to **EM > Licensing > General Settings**, and use one of the following to install your license:
 - If you use Nodal Licensing:
 - i. Ensure the **Licensing** drop-down menu is set to **Nodal Licensing**.
 - ii. Copy the complete license key provided to you.
 - iii. Paste the license into the **Keys** field.
 - iv. Click **Save**.
 - If you use a License Server:
 - i. Ensure the **Licensing** drop-down menu is set to **License Server**.
 - ii. Copy the complete license key provided to you.
 - iii. Paste the license into the **Add License Keys** field.
 - iv. Click **Validate**.
 - v. Click **Save**.
 - vi. Click **Confirm**.
 - If you use an Avaya WebLM license, see Configuring WebLM server licensing.

Related topics:

[Configuring WebLM Server licensing](#) on page 63

Quick call testing, monitoring, and debugging

This simplified procedure for using Avaya MS takes you through the following tasks:

- Placing a RFC4240 call
- Viewing an active session on the management system
- Reviewing the session records
- Using a SIP message trace for debugging

Making a test call and monitoring active sessions

About this task

To quickly and easily make test calls to the media server using the built-in RFC4240 conferencing application, you need two SIP clients and an installed, licensed, and running Avaya MS.

Procedure

1. Create a session on your running and licensed Avaya MS by placing a RFC4240 conference call to the built-in conference application, using an address such as the following in a SIP client: `conf=<confname>@<serverIP>`, where *confname* is the name of your choice for your conference and *serverIP* is the address of your server. For example: `conf=test@135.60.86.209`.
2. After Avaya MS answers the call, monitor the active session on Avaya MS by navigating to **EM > System Status > Monitoring > Active Sessions**.
3. Follow the on instructions to download and install Microsoft Silverlight, if you have not already installed Microsoft Silverlight for your browser.

On the **Active Sessions** page, you can see the resources used by your session.

You can see one Active Sessions, one Conference Resource, and your session details listed at the bottom of the page.

4. You can use the **Refresh** button and the refresh interval drop-down menu to refresh current data.

Active Sessions (Cluster)

Active Sessions: 1	Conference Resources: 1	Session Attempts/Interval: 1
IVR Resources: 2	MRCP Resources: 0	CPU Load (%): 0

Viewing Active Sessions

Filter: None Sessions Listed: 1

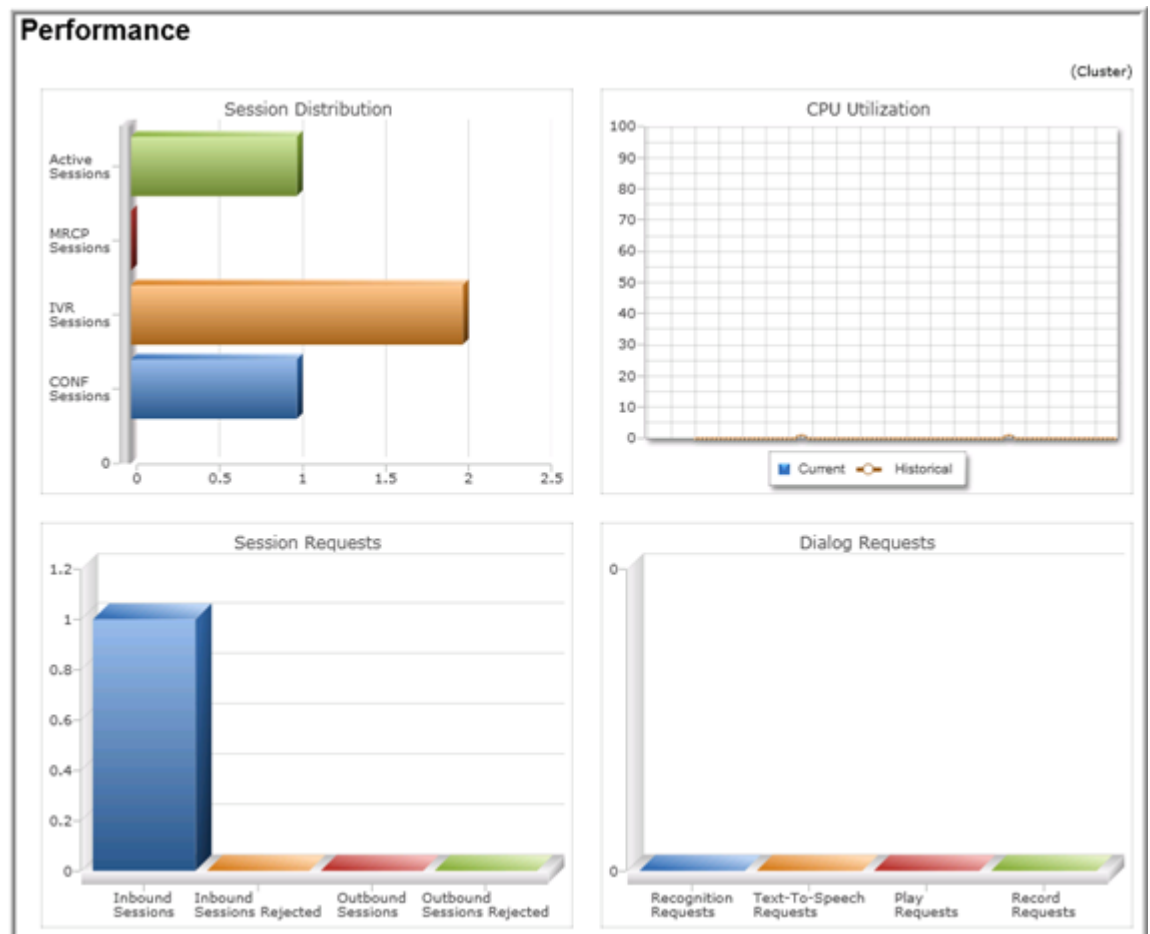
Criteria: None Filtered Sessions: 0

Select... Refresh Every 30 Seconds

Remote Party	Start Timestamp	Application Name	Endpoint	QOS R-Factor	QOS Rou
"Paul"<slip:pd@avaya.com>	4/27/2011 10:45:18 AM	RFC4240	Nortel PCC 7.4.40	91	66

You can monitor system performance by comparing the number of sessions with the CPU utilization.

5. Navigate to **EM > System Status > Monitoring > Performance** to see graphs of the current system performance.



6. Place a second call from another client in the same conference, `conf=test@135.60.86.209`.
7. You can see the resources used as a result of your second call on the **Active Sessions** page.
You can see two Active Sessions, one Conference Resource, and your second call details listed at the bottom of the . You can also see similar changes on the **Performance** page.

Active Sessions (Cluster)

Active Sessions: 2 Conference Resources: 1 Session Attempts/Interval: 2

IVR Resources: 3 MRCP Resources: 0 CPU Load (%): 0

Viewing Active Sessions

Filter: Sessions Listed: 2

Criteria: Filtered Sessions: 0

Select... Every

Remote Party	Start Timestamp	Application Name	Endpoint	QOS R-Factor	QOS Round
"Paul"<slp:pd@avaya.com>	4/27/2011 10:45:18 AM	RFC4240	Nortel PCC 7.4.40	91	66
"David"<slp:dm@avaya.com>	4/27/2011 10:45:36 AM	RFC4240	Nortel PCC 7.4.40	91	62

- End one call and then end the other call while looking at the **Active Sessions** page.
The system frees the resources and removes call end points from the list.

Reviewing session detail records

About this task

Calls generate Session Detail Records (SDRs) to capture all the information about the session. EM has an SDR Browser to review the details of any sessions handled by the media server. There are many queries and filter options available to help you find particular sessions.

Perform the following procedure to review the SDRs for the test calls you completed:

Procedure

- To browse a Session Detail Record (SDR) for a past call, navigate to **EM > Tools > Session Detail Record Browser**.
- Execute a query with a time range which includes the time frame for your test calls.
For example, advance the **Start** date back one day and the **End** date forward one day and then click **Execute**.
- Click one of the rows in the list of sessions which appear as a result of the query execution.
You can see the details of the session in the **Session Detail Records** pane.

Session Detail Record Browser

Query (server4803)

Type: Browse Records In Date Range Limit: 100 4/27/2011 11:27:34 AM Central Standard Time

Start: 4/26/2011 15 7:00:00 PM ☒ Use Local Time

End: 4/28/2011 15 11:59:59 PM Execute

Global Session Id	Start Timestamp	End Timestamp	Server
a638f32-2e9c-3bb7-af3e-b1cb0d80db5c	4/27/2011 10:45:18 AM	4/27/2011 10:56:34 AM	server4803
0f5061f5-374a-3b1b-97f5-860176c50a8b	4/27/2011 10:45:36 AM	4/27/2011 10:48:26 AM	server4803
a35ce6a7-a063-3627-860c-3164de7d57fb	4/27/2011 10:13:44 AM	4/27/2011 10:44:38 AM	server4803
ef7e39c5-a6e2-33cf-88c1-667c78d1f7f4	4/27/2011 9:20:04 AM	4/27/2011 9:20:04 AM	server4803

Result

Session Detail Records

Filter: None ☒ Display Trace Details

Field	Value	Timestamp
Global Session Id	0f5061f5-374a-3b1b-97f5-860176c50a8b	4/27/2011 10:45:36 AM
Start Timestamp	2011-04-27 15:45:36	4/27/2011 10:45:36 AM
Server	server4803	4/27/2011 10:45:36 AM
SIP Remote User Information	"David"<sip:dm@avaya.com>	4/27/2011 10:45:36.522 AM
Application Name	RFC4240	4/27/2011 10:45:36.523 AM

Viewing call traces for debugging

About this task

You can debug calls using the **Active Sessions** page. SIP message details, session filters, resource consumption statistics, and graphical SIP message flows provide you the necessary tools to trace and troubleshoot call processing problems.

Procedure

1. Navigate to **EM > System Status > Monitoring > Active Sessions**, to set up trace monitoring, before making the call.
2. On the **Active Sessions** page, from the **Select...** drop-down list, select **Monitor Next Session**.
The system displays a message to inform that the system is waiting for a new session to start.
3. Call the built in conference application, using an address such as your SIP client: `conf=<confname>@<serverIP>`, where *confname* is the name of your choice for your conference and *serverIP* is the address of your server. For example, `conf=test@135.60.86.209`.

After answering your call, the system displays a detailed call performance summary in the **Active Sessions** page.



4. To view session records of the call including the SIP message content, select **Select Viewing Options... > View Session Detail Records**.

Active Sessions

Filter: None Viewing Session Detail Records Records Listed: 19
Gslid: 57b7bbaa-bf9c-355d-6e19a1696a96 Filtered Records: 0

Select Viewing Options... Stop Monitoring

Field	Value	Timestamp
Global Session Id	57b7bbaa-bf9c-355d-6e19a1696a96	4/27/2011 1:43:23 PM
Start Timestamp	2011-04-27 18:43:23	4/27/2011 1:43:23 PM
ENG[001-A] <idle> Incoming SIP Message: INVITE sip:conf-test@135.60.86.209 SIP/2.0		
INVITE sip:conf-test@135.60.86.209 SIP/2.0		
From: "Paul"<sip:pd@avaya.com>;tag=a9-15ec-4b4-fffff		
To: <sip:conf-test@135.60.86.209>		
Call-ID: 6eca54892d4b4ed1745e8d34c0b6d478234a654@135.60.77.24		
CSeq: 1 INVITE		
Via: SIP/2.0/UDP 135.60.77.24.5060;branch=z9hG4bK-a8732f-9201efe6-4cbf958f		
Contact: <sip:pd@135.60.77.24.5060;nt_end_pt=YM0+~Kp1IAkP-Q041tnk_CB.1Ez-Unc_mg6vk ey-H9_Swt7mN-PcT2Zi9yXDJy.1-6n5a5>		
S417-LKT_cKbnYraus4-Mi7B-AAf4m-Nn7XKGFOuk~X9rnelgOpimy-LWMrZelCRke30PJ-AAf_cod-PSS.QfOlcc-24bzb99yfrp9P-RT2mJEv6S86QtdE1.nt_server_host=135.60.77.24.5060		

5. To view a graphical SIP message flow, select **Select Viewing Options... > View SIP Protocol Trace**.



6. End the call.
7. Click **Stop Monitoring**.

Chapter 3: Basic management tasks

Logging in to and navigating in EM

About this task

Perform the following procedure to gain access to Element Manager (EM) management system for Avaya Media Server (MS):

Procedure

1. Use a Web browser with this URL:
`http://<serverIP>:8080/em`, where *serverIP* is the address of your server.
For example, `http://135.60.86.209:8080/em`.
2. Log in using the server admin or root user and password.

Perform the procedure when you see navigation steps in this document. For example, if you see **EM > System Status > Element Status**, follow Step 1 and Step 2 to gain access to EM. After you have logged in to EM, click **System Status** and then click **Element Status**.

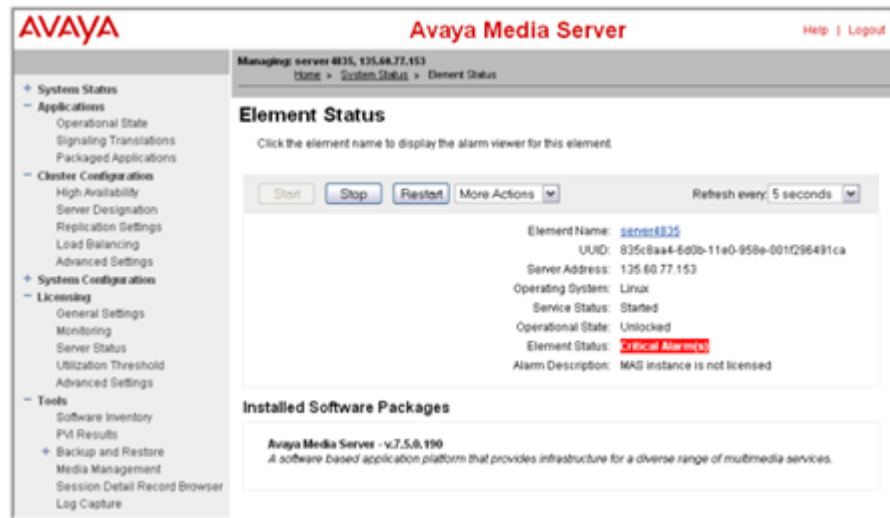
Observing the current operational status using EM

About this task

Perform the following procedure to observe the current operational status of the server you are administrating:

Procedure

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



On the **Element Status** page you can find:

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

Starting and stopping the media server

Before you begin

Avaya recommends that you set the Operational State of the Avaya MS to Pending Lock and then Lock before stopping or restarting a server with active sessions. For details, see Setting the operational state.

About this task

Perform the following procedure to Start, Stop or Restart Avaya MS using EM. The Start, Stop and Restart actions for Avaya MS operate as follows:

Action	Description
Start	The Service Status of Avaya MS must be set to Stopped before you can start Avaya MS. Starting Avaya MS launches all the necessary software processes to enable media server functionality.
Stop	The Service Status of Avaya MS must be set to Started before you can stop Avaya MS. Stopping Avaya MS ends all software processes that enable media server functionality and take the element out of service.
Restart	The Service Status of Avaya MS must be set to Started before you can restart Avaya MS. Restarting Avaya MS is the same as stopping the media server and then starting the media server again.

Procedure

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

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

Related topics:

[Setting the operational state](#) on page 29

Setting the operational state

About this task

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

Operational state	Description
Lock	The Operational State of Avaya MS must be set to Unlocked or Pending Locked before you can lock Avaya MS. When the media server enters a locked state, the system ends existing sessions, does not accept new requests, and redirects new traffic to other nodes in the cluster. You typically place the system into locked state when performing maintenance.
Unlock	The Operational State of Avaya MS must be set to Locked or Pending Locked before you can unlock Avaya MS. Unlocking allows incoming session requests to be accepted by the system for processing.
Pending Lock	The Operational State of Avaya MS must be set to Unlocked or Locked before you can transition to Pending Lock on Avaya MS. When the system enters a Pending Locked state, the system does not accept new requests and redirects new traffic to other nodes in the cluster. Unlike Lock , Pending Lock preserves existing sessions. You typically place the system into a Pending Locked state before transiting to a Locked State when you prepare for system maintenance. This allows sessions to naturally end over time, without being ended unexpectedly for users of the system.
Failover	If you select Failover when the media server is in a High Availability configuration with another node, all the active sessions are transitioned from this media server to the peer. The peer automatically becomes the active node. All new session requests are automatically directed to the newly active peer node. The failed node enters the Standby state and is ready for maintenance or other activities while the peer continues to provide service.

Procedure

1. Navigate to **EM > System Status > Element Status**.
2. Click **More Actions** and select the state from the list of applicable states. The list is dynamic and is dependent on the current state.
3. Click **Confirm** to proceed with the action.

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

Managing the High Availability state

About this task

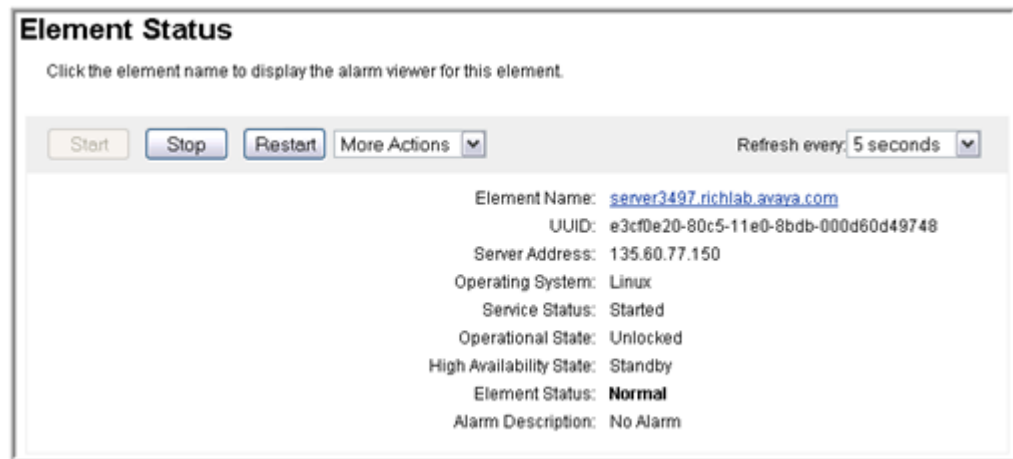
If you have configured Avaya MS for High Availability, the system displays the High Availability state of the server on **EM > System Status > Element Status** page. The **More Actions** drop-down menu contains state transition options which are available only when HA is enabled. The High Availability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

High availability state	Description
Active	The server has a configured Service IP address and is providing service.
Standby	The server is inactive but remains synchronized with the active server.
Failed	The server has determined that it has failed. The server will soon restart and transition to a Searching state.
Locked Active	The active HA server is Locked Active when Local High Availability State Lock (Cluster Configuration > High Availability) is selected and the server is not shutdown.
Locked Standby	The standby HA server is Locked Standby when Local High Availability State Lock (Cluster Configuration > High Availability) is selected, and the server is not shutdown.
Shutdown	The server is in a management shutdown state and is not providing service.
Searching	The server tries to determine the state of the other server in the HA pair. The server remains in this state for less than a second before transiting to the Active or the Standby state.

Procedure

1. Navigate to EM for one of the paired High Availability servers, and then navigate to **EM > System Status > Element Status**.

The following image shows that servers in the High Availability mode display an additional field, **High Availability State**, on the **Element Status** page.



2. Use the **More Actions** drop-down menu to select **High Availability State**. For example, you can choose **Failover**.
The High Availability states listed on the menu are dependent upon the current **High Availability State**, which is shown on the **Element Status** page.
3. Read the warning and then click **Confirm** to apply the state change.
4. On the **Element Status** page, ensure that the **High Availability State** now reports the new state.

Viewing the software inventory

About this task

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

Perform the following procedure to gain access to the software inventory:

Procedure

To display the list of installed software with the corresponding version and patch level information, navigate to **EM > Tools > Software Inventory**.

Software Name	Version	Patch Level
Avaya Media Server	7.5.0.242	None
Element Manager	7.5.0.242	None

The system shows a tabular view of the installed software with the version and patch level information.

You can sort the columns on the **Software Inventory** page in the ascending or descending order by clicking the column name.

Reviewing the PVI Checker results

About this task

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

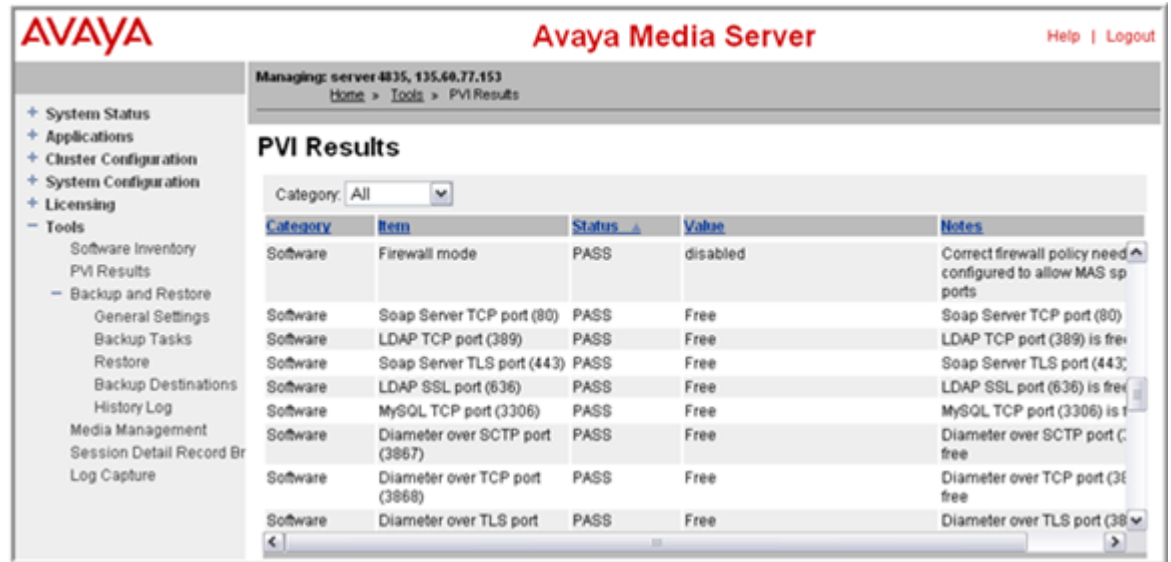
The Platform Vendor Independent Checker (PVI Checker) software ensures that the server and the configured operating system meet the hardware, software, and storage requirements for Avaya MS.

PVI Checker is integrated into the Avaya MS installer and produces a report which is stored in the system for reference.

Procedure

To review the report, navigate to **EM > Tools > PVI Results**.

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



Avaya Media Server

Managing: server 4835, 135.60.77.153
Home > Tools > PVI Results

PVI Results

Category: All

Category	Item	Status	Value	Notes
Software	Firewall mode	PASS	disabled	Correct firewall policy need configured to allow MAS sp ports
Software	Soap Server TCP port (80)	PASS	Free	Soap Server TCP port (80)
Software	LDAP TCP port (389)	PASS	Free	LDAP TCP port (389) is free
Software	Soap Server TLS port (443)	PASS	Free	Soap Server TLS port (443)
Software	LDAP SSL port (636)	PASS	Free	LDAP SSL port (636) is free
Software	MySQL TCP port (3306)	PASS	Free	MySQL TCP port (3306) is free
Software	Diameter over SCTP port (3867)	PASS	Free	Diameter over SCTP port (3867)
Software	Diameter over TCP port (3868)	PASS	Free	Diameter over TCP port (3868)
Software	Diameter over TLS port (3869)	PASS	Free	Diameter over TLS port (3869)

System configuration and trace logs

The Log Capture tool provides an easy way to collect all system configuration and trace logs that might be required by Avaya technical support teams to debug system issues you have reported.

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

Enabling Debug Tracing

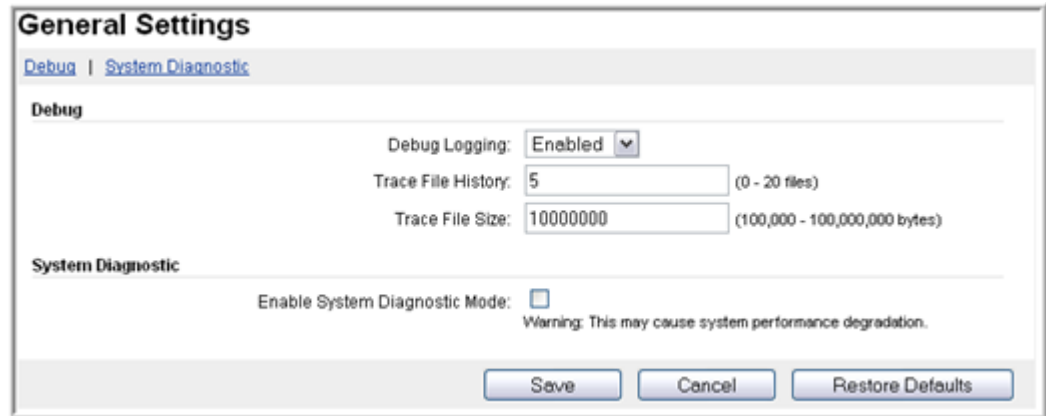
About this task

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

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

Procedure

1. Navigate to **EM > System Configuration > Debug Tracing > General Settings**.



2. Select **Enabled** from the **Debug Logging** drop-down menu.
3. If instructed by Avaya support engineers, change the **Trace File History**.
Trace File History defines the number of rotating trace files to keep before discarding the oldest files. Increasing this value allows more data to be collected, but consumes more disk space.
4. If instructed by Avaya support engineers, change the **Trace File Size**.
Trace File Size defines the size of the trace files. Increasing this value allows more data to be collected, but consumes more disk space.
5. Click **Save**.

Downloading log capture

About this task

The Log Capture tool collects advanced system trace and debug logs required by support engineers to troubleshoot your system. When instructed by Avaya support engineers, ensure that you enable debug logging to collect required traces before using the log capture tool.

Procedure

1. Navigate to **EM > Tools > Log Capture**.
2. If instructed by Avaya support engineers, select **Include trace logs**.
3. If instructed by Avaya support engineers, select **Include video capture**.
4. Click **download**.
 The system gathers all the trace files together in the form of a zip file and displays a dialog box for you to save the file in your computer.

Obtaining the UUID of a media server

About this task

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

Perform the following procedure to gain access to the UUID:

Procedure

1. Navigate to **EM > Cluster Configuration > Server Designation**.
In the content pane, under **Local Server**, you can see the server **Name**, **Address**, **Role**, and the **UUID** which looks similar to this:
835c8aa4-6d0b-11e0-958e-001f296491ca.
 2. Highlight the UUID.
Ensure you get all the characters. Triple-clicking on the UUID works in most browsers.
 3. To copy the highlighted UUID, select **Copy** from the **Edit** menu of your browser, or press `Control+C`, or right-click **UUID** and select **Copy**.
 4. Click in the target field related to the cluster configuration procedure you are following.
 5. To paste the UUID in the field, select **Paste** from the **Edit** menu of your browser, or press `Control+V`, or right-click on the target field and select **Paste**.
-

Changing users for EM login on Linux

About this task

You can change the users allowed to log in to EM after Avaya MS is installed. Authenticated EM users must meet the following criteria:

- Users must successfully authenticate against SSH (Secure Shell).
- Users must be members of the groups specified in the Apache-Tomcat local-login configuration.

Change the Apache-Tomcat configuration for authenticated groups and users using this procedure.

Procedure

1. Using a Linux shell on Avaya MS, change to the Apache-Tomcat configuration directory by entering the following command:
`cd $MASHOME/../../apache-tomcat/mas/conf`
 2. Edit the properties file by entering the following command:
`vi local-accounts.properties`
 3. Find the property:
`locallogin.authenticable.groups`
 4. If the Linux group that the new user is a member of is not listed in the value field, add the user group, separating multiple entries with semicolons.
For example, `locallogin.authenticable.groups=root;admins`
 5. Configure users using the `locallogin.authenticable.users` property.
You can configure specific users in a semicolon separated list or use the wildcard asterisk (*) to allow all users of the `locallogin.authenticable.groups` to log in.
For example, `locallogin.authenticable.users=*`
 6. Save changes.
 7. Close all Web browsers.
 8. Restart the Avaya EM Service by entering the following command:
`/sbin/service avaya.em restart`
-

Chapter 4: Configuration

Configuration overview

This chapter includes license activation, defining translations, setting protocol preferences, configuring server clusters and setting up high availability configurations.

Before you use the configuration procedures, ensure you have installed Avaya Media Server (MS) using either the Quick Setup procedure or the installation procedures mentioned in *Installing, Patching and Upgrading Avaya MS 7.5*.

Cluster configuration

A cluster is a collection of Avaya MS that work together and can be viewed as one node capable of providing service at an increased capacity and with redundancy. All the nodes in a cluster must be running the same application set.

The Avaya MS cluster must consist of a Primary and Secondary server. You can optionally add other servers, known as Standard servers.

Perform the following procedures to first configure the Primary, Secondary, and optional Standard servers and then to bind the servers in a cluster.

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

An Avaya MS cluster must use a Simple Network Time Protocol (SNTP) server for clock synchronization. For details, see the Setting the SNTP source server section.

Limitations:

- The maximum number of servers in a cluster is eight.
- Clustering and High Availability are two different configuration options that cannot be combined.
- A cluster must not span geographical locations. Cluster members must be on the same local network.

Related topics:

[Setting the SNTP source server](#) on page 66

Configuring a Primary server for a cluster

About this task

Perform the following procedure to use Element Manager (EM) to configure the role of an Avaya MS to be the Primary server in a media server cluster:

Procedure

1. Gain access to the server on EM that you want to designate as Primary and navigate to **EM > Cluster Configuration > Server Designation**.

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: server3496.richlab.avaya.com
 Address: 135.60.77.148
 UUID: ac9905a0-80c5-11e0-8aa8-000d60d49a6c
 Role: Primary

Server Designation

☐ Server Address	Server UUID	Role

Replication Account

Enable Replication Account: ☒

Username: amsuser (8-16 characters)
 Password: (6-32 characters)

2. In the **Local Server** section, ensure the **Role** is set to **Primary** using the drop-down menu.

3. Note the Primary node IP address and the UUID.
You will need these later to configure the other nodes in the cluster.
4. In the **Replication Account** section, ensure **Enable Replication Account** is selected.
5. In the **Username** and **Password** fields, enter a user name and password.

 Note:

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

6. Click **Save**.
 7. Click **Confirm** to accept the changes.
-

Configuring a Secondary server for a cluster

Before you begin

- Configure a separate Avaya MS with the Role of Primary and with an enabled Replication Account.
- Obtain the UUID and the IP address of the Primary server.
- Obtain the user name and the password of the Replication Account.

About this task

Perform the following procedure to use EM to configure the role of an Avaya MS to be a Secondary server in a media server cluster:

Procedure

1. Gain access to the server on EM that you want to designate as Secondary and navigate to **EM > Cluster Configuration > Server Designation**.

2. In the **Local Server** section, set the **Role** to **Secondary** using the drop-down menu.
The system updates the page with fields specific to the Secondary node configuration.
3. From the Primary servers EM, copy the Primary servers UUID.
For more information on copying the UUID, see Obtaining the UUID of a media server.
4. Using EM for the Secondary server, paste the UUID of the Primary server in the **Primary Server UUID** field.
5. In the **Primary Server Address** field, enter the IP address of the Primary server.
6. In the **Replication Account** section, ensure **Enable Replication Account** is selected.
7. In the **Username** and **Password** fields, enter the user name and password for the Replication Account on the Primary server.

*** Note:**

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

8. Click **Save**.
9. Click **Confirm** to accept the changes.

Related topics:

[Obtaining the UUID of a media server](#) on page 36

Configuring a Standard server for a cluster

Before you begin

- Configure a separate Avaya MS with the Role of Primary and with an enabled Replication Account.
- Obtain the UUID and the IP address of the Primary server.
- Obtain the user name and the password of the Replication Account.

About this task

Perform the following procedure to use EM to configure the role of an Avaya MS to be a Standard server in a media server cluster:

Add Standard nodes after you have added Secondary nodes to the cluster.

Procedure

1. Gain access to the server on EM to designate as Standard and navigate to **EM > Cluster Configuration > Server Designation**.

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: server4837
 Address: 135.60.77.155
 UUID: 835c8aa4-6d0b-11e0-491c-001f296958ea
 Role: Standard

Server Designation

Primary Server UUID: 1e0-958e-001f296491ca
 Primary Server Address: 135.60.77.153

Replication Account

Enable Replication Account: ☒
 Username: amsuser (8-16 characters)
 Password: •••••••• (6-32 characters)

Save Cancel

2. In the **Local Server** section, set the **Role** to **Standard** using the drop-down menu.
 The system updates the page with fields specific to Standard node configuration.
3. From the Primary servers EM, copy the Primary servers UUID.

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

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

 Note:

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

8. Click **Save**.
9. Click **Confirm** to accept the changes.
Repeat Step 1 to Step 9 for each additional Standard server that you add to the cluster.

Related topics:

[Obtaining the UUID of a media server](#) on page 36

Configuring the replication settings for a cluster

About this task

Perform the following procedure to use EM to configure the replication preferences in a media server cluster:

Procedure

1. Gain access to EM for the Primary server in your cluster and navigate to **EM > Cluster Configuration > Replication Settings**.
2. Select **Configuration Replication**.
The selection of **Configuration Replication** ensures that any changes to settings on the Primary server are replicated automatically to all the other nodes in the cluster. When you enable **Configuration Replication**, many configuration changes can only be performed from the EM of the Primary server, providing one central place for making changes.
3. (Optional) Select any other items that you would like to replicate across all nodes in the cluster.

4. Click **Save**.
 5. Restart the system for the changes to take effect.
-

Configuring replication of Content Store data between clusters

Before you begin

- Configure an Avaya MS cluster to function as the master cluster.
- Configure an Avaya MS cluster to function as the replica cluster.
- Obtain the IP address of the Primary server in the master cluster.
- Obtain the username and password for the Replication Account of the Primary server in the master cluster.

About this task

Content Store replication is a one-way data copy from a master cluster to a replica cluster. The master cluster can have up to four directly-connected replica clusters. You can create chains of replica clusters, thereby creating hierarchies that scale to greater than four replica clusters in the network. In these cascading hierarchies, intermediate replica clusters act as master clusters for replica clusters further down the hierarchy.

No changes are required on the master cluster to enable replication. Replica clusters connect to the master cluster using the Replication Account for authentication.

Content Store replication between clusters provides the following capabilities:

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

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

Procedure

1. Gain access to EM for the Primary server in the replica cluster and navigate to **EM > Cluster Configuration > Replication Settings**.
2. Enter the address of the Primary server of the master cluster in the **Master Cluster Primary Node Address** field.
3. Click **Save**.

The system activates replication immediately. All of the content data on the master cluster is copied to the replica cluster.

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

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

Disabling replication of Content Store data between clusters

About this task

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

Procedure

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

The system disables replication immediately.

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

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

Configuring SIP load balancing for a cluster

About this task

Perform the following procedure to use EM to enable algorithms that balance the load of sessions across all the servers in a cluster:

Procedure

1. Gain access to EM of the Primary server and navigate to **EM > Cluster Configuration > Load Balancing**.

2. Configure **Application Key For Load Reporting**, if required by your application.
3. Select **Cluster Load Balancing** to distribute the load evenly across cluster members or clear **Cluster Load Balancing** to disable load distribution across cluster members.
4. Select **Cluster Redirect In a Non Unlocked Operational State** to enable SIP 300 or 302 responses to redirect calls when in a non-unlocked state.
When you enable **Cluster Redirect In a Non Unlocked Operational State**, the system redirects calls if the node is in locked or pending-locked state.
5. Set **Minimum Delta In Sessions Before Redirecting** to choose the difference in the number of sessions between nodes before balancing the load of sessions across all the servers in a cluster.
6. Select **Restrict Redirection List To Single Entry** to limit the number of servers the system offers for redirection to one entry in a SIP 302 response, representing the least loaded server in the cluster.
Clear **Restrict Redirection List To Single Entry** to enable the system to provide a list of alternate servers in a SIP 300 response, listing the least loaded servers first.
7. Click **Save**.

Replication of configuration settings in a cluster

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

High Availability configuration

The High Availability configuration ensures uninterrupted availability of media processing when a media server fails. Use the High Availability configuration option when you require the service providing capacity of only a single Avaya MS.

The High Availability configuration deploys a single active Primary server with a Backup server waiting in synchronized hot standby. Both the servers have identical configuration and can provide full media processing service if one server fails. Only one server is active at a time while the other server waits in standby to take over instantly.

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

Perform the High Availability configuration procedures in the following sequence:

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

High Availability synchronization overview

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

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

Both the Backup and the Primary server can become active at the same time if the servers become network isolated from each other. When the servers reconnect they exchange state information. The system uses the state information to select which server becomes the active server and which server becomes the standby server. The system selects the server that was the last server to process a new session as the active server. If the system did not process a

new session then the server which was active the longest becomes active. In most cases, the server that was active for the longest period, is the server that was active before the network isolation occurred.

Restrictions and limitations of High Availability

The High Availability feature has the following restrictions and limitations:

- High Availability functionality is limited to specific applications. To determine if you can configure an application with High Availability, see adopting product documentation. Do not configure High Availability unless the adopting product documentation indicates it is supported.
- High Availability can be configured only in 1+1 configuration. Clustering and High Availability are two different configuration options that you cannot combine.
- High Availability is available only if the servers are installed on the Linux operating system.
- High Availability peer servers must be on the same subnetwork and the subnetwork must have Layer 2 network redundancy.
- Avaya recommends configuring High Availability servers with network interface bonding for increased performance and network interface redundancy.
- Both the Primary and the Backup Avaya MS must use a common Simple Network Time Protocol (SNTP) server for clock synchronization.
- After the Backup server is active, service falls back to the Primary server only when the Primary server is idle or the Backup server fails. To restore the Primary server to the active state immediately, manually set the Backup server status to **Failover**, from the **More Actions** drop-down list on **EM > Element Status**.

Configuring the Primary server for High Availability

Before you begin

Ensure that the system is configured with a license.

About this task

Perform the following procedure to configure the role of Avaya MS to be a Primary server in a High Availability pair:

Procedure

1. Gain access to EM for the Linux based Avaya MS to designate as Primary server and navigate to **EM > Cluster Configuration > Server Designation**.
2. In the **Local Server** section, set the **Role** to **Primary**.

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: server3496.richlab.avaya.com
Address: 135.60.77.148
UUID: ac9905a0-80c5-11e0-8aa8-000d60d49a6c
Role: Primary

Server Designation

☐	Server Address	Server UUID	Role
☐			
☐			

Replication Account

Enable Replication Account: ☒

Username: (8-16 characters)
Password: (6-32 characters)

- Note the Primary node IP address and the UUID.
You need these while configuring the Backup node.
- In the **Replication Account** section, ensure **Enable Replication Account** is selected.
- In the **Username** and **Password** fields, enter a user name and password.

! Important:

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

- Click **Save**.
- Click **Confirm** to accept the changes.

Configuring the Backup server for High Availability

Before you begin

- Configure a separate Avaya MS with the role of Primary and with an enabled Replication Account.
- Obtain the UUID and the IP address of the Primary server.
- Obtain the user name and the password of the Replication Account.
- Ensure that the Primary and Backup servers are on the same subnet.

About this task

Perform the following procedure to configure the role of Avaya MS to be a Backup server for a Primary Avaya MS:

Procedure

1. Gain access to EM for the Linux based Avaya MS to designate as Backup and navigate to **EM > Cluster Configuration > Server Designation**.

2. In the **Local Server** section, set the **Role** to **Backup** using the drop-down menu. The system updates the page with fields specific to Backup node configuration.
3. From the EM of the Primary server, copy the UUID of the Primary server. For more information on copying the UUID, see Obtaining the UUID of a Media Server.

4. In the EM of the Backup server, paste the Primary server UUID in the **Primary Server UUID** field.
5. In the **Primary Server Address** field, enter the IP address of the Primary server.
6. In the **Replication Account** section, ensure **Enable Replication Account** is selected.
7. In the **Username** and the **Password** fields, enter the user name and the password that you entered for the Replication Account on the Primary server.

 Important:

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

8. Click **Save**.
9. Click **Confirm** to accept the changes.

Related topics:

[Obtaining the UUID of a media server](#) on page 36

Completing High Availability cluster configuration

Before you begin

Configure Primary and Backup servers.

About this task

Perform the following procedure to complete the High Availability server pairing:

Procedure

1. Gain access to EM for the designated Primary server and navigate to **EM > Cluster Configuration > Server Designation**.
2. Confirm the following:
 - **Local Server Role** is set to **Primary**.
 - One server is shown in the **Server Designation** section and the server has the **Role** of **Backup**.
 - **Enable Replication Account** is selected.
3. If the Backup server is not listed in the **Server Designation** section, then perform the following steps to add the Backup server:
 - a. Click **Add**.
 - b. Enter the address of the Backup server in the **Server Address** field.

- c. Enter the UUID of the Backup server in the **Server UUID** field.
 - d. Select **Backup** for the Role.
 - e. Click **Save**.
-

Enabling High Availability

Before you begin

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

About this task

After configuring the primary and the backup servers, assign a floating IP address to the pair and enable the High Availability feature on both servers. With the floating IP address, the backup server automatically starts processing calls after a failover.

Perform the following procedure to configure the floating IP address on both the Primary and the Backup servers and to activate High Availability:

Procedure

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

3. Enter the floating service IP address in the **Service IP Address** field.
4. Enter the subnet mask for the floating IP address in the **Service IP Address Mask** field.
5. Clear **Local High Availability State Lock**, if selected.
6. (Optional) In the **Failure Notification List** area, click **Add** to add the address of the server in the adopting product which is to be notified when a failover occurs.
See the documentation of the adopting product for information regarding which address to provide.
7. Click **Save**.
8. Click **Confirm**.
Perform Step 1 to Step 8 using the same values for both the Primary and the Backup servers.

Reviewing High Availability configuration and status

About this task

After the High Availability pair is formed, several EM pages display new features that reflect the new paired High Availability state.

Perform the following procedures to use the new features of High Availability and to ensure High Availability is in full service:

Procedure

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

Cluster Status

Select an element name to view the alarm viewer for that element.

[System Status](#) | [System Performance Summary](#)

System Status Refresh every: No Refresh ▼

Element Name	UUID	Element Role	Element Status ▼	Alarm Description
server3496.richlab	ac9905a0-80c5-11e0-8aa8-000d60d49a6c	Primary	Normal	No Alarm
server3497.richlab	e3cf0e20-80c5-11e0-8bdb-000d60d49748	Backup	Normal	No Alarm

System Performance Summary Refresh every: 15 seconds ▼

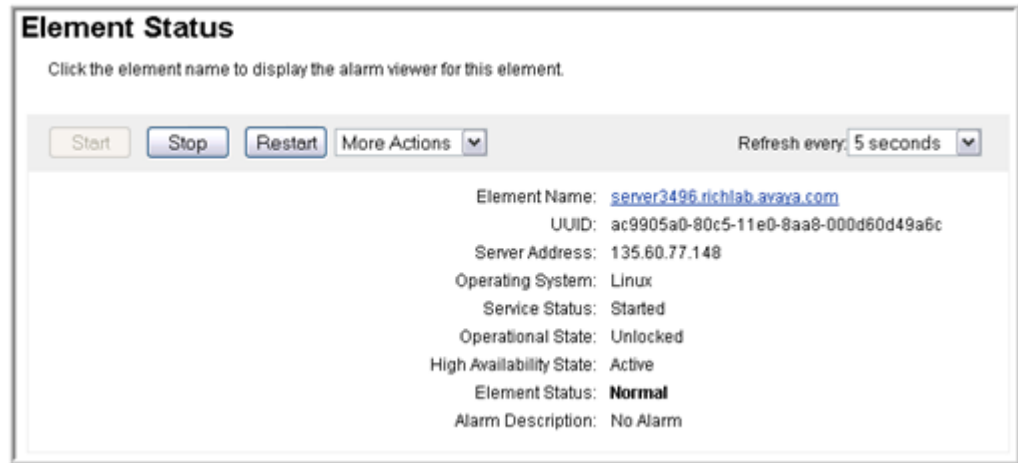
Name ▲	Value (Aggregate)
Active Sessions	0
SIP Inbound Call Attempted	0
SIP Outbound Call Attempted	0

3. On EM, for the designated Primary server, navigate to **EM > System Status > Element Status**.

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

High Availability State must be **Active**.

Ensure no alarms or service impacting states exist.

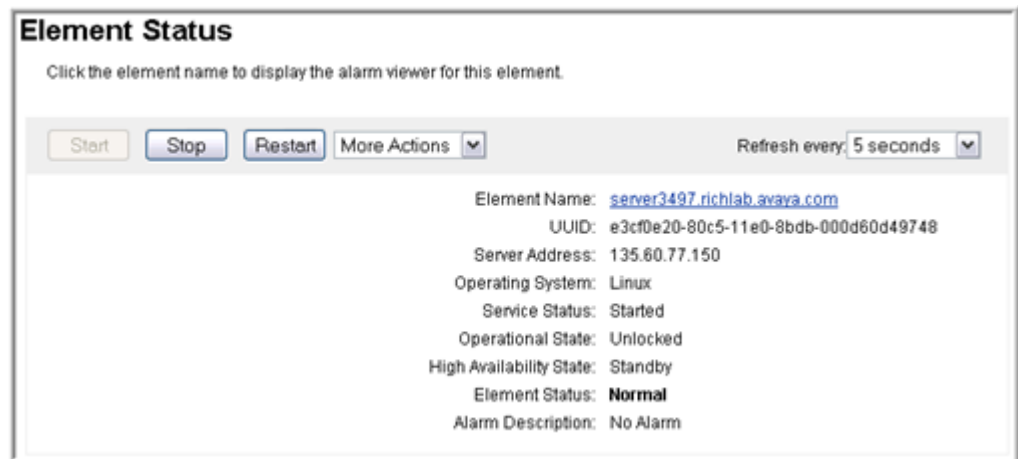


4. Gain access to EM for the designated Backup server and navigate to **EM > System Status > Element Status**.

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

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

Ensure no alarms or service impacting states exist.



Changing the Service IP Address for a High Availability configuration

Before you begin

Stop both High Availability Avaya MS peers before changing the Service IP Address. For details, see Starting and stopping the media server.

About this task

Perform the following procedure to update the Service IP Address for a High Availability pair of servers:

Procedure

1. Navigate to **EM > Cluster Configuration > High Availability** and update the **Service IP Address**.
2. Click **Save**.
3. Click **Confirm**.
Repeat Step 1 and Step 3 for the peer server.
4. Start Avaya MS by navigating to **EM > System Status > Element Status**.
5. Click **Start**.
6. Click **Confirm**.
7. Unlock Avaya MS if the **Operational State** is **Lock** or **Pending Lock** by navigating to **EM > System Status > Element Status**.
8. Select **Unlock** from the **More Actions** drop-down menu.
9. Click **Confirm**.
Repeat Step 4 and Step 9 for the peer server.

Related topics:

[Starting and stopping the media server](#) on page 28

Replication of configuration settings in a High Availability configuration

After you have configured the High Availability pair, the system disables most configurable settings in EM as unavailable for the server with the Role of Backup.

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

License configuration

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

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

License type	Description
License Server	License Servers are used for both cluster and standalone server configurations. A single license is shared by all nodes in a cluster.
Nodal Licensing	A Nodal License is bound to a particular Avaya MS server and is not shared across Avaya MS nodes. In this node-locked configuration, you must configure each Avaya MS node with its own license key.
WebLM Server	WebLM Servers use the Avaya WebLM Web-based licensing management system.

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

Configuring License Server keys

About this task

License Servers provide licensing for both cluster and standalone server configurations. In a cluster, the License Servers reside only on the Primary and Secondary servers in the cluster.

If you have a License Server key, then perform the following procedures to use the key and configure the License Server:

Procedure

1. Gain access to EM of the Primary server and navigate to **EM > Licensing > General Settings**.
2. From the **Licensing** drop-down menu, select **License Server**.

General Settings

Licensing: License Server

Add License Keys :

```
j1F8mgHQpLnhTwhLy6m+ereOPfGXCOViHYB
AIDD8Ojk4uNjFHVp5eFgwrCLkzmPygpLe2N
rbG1tLQ0M= # inst::auth 1.0
00:0c:29:49:6e:d8 (10) 360 secs
Mon Jun 18 01:00:00 2012
```

Display Licenses

License Details

Feature	Release	MAC Address	Available	Expiration Date(CTD)
Media Server Instances	1.0	0:c:29:49:6e:d8	10	2012-06-17 19:00:00
Media Server Audio Sessions	1.0	0:c:29:49:6e:d8	10	2012-06-17 19:00:00

Save Cancel Restore Defaults

3. Apply the license key:
 - If you are licensing a cluster configuration, copy and paste all the license keys in the **Add License Keys** or the **Replace License Keys** field.
 - If you are licensing a standalone server, copy and paste the single license key in the **Add License Keys** or the **Replace License Keys** field.
4. Click **Display Licenses** to ensure the license keys are valid and to see the features included with the license keys.
The features are listed in the **License Details** section.
5. Click **Save**.
The system displays a confirmation page.
6. Click **Confirm**.
7. If you are licensing a cluster configuration, restart the License Server on the Secondary, Backup, and Standard nodes:
 - a. Navigate to **EM > Licensing > License Server Status**.
 - b. Click **Restart**.
The system displays a confirmation page.
 - c. Click **Confirm**.

Configuring License Server chunk size

About this task

Avaya MS platform allocates licenses in chunks to minimize session setup delays, which is especially important during peak traffic times. A license chunk is released to the cluster when the platform detects that the cluster is idle for a specific period of time.

First determine the chunk size required for your system. To ensure peak performance of the platform, you must change the license chunk size based on the number of nodes in the cluster and the expected capacity for each node. You must purchase sufficient licenses so that the licenses can be evenly distributed based on the license chunk size. For example, suppose you have a cluster with three active nodes, each with a peak capacity of 200 sessions, and a recommended chunk size of 100. Each node requires two chunks ($200 / 100 = 2$) for peak capacity and the cluster must have at least 600 licenses ($3 \times (2 \times 100) = 600$).

The following table provides recommended chunk size based on expected node peak capacity:

License chunk sizing recommendations	
Node peak capacity	Recommended chunk size
200 or greater	100
51-100	25
31-50	10
30 or fewer	2

Procedure

1. Gain access to EM of the Primary server and navigate to **EM > System Configuration > Engineering Parameters > License**.
 2. Enter the recommended chunk size in the **License Provider PLIC Minimum Chunk** field.
Retain the default values for the other license properties.
 3. Click **Save**.
 4. To confirm your license configuration, verify there are no active licensing alarms raised on **EM > System Status > Alarms**.
 5. To check the License Server status, navigate to **EM > Licensing > Server Status**.
-

Updating License Server keys

About this task

If you have a new License Server key, then perform the following procedure to update an existing key:

Procedure

1. Gain access to EM of the Primary server and navigate to **EM > Licensing > General Settings**.
2. Remove all old license keys by clicking in the **Replace License Keys** field and pressing **Control+A** to select all the text.
Alternatively, select only the individual license key to replace.
3. Press the **Delete** or **Backspace** key.
4. Copy and paste the new license keys in the **Replace License Keys** field.
5. Click **Display Licenses** to ensure that the license keys are valid and see the features included with the license keys.
The features are listed in the **License Details** section.
6. Click **Save**.
The system displays a confirmation page.
7. Click **Confirm**.
8. If you are licensing a cluster configuration, restart the License Server on the Secondary, Backup, and Standard nodes:
 - a. Navigate to **EM > Licensing > License Server Status**.
 - b. Click **Restart**.
The system displays a confirmation page.
 - c. Click **Confirm**.

Configuring Nodal Licensing

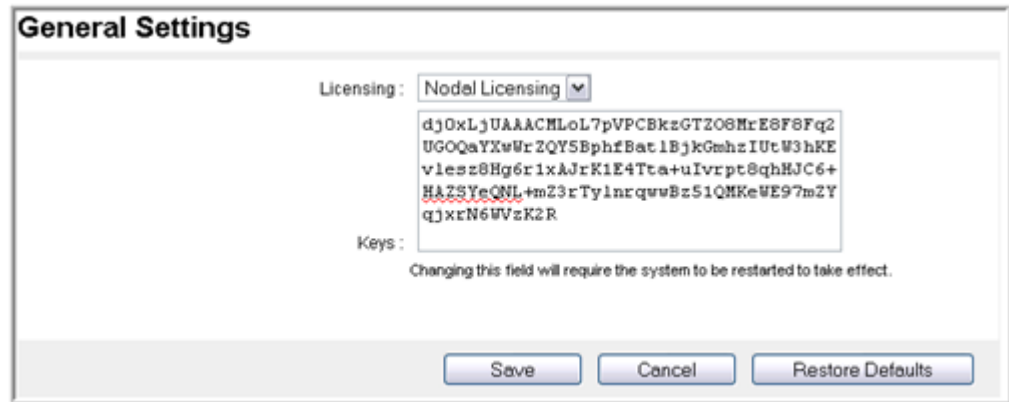
About this task

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

Perform the following procedure to configure a nodal license:

Procedure

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



3. Apply the license key generated specifically for this server by copying and pasting the license key into the **Keys** field.
4. Click **Save**.
The system displays a confirmation page.
5. Click **Confirm**.
6. Restart Avaya MS for the new license to be effective.
7. To confirm your license configuration, verify that there are no active licensing alarms raised on **EM > System Status > Alarms**.
Repeat Step 1 to Step 6 for each media server in the cluster.

Updating Nodal Licensing keys

About this task

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

Procedure

1. Gain access to EM for each of your servers and click **EM > Licensing > General Settings**.
2. Remove the old license key by clicking **Keys** field and then pressing **Control+A** to select the old key.
3. Press the **Delete** or the **Backspace** key.

4. Copy and paste the new license keys into the **Keys** field.
 5. Click **Save**.
The system displays a confirmation window.
 6. Click **Confirm**.
 7. Restart Avaya MS to apply the new license.
 8. To confirm your license configuration, verify that there are no active licensing alarms raised on **EM > System Status > Alarms**.
Repeat Step 1 to Step 8 for each media server in the cluster.
-

Configuring WebLM Server licensing

Before you begin

Install Avaya WebLM server.

About this task

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

Each Avaya MS is configured with the URL of the WebLM server, in order to acquire licenses from the WebLM server.

For more information, see *Installing and Configuring Avaya WebLM Server* which is available at <http://www.avaya.com/support>.

Procedure

1. Gain access to EM for each of your servers and navigate to **EM > Licensing > General Settings**.
2. From the **Licensing** menu, select **WebLM Server**.

General Settings

Licensing: WebLM Server

Server Host Name or IP Address: 135.60.86.220

Server Port: 52233

URL Suffix: /WebLM/LicenseServer Open WebLM Server

License Details

Feature	Maximum Number	Minimum Number
Call Progress Detection	1	0
Media Server Instances	1	0
Media Server Text-To-Speech Sessions	1	0
Media Server Speech Recognition Sessions	1	0
Media Server Audio Sessions	1	0
Media Server Video Sessions	1	0

Save Cancel Restore Defaults

3. Enter the address of the WebLM server you plan to use in the **Server Host Name or IP Address** field.
4. Enter the port to use with the WebLM server in the **Server Port** field.
The WebLM server processes license requests from the port you configure in the **Server Port** field. The default port is 53322.
5. Enter the **URL Suffix** used to identify the WebLM server.
The default **URL Suffix** is /WebLM/LicenseServer.
6. In the **License Details** area, set the **Maximum Number** and **Minimum Number** based on the number of sessions the cluster supports.
7. Click **Save**.
The system displays a confirmation page.
8. Click **Confirm**.
9. Restart Avaya MS to apply the new license.
10. To confirm your license configuration, verify that there are no active Licensing alarms raised on **EM > System Status > Alarms**.
11. After you configure the WebLM licensing properties, use the **Open WebLM Server** button on the **General Settings** page to gain access to the WebLM server.
Repeat Step 1 to Step 10 for each media server in the cluster.

License utilization alarm threshold configuration

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

Setting license server alarm thresholds

About this task

Perform the following procedure when you have selected the **License Server** option:

License utilization threshold alarms and license exhausted alarms generated by the License Server can be either enabled or disabled. The alarms are enabled by default.

Procedure

1. Navigate to **EM > Licensing > Utilization Threshold**.
 2. Select **Enable License Exhausted Alarms** to generate alarms when a license is 100 percent utilized.
 3. Select **Enable License Utilization Threshold Alarms** to generate alarms when license utilization exceeds the percentage specified in **License Utilization Threshold**.
 4. In the **License Utilization Threshold** field, enter the threshold percentage.
You can only modify **License Utilization Threshold** field when license utilization threshold alarms are enabled.
 5. Click **Save**.
-

Setting nodal licensing alarm thresholds

About this task

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

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

Procedure

1. Navigate to **EM > Licensing > Utilization Threshold**.
2. In the **Nodal License Utilization Threshold** field, enter the threshold percentage for the alarm.

3. Click **Save**.
-

Modifying predefined server profiles

About this task

Perform the following procedure to view and modify predefined server profiles:

Enabling or disabling features in a server profile allows you to control optional functionality on the media server. Avaya MS Release 7.5 supports only the **Default** profile.

Procedure

1. Navigate to **EM > System Configuration > Server Profile**.
 2. Ensure that the **Server Profile** drop-down menu is set to **Default**.
 3. Using the check boxes, select the required functionality.
 4. Click **Save**.
Restart the system for the changes to take effect.
-

Network settings configuration

Setting the SNTP source server

About this task

All the Avaya MS clusters and the High Availability pairs must use a common Simple Network Time Protocol (SNTP) source to ensure the time across the nodes is synchronized. You might encounter problems if you do not have synchronized time.

Perform the following procedure to configure the SNTP source for each Avaya MS:

Procedure

1. Navigate to **EM > System Configuration > Network Settings > General Settings > General**.
2. In the **SNTP Source Server** field, enter the IP address or host name of your SNTP server.

Enter `localhost` if you want to designate this server as the time source.

3. Click **Save**.
-

Enabling SNMP traps

About this task

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

Avaya MS reports the SNMP traps to the management system when a corresponding event triggers. For example, Avaya MS reports an SNMP trap when an alarm is raised. By default, the SNMP service is disabled on Avaya MS.

Perform the following procedure to enable and configure SNMP reporting:

Procedure

1. Navigate to **EM > System Configuration > Network Settings > General Settings > SNMP Traps**.
 2. Select **Delivery of Alarms via Traps** and **Delivery of Logs Via Traps** to enable respective reporting of alarms and events to a management system.
After one of the delivery options is selected, the **SNMP Network Manager Address** becomes configurable.
 3. Enter the address and the port number of the SNMP server that receives the reports.
The format of the address and port number must be address:port. The default port number is 162.
 4. Specify the community string shared with the SNMP management server in the **Community String** field.
The SNMP management server rejects reports that do not match the expected community string.
 5. Click **Save**.
 6. Restart the system.
-

Configuring the Avaya MS SNMP agent

About this task

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

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

Perform the following procedure to configure Avaya MS SNMP Agent:

Procedure

1. Navigate to **EM > System Configuration > Network Settings > General Settings > SNMP Agent**.
 2. Specify the community string shared with the SNMP management server in the **Community String** field.
Avaya MS SNMP Agent rejects queries that do not match the expected community string.
 3. Specify the SNMP Agent **Port Number**.
The default port is 161.
 4. Click **Save**.
 5. Restart the system.
-

Configuring SOAP

About this task

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

Perform the following procedure to configure Avaya MS SOAP attributes:

Procedure

1. Navigate to **EM > System Configuration > Network Settings > General Settings > SOAP**.
2. (Optional) Set the **Server Private Key**.
If you use this key, ensure the key matches on the client as well as the server side of the SOAP interface.

3. Select **Enable Trusted SOAP Nodes** if you want to restrict the SOAP connections to Avaya MS.
 4. In the **Trusted Nodes** field, enter the addresses of the nodes that can gain access to the SOAP services offered by Avaya MS.
Separate multiple addresses with semicolons.
The **Trusted Nodes** field needs to be populated only if **Enable Trusted SOAP Nodes** is selected.
 5. (Optional) Configure **Enable HTTP Digest Authentication**.
If you choose to enable HTTP Digest Authentication, configure the following:
 - HTTP Digest Authentication Domain
 - HTTP Digest Authentication User Name
 - HTTP Digest Authentication Password
 6. Select **Enable SOAP TLS Transport** to use TLS for SOAP connections to Avaya MS.

 **Important:**
If you enable SOAP TLS, you must configure a SIP TLS service profile and a certificate for the SIP TLS service profile.
 7. Click **Save**.
 8. Restart the system.
-

Configuring connection security options

About this task

Perform the following procedure to configure connection security options:

Procedure

1. Navigate to **EM > System Configuration > Network Settings > General Settings > Connection Security**.
2. Select or clear the **Connection Security** settings as required for your network.

General Settings

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

[General](#) | [SNMP Traps](#) | [SNMP Agent](#) | [SOAP](#) | [Connection Security](#)

Connection Security

Verify Host Name: ☒

Enable TCP TLS Transport: ☐

Enable OCSP: ☐

OCSP Response Timeout (ms): (100 - 3000)

OCSP Permit if no Response: ☒

Enable OCSP Synchronous Mode: ☐

TCP TLS Enable Cipher AES 128 SHA: ☒

TCP TLS Enable Cipher AES 256 SHA: ☒

TCP TLS Enable Cipher DES CBC3 SHA: ☒

TCP TLS Enable Cipher NULL SHA: ☐

TCP TLS Session Renegotiation Enable: ☒

TCP TLS Session Renegotiation Timer (min): (0 - 1440)

3. Click **Save**.
4. Restart the system.

Configuring transmit prioritization

About this task

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

Note:

Before following the procedure, if you observe the Transmit Prioritization Configuration Error alarm consult with Avaya support engineers.

Procedure

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

Selecting IP interface assignments

Before you begin

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

About this task

Avaya MS uses the IP interface assignments to function as follows:

When **Transport** is set to **IPv4 Only**:

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

When **Transport** is set to **Dual IPv4/IPv6**:

- Avaya MS generates an SDP offer containing both IPv4 and IPv6 using ANAT. The ordering of IPv4/IPv6 is determined by using the **Preferences for Local Offers** as follows:
 - If **Preferences for Local Offers** is set to **IPv4 Preferred**, then the SDP contains ANAT with both IPv4/IPv6 and with IPv4 first in the ANAT group.
 - If **Preferences for Local Offers** is set to **IPv6 Preferred**, then the SDP contains ANAT with both IPv4/IPv6 and with IPv6 first in the ANAT group.
- Avaya MS generates SDP answer using the **Preferences for Remote Offers** as follows:
 - If **Preferences for Remote Offers** is set to the default of **Use Remote Preference**, then the selection of IPv4 or IPv6 is based on the received SDP preference:
 - For incoming IPv4 only SDP, IPv4 only SDP is used.
 - For incoming ANAT SDP with IP4 then IPv6 order, IPv4 is used in the ANAT response.
 - For incoming ANAT SDP with IPv6 then IPv4 order, IPv6 is used in the ANAT response.
 - If **Preferences for Remote Offers** is set to **IPv4 Preferred**, the system overwrites the remote preference and sets IPv4 is in the offer.
 - For incoming IPv4 only SDP, IPv4 only SDP is used.
 - For incoming ANAT SDP with IP4 then IPv6 order, IPv4 is used in the ANAT response.
 - For incoming ANAT SDP with IPv6 then IPv4 order, IPv4 is used in the ANAT response.
 - If **Preferences for Remote Offers** is set to **IPv6 Preferred**, the system overwrites the remote preference and sets IPv6 is in the offer.
 - For incoming IPv4 only SDP, IPv4 only SDP is used.
 - For incoming ANAT SDP with IP4 then IPv6 order, IPv6 is used in the ANAT response.
 - For incoming ANAT SDP with IPv6 then IPv4 order, IPv6 is used in the ANAT response.

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

Procedure

1. Navigate to **EM > System Configuration > Network Settings > IP Interface Assignments**.
2. Under **IPv4 Interfaces**, select the desired IPv4 address for each interface: **Signaling, Media, Cluster** and **OAM**.
3. If IPv6 is enabled for your system, then configure the following:
 - a. In the **IP Configuration** section, select the **Transport mode** as either **Dual IPv4/IPv6** or **IPv4 Only**.

- b. In the **IP Configuration** section, select **Preferences for Remote Offers**.
 - c. In the **IP Configuration** section, select **Preferences for Local Offers**.
 - d. In the **IPv6 Interfaces** section, select the desired IPv6 address for the **Media** interface.
4. Click **Save**.
-

Computer name and IP address modification

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

 Note:

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

Related topics:

[Security configuration](#) on page 118

Changing the computer name on Linux

Before you begin

Stop Avaya MS before changing the computer name. For details, see Starting and stopping the media server.

About this task

Perform the following procedure if you need to change the host name of a Red Hat 5.x Linux based Avaya MS:

Procedure

1. Edit the file `/etc/hosts`.
2. Update the host name wherever the host name appears in the file.
3. Save the file.
4. Edit the file `/etc/sysconfig/network`.
5. Update the host name wherever the host name appears in the file.
6. Save the file.

7. Using a Linux shell, enter the following command to apply the host name change to the system:

```
hostname <new_hostname>
```

Where <new_hostname> is the new name for the server.

Related topics:

[Starting and stopping the media server](#) on page 28

Changing the computer name on Windows

Before you begin

Stop Avaya MS before changing the computer name. For details, see [Starting and stopping the media server](#).

About this task

Perform the following procedure if you need to change the name of a Windows 2008 based Avaya MS:

Procedure

1. Click the Windows **Start** button.
2. Right-click **Computer**, and select **Properties** on the shortcut menu.
3. Click **Advanced system settings**.
4. In the System Properties window, click the **Computer Name** tab.
5. Click **Change**.
6. In the **Computer name** field, type the new computer name.
7. Click **OK**.
The system displays a message box warning you to restart the computer to apply the change.
8. Click **OK**.
9. In the System Properties window, click **Close**.
The system displays a message box warning you to restart the computer to apply the change.
10. Click **Restart Now**.

Related topics:

[Starting and stopping the media server](#) on page 28

Changing the IP address on Linux

Before you begin

Stop Avaya MS before changing the IP address. For more information, see Starting and stopping the media server.

About this task

To change the IP address of a Red Hat 5.x Linux based Avaya MS, perform the following procedure:

Procedure

1. Edit the file `/etc/hosts`.
2. Update the IP address wherever the IP address appears in the file.
3. Save the file.
4. Edit the file `/etc/sysconfig/network-scripts/ifcfg-eth0`.
5. Update the IP address wherever the IP address appears in the file.
6. Save the file.
7. Using the local Linux console shell, enter the following commands to apply the IP address change to the system:

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

```
/etc/init.d/network start
```
8. Login to EM using the new IP address in the URL for the EM login.
9. Navigate to **EM > System Configuration > Network Settings > IP Interface Assignment**.
10. **IP Interface Assignment** fields show errors, as a result of the IP address change. Select valid IP addresses from the drop-down menus for each field showing **Invalid**.
11. Click **Save**.
12. Click **Confirm**.
13. If this server is a member of a cluster or High Availability pair, then navigate to **EM > Cluster Configuration > Server Designation** on each server and ensure the IP address you just changed is updated on each server. For more information, see Cluster configuration.
To change the High Availability Service IP address, see Changing the Service IP Address for a High Availability configuration.

Related topics:

[Starting and stopping the media server](#) on page 28

[Cluster configuration](#) on page 39

[Changing the Service IP Address for a High Availability configuration](#) on page 56

Changing the IP address on Windows

Before you begin

Stop Avaya MS before changing the IP address. For more information, see [Starting and stopping the media server](#).

About this task

To change the IP address of a Windows 2008 based Avaya MS, perform the following procedure:

Procedure

1. Click the Windows **Start** button.
2. Click **Control Panel**.
3. Click **Network and Internet**.
4. Click **Network and Sharing Center**.
5. Click **Local Area Connection**.
6. Click **Properties**, on the **General** tab of the Local Area Connection Status window.
The system displays the Local Area Connection Properties window.
7. Under **This connection uses the following items**, select **Internet Protocol Version 4 (TCP/IPv4)**.
8. Click **Properties**.
The system displays the Internet Protocol Version 4 (TCP/IPv4) Properties window.
9. On the **General tab**, select **Use the following IP address**.
10. In the **IP address** field, type the IP address that you want to use.
11. (Optional) Update the **Subnet mask**, **Default gateway**, **Preferred DNS server**, and **Alternate DNS server**.
12. Click **OK**.
13. Click **Close**.
The IP address is immediately changed.
14. Click **Close**.

15. Navigate to **EM > System Configuration > Network Settings > IP Interface Assignment**.

 Note:

If you are using a remote browser to gain access to EM, use the new IP address in the URL for the EM login.

16. **IP Interface Assignment** fields show errors, as a result of the IP address change. Select valid IP addresses from the drop-down menus for the each field showing **Invalid**.
17. Click **Save**.
18. Click **Confirm**.

Related topics:

[Starting and stopping the media server](#) on page 28

[Cluster configuration](#) on page 39

SIP configuration

The Session Initiation Protocol (SIP) is a signaling protocol used to create, modify and end text messaging and voice and video sessions consisting of one or more media streams.

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

Configuring SIP general settings

About this task

 Important:

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

If you enable SOAP (TLS), you must configure a SIP TLS profile and a certificate for the SIP TLS service profile.

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

Definitions for SIP settings	
Setting	Description
Always Approve SIP TLS Certificate	Select if you want the system to accept remote certificate over SIP TLS. The default is disabled.
Always Use SIP Default Outbound Proxy	Select to enable the system to route SIP requests that do not match the domain proxy configuration, through the default outbound proxy, even if an IP address is specified in the host portion of the destination URI.
Answer Delay (rings)	The number of rings before an incoming SIP call is answered. You can configure the duration of a ring using the Ring Interval engineering parameter. A value of 0 indicates an immediate answer. The default value is 1 ring. The range is 0 to 10 rings.
Enable SIP TCP Transport	Select if you want the system to accept and request SIP over TCP.
Enable SIP TLS Mutual Authentication	Select to enable the mutual authentication option for SIP TLS.
Enable SIP TLS Transport	Select to allow the system to accept and request SIP over TLS. Ensure that a certificate has been configured for the SIP TLS service profile.
Enable SIP UDP Transport	Select to allow the system to accept and request SIP over UDP.
Enable SIP UPDATE method	Select to allow session participants to modify the characteristics of the multimedia session through re-INVITE messages or UPDATE messages. Re-INVITE and UPDATE messages initiate session changes, such as hold and retrieve, codec changes, and adding or dropping media.
Enforce SIP Route Configuration	Select if outgoing route configuration is required. By default, the system raises an alarm if route configuration is missing. If outgoing route configuration is not required, clear the check box.
Enforce SIP TLS in Secured Media Mode	Select to disable the non-TLS transport in secured media mode.
Enforce SIPS for Security Enforced Calls	Select to require sips: in the URI to negotiate to use SRTP for media transport. Clear to allow SRTP with both sip: and sips: URIs.

Definitions for SIP settings	
Setting	Description
Hide SIP User-Agent Header	Select to prevent the User-Agent header from being included in SIP messaging.
Long Call Audit Refresh Timer	The time period in seconds for sending a refresh request. The default is 600 seconds. The range is 90 to 3600 seconds.
Long Call Audit Type	Select the preferred Long Call Method to use: Disable Audit, INFO Ping, re-INVITE, or UPDATE.
Minimum Session Interval (RFC4028 Min-SE)	The minimum value for the session interval that the application can accept. RFC4028 recommends a Min-SE value of 90 seconds. The default is 90 seconds. The range is 90 to 3600 seconds.
Require SIPS for Best Effort Calls	Select to include capability negotiation (crypto) offers when sips: is used. Do not include capability negotiation (crypto) offers when sip: is used. Clear to include capability negotiation (crypto) for both sip: and sips: URIs.
Session Expires Value (RFC4028)	The number of seconds before a call times out if the call is not successfully refreshed. The default is 1800 seconds. The range is 90 to 3600 seconds.
Session On Hold Teardown Delay (sec)	The number of seconds a session can remain on hold before the system ends the session. A value of 0 indicates the system will not end a session on hold. The default is 3600 seconds. The range is 0 to 100000 seconds.
SIP Hold Before Refer	The call is placed on Hold prior to REFER.
SIP Response Code When System/ Application Locked	The SIP Response Code needed to restore service when the application is locked, out-of-service, or exceeds engineering limits. The default value is 480. The range is 400 to 699.
Trusted Node Access Only	Select to prevent traffic from nodes that are not trusted. If a default proxy is configured, the call is redirected with a 305 Use Proxy message. Otherwise, the call attempt is rejected with a 403 Forbidden message.
Use SIPS for Best Effort Calls	Select to use sips: in the URI for outgoing best-effort offers originated from the Avaya

Definitions for SIP settings	
Setting	Description
	MS. Clear to use sip: in the URI for outgoing best-effort offers.

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

Procedure

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

Note:

Some of the changes require system restart to take effect.

Adding SIP domains

About this task

A network provisioned SIP domain must be added only if:

- Avaya MS needs to send SIP Register to the network
- Avaya MS is connected to more than one SIP domain that are controlled by different proxies and calls can originate from Avaya MS.

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

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

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

Procedure

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

4. Click **Save**.
-

Adding SIP accounts

About this task

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

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

Procedure

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

Configuring SIP trusted nodes

About this task

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

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

Procedure

1. Navigate to **EM > System Configuration > Signaling Protocols > SIP > Nodes and Routes**.

2. In the Trusted Nodes area, click **Add..** to add a new SIP trusted node.
3. On the **Add SIP Trusted Node** page, enter the address of the SIP node in the **Host or Server Address** field.
4. Click **Save**.

Configuring SIP routes

Before you begin

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

About this task

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

You can configure up to 32 routes for each domain.

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

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

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

Definitions for SIP route settings	
Setting	Description
Enabled	Select to enable or disable a SIP route. Typically, routes are enabled. However, a route can be disabled to remove the route temporarily without reconfiguring the system.
Domain	The name of the domain to which you are adding the route. The SIP route is associated with the domain.
Trusted Node	The trusted nodes associated with the route.
Transport	Select the appropriate SIP transport (UDP, TCP, or TLS). When you select the transport type of TLS, ensure that a certificate is configured for the SIP TLS service profile.

Definitions for SIP route settings	
Setting	Description
Remote Port	The remote port from which the route accepts SIP requests. The default port is 5060.
Priority	The priority value for the route. The default value is 0. The range is from 0 to 65535 with the lowest value having the highest priority. The highest priority routes, which have lower values, are selected first.
Weight	Weight is used to select routes within the same priority level. The default value is 10. The range is 0 to 65535.
Proxy	Select to assign a proxy server role to the route. A SIP proxy server accepts Avaya MS requests and uses the SIP registrar server to obtain recipient addressing information.
Registrar	Select to assign a registrar server role to the route. A SIP registrar server is a database that contains the location of all user agents within a domain.
IM Proxy	If there are multiple proxy routes in the domain, route IMs to the route which is enabled.

Procedure

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

Important:

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

7. In the **Remote Port** field, enter the port number of the remote port.
8. In the **Priority** field, set the priority of the route by entering a value.

9. In the **Weight** field, set the weight of the route by entering a value.
 10. In the **Roles** area, select whether the route is associated with the **Proxy** server, the **Registrar** server, or both by selecting **Proxy** and **Registrar**.
 11. Select **IM Proxy** to route instant messages only to the route that is enabled if there are multiple proxy routes in the domain.
 12. Click **Save**.
 13. Restart the server for the SIP route additions to take effect.
-

Configuring SIP route properties

Before you begin

You must have configured a SIP route. You must define a SIP route before you can configure the route properties.

About this task

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

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

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

Perform the following procedure to change SIP route properties for a configured SIP route:

Procedure

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

Editing a SIP domain or a SIP account

About this task

Perform the following procedure to edit an existing SIP domain or SIP account:

Procedure

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

Changing the SIP account password

About this task

Perform the following procedure to change the password for the SIP account:

Procedure

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

Deleting a SIP domain or a SIP account

Before you begin

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

About this task

Perform the following procedure to delete an existing SIP domain or SIP account:

Procedure

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

Editing a SIP trusted node or a SIP route

About this task

Perform the following procedure to edit an existing SIP trusted node or SIP route:

Procedure

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

Deleting a SIP trusted node or a SIP route

Before you begin

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

About this task

Perform the following procedure to delete an existing SIP trusted node or SIP route:

Procedure

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

MRCP configuration

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

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

You can also add custom MRCP vendors to allow for additional speech resources, in addition to the built-in Nuance and Loquendo support included with the Avaya MS installation.

Note:

In Avaya MS Release 7.5, Loquendo is added as a supported built-in MRCP vendor. IBM is no longer a built-in MRCP vendor. You can add IBM as a custom MRCP vendor using the procedures defined in this section.

Configuring an MRCP general settings

About this task

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

Definitions for MRCP general properties	
Property	Description
Maximum MRCP Channels	The maximum number of MRCP channels or sessions for each node that can be allocated by the server. Avaya MS uses this value to determine the maximum MRCP channels available on an MRCP server. This value is also used to initialize the MRCP stack. The Maximum MRCP Channels field is not a keycoded value. The default value is 512. The range is 0 to 2000.
MRCP Resource Ping Interval	The number of seconds between successive test allocations of configured MRCP resources. This value is used by Avaya MS to monitor the status of the MRCP servers. A value of 0 disables test allocations. The default value is 300 seconds. The range is 0 to 31536000 seconds.
MRCP RTP Start Port	The local RTP start port to use for MRCP v1 RTP connections to speech servers. The default port is 16000 for Windows and 1030 for Linux. The range is 1024 to 64000.
Recognition Timeout	The maximum duration, in milliseconds, that a recognition session is active before Avaya MS ends the session and generates a resource fault. The default value is 600000 milliseconds. The range is 0 to 31536000 milliseconds.
Retry Limit	The number of retry attempts when a resource allocation fails. The system attempts to connect to the server with the smallest load first, followed by the server with the second smallest load, and then the server with the third smallest load. The default is 2 retry attempts. The range is 0 to 2.
MRCP Transaction Timeout	The maximum duration, in milliseconds, that an MRCP transaction can last before Avaya MS ends and generates a resource fault. The default value is 10000 milliseconds. The range is 0 to 31536000 milliseconds.

Perform the following procedure to change MRCP general settings:

Procedure

1. Navigate to **EM > System Configuration > Signaling Protocols > MRCP > General Settings**.
 2. In the **Maximum MRCP Channels** field, enter a value for the maximum number of MRCP channels that can be allocated.
 3. In the **Retry Limit** field, enter the number of allocation retries before an allocation attempt fails.
 4. In the **MRCP Resource Ping Interval** field, enter the number of seconds between successive test allocations of configured MRCP resources.
A value of 0 disables test allocations.
 5. In the **MRCP RTP Start Port** field, enter the local RTP port to use for MRCP connections to speech servers.
 6. In the **MRCP Transaction Timeout** field, enter the maximum duration, in milliseconds, that an MRCP transaction can last before Avaya MS ends and generates a resource fault.
 7. In the **Recognition Timeout** field, enter the maximum duration, in milliseconds, that a recognition session is active before Avaya MS ends and generates a resource fault.
 8. Click **Save**.
 9. Restart the system for the changes to take effect.
-

Adding an MRCP server

About this task

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

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

Definitions for MRCP server properties	
Property	Description
Add to Default Pool	Select the check box to add the server to the default pool. This check box is only available when adding an MRCP Server. If no default pool exists, the system creates one pool based on the server configuration. The default pool uses the following names: lvr.mrcpv1.default or extts.mrcpv1.default. However, if there are no default pools and the pool names

Definitions for MRCP server properties		
Property	Description	
	(lvr.mrcpv1.default and extts.mrcpv1.default) already exist, the operation fails. The Add to Default Pool operation can also fail, if the server and default pool attributes do not match.	
Codec	Select the appropriate audio codec (PCMU, G711 or L16). The default value is based on the settings of the selected vendor.	
Port	The port from which the server receives requests. The default port is based on the settings of the selected vendor. The range is 0 to 65535.	
Server address	The IP address of the MRCP server. The maximum length is 64 characters.	
Server description	A brief description of the server. The maximum length is 512 characters.	
Server Name	The name used to identify this MRCP server. The maximum length is 128 characters.	
State	The operational state:	
	Unlocked	The server is online and available for allocation. This is the default.
	Locked	The server is offline and unavailable for allocation.
Vendor	Select the appropriate MRCP vendor identifier such as Nuance, Loquendo or those added on the Custom MRCP vendors page. The default is Nuance.	

 Important:

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

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

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

Procedure

1. Navigate to **EM > System Configuration > Signaling Protocols > MRCP > Servers**.
2. On the **Servers** page, click **Add...**

3. On the **Add MRCP Server** page, from **General**, in the **Server Name** field, enter the name used to identify the MRCP server.
4. In the **Server description** field, enter a description of the server.
5. In the **Server address** field, enter the host name or server address of the MRCP server.

 Important:

You must enable the DNS on the network if the host name is used.

6. In the **Port** field, enter the port number of the MRCP server where it is listening for MRCP requests.
7. From the **Vendor** list, select the vendor.
8. From the **Codec** list, select the audio codec type.
9. From the **State** list, select the appropriate initial operational state, either **Locked** or **Unlocked**.
The default value is **Unlocked**.
10. If you want to add the server to the default pool, select **Add to Default Pool**.
11. Click **Save**.

Adding MRCP server resources

About this task

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

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

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

Definitions for MRCP server resource properties	
Property	Description
Type	Select the appropriate resource capabilities (LVR or TTS) supported by MRCP. The default value is based on the settings of the selected vendor.
URL Suffix	<p>The URL suffix used to identify the resource. This feature is enabled only when the Type is LVR or TTS.</p> <p>For Nuance:</p> <ul style="list-style-type: none"> • LVR —media/speechrecognizer. This is the default. • TTS — media/speechsynthesizer <p>For Loquendo:</p> <ul style="list-style-type: none"> • LVR — media/recognizer • TTS — media/synthesizer <p>The default value is based on the settings of the selected vendor.</p>
Vendor name	The name of the current vendor such as Nuance, Loquendo or those added on the Custom MRCP vendors page.
Weight	The weighted value of the server. This value is used for distributing server resources within the pool. The default value is 1. The range is 0 to 65535.

 Note:

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

Procedure

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

The URL suffix must match the configuration on the speech server.

8. In the **Weight** field, enter the server weight used to distribute server resources within a pool.
9. In the **Maximum Sessions** field, enter the maximum number of sessions for this server.
10. Add desired languages in one of two ways:
 - Make a selection from the **Languages** drop-down menu, where the system prompts **Select a Language**. Click **Add** to add the selected language to the list of supported languages.
 - Click **Add New**.

In the text field that the system displays, type your desired language.

11. Click **Continue**.
 12. On the **Edit MRCP Server** page, click **Save**.
-

Adding an MRCP pool

About this task

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

Important:

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

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

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

Definitions for MRCP pool properties	
Property	Description
Pool name	The name used to identify this pool. The name can be up to 128 characters. An MRCP server can be assigned to many different pools.
Pool description	A brief description of the pool. The description can be up to 512 characters.
Pool type	The type of pool (LVR or TTS).

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

Perform the following procedure to add an MRCP pool:

Procedure

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

10. To make the pool available, select **Available**.
 11. Click **Save**.
-

Adding a server to an MRCP pool

About this task

You can assign an MRCP server to multiple pools.

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

Procedure

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

Important:

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

6. Click **Save**.
-

Adding custom MRCP vendors

About this task

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

Important:

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

Procedure

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

2. On the **Custom Vendors** page, click **Add...**
3. In the **Vendor Name** field, enter the name of the new vendor.
4. Select the desired **Default Codec** from the list.
5. In the **Default Port** field, enter the default port number associated with the MRCP resource.
6. In the **Associated Caps** heading, click **Add...**

 Important:

Only one LVR and one TTS capability can be created for each vendor.

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

Editing custom MRCP vendors

About this task

Perform the following procedure to edit custom MRCP vendors:

 Important:

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

Procedure

1. Navigate to **EM > System Configuration > Signaling Protocols > MRCP > Custom Vendors**.
2. On the **Custom Vendors** page, select the check box next to the MRCP vendor resource that you want to edit.

 Important:

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

3. Click **Edit**.
4. On the **Edit Custom Vendors** page, edit the **Default Codec** and **Default Port**.

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

Deleting custom MRCP vendors

About this task

Perform the following procedure to delete custom MRCP vendors:

 Important:

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

Procedure

1. Navigate to **EM > System Configuration > Signaling Protocols > MRCP > Custom Vendors**.
2. On the **Custom Vendors** page, select the check box next to the MRCP vendor resource that you want to delete.

 Important:

If you delete a custom MRCP vendor, it deletes all MRCP servers containing the selected vendor.

3. Click **Delete**.
 4. Click **Confirm** to acknowledge the deletion of the MRCP vendor resource.
-

Editing an MRCP server or server resources

About this task

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

Procedure

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

 Important:

To view the resources assigned to an MRCP server in the lower pane, click the name of the corresponding server in the **Server Name** column.

2. On the **Servers** page, select the check box next to the MRCP server that you want to edit.
 3. Click **Edit...**
 4. Edit the **General** MRCP server properties.
 5. To edit a particular server resource, select the check box next to the server resource to be edited and click **Edit...**
 6. Click **Save**.
-

Deleting an MRCP server

About this task

Perform the following procedure to delete an MRCP server:

Procedure

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

Deleting MRCP server resources

About this task

Perform the following procedure to delete the server resources for an MRCP server:

Procedure

1. Navigate to **EM > System Configuration > Signaling Protocols > MRCP > Servers**.
2. On the **Servers** page, select the check box next to the MRCP server.
3. Click **Edit**.

4. In **Server Resources** on the **Edit MRCP Server** page, select the check boxes next to the server resources you want to delete.
 5. Click **Delete**.
 6. On the **Edit MRCP Server** page, click **Save**.
-

Editing an MRCP pool

About this task

Perform the following procedure to edit an MRCP pool:

 Important:

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

Procedure

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

 Tip:

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

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

 Tip:

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

5. Click **Save**.
-

Changing status of MRCP pools

About this task

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

Procedure

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

Deleting an MRCP pool

About this task

Perform the following procedure to delete an MRCP pool:

Procedure

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

Removing MRCP server from a pool

About this task

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

Procedure

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

6. Click **Save**.

Media settings configuration

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

Configuring QoS monitoring settings

About this task

Perform the following procedure to configure Quality of Service (QoS) monitoring:

Procedure

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

 Note:

Some of the changes require system restart to take effect.

Definitions for QoS monitoring properties	
Property	Description
Alert Interval (ms)	The minimum time period between QoS alert monitoring, measured in milliseconds. The default value is 60 milliseconds. The range is 1 to 2147483647 milliseconds.
Critical R Threshold (%)	The R-factor threshold that generates a critical alert after the threshold is crossed. The default value is 70 percent. The range is 0 to 100 percent.
Maximum Alerts	Sets the maximum number of alerts allowed by the IVR. The maximum number of alerts that can be generated

Definitions for QoS monitoring properties	
Property	Description
	during a particular interval is known as QoS Monitoring Alert Interval. This property is used to reduce network traffic. The default value is 100 alerts. The range is 0 to 2147483647 alerts.
QOS Monitoring	Select to enable QoS monitoring.
Refresh Interval (sec)	The minimum period between QoS statistic reporting, measured in seconds. On the EM, default value is 60 seconds. The range is 0 to 2147483647 seconds.
Warning R Threshold (%)	The R-Factor threshold that generates a warning alert after the threshold is crossed. The default value is 80 percent. The range is 0 to 100 percent.

Configuring QoS streaming settings

About this task

Perform the following procedure to configure QoS streaming:

Procedure

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

Note:

Some of the changes require system restart to take effect.

Definitions for QoS streaming properties	
Property	Description
Audio DSCP	The Packet Scheduler (psched) QoS value for audio (ServiceTypeGuaranteed). The default value is 46. The range is 0 to 63.

Definitions for QoS streaming properties	
Property	Description
QOS Maximum Bandwidth Per H.263 Video Flow (bytes)	The QoS maximum bandwidth reserved for the H.263 video flow, measured in bytes. On EM default value is 300000 bytes. The range is 12000 to 1000000 bytes.
QOS Maximum Bandwidth Per NNVC Video Flow (bytes)	The QoS maximum bandwidth reserved for the NNVC video flow, measured in bytes. On EM default value is 300000 bytes. The range is 12000 to 1000000 bytes.
RTCP DSCP Bandwidth	The bandwidth for RTCP DSCP. The range is 100 to 10000.
RTCP DSCP Enable	When enabled, RTCP packets are marked with the same DSCP marking as the RTP session.
Video DSCP	The Packet Scheduler (psched) QoS value for video (ServiceTypeControlledLoad). The default is 34. The range is 0 to 63.

Configuring silence suppression

About this task

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

Perform the following procedure to configure the silence suppression options:

Procedure

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

 Note:

Some of the changes require system restart to take effect.

Definitions for silence suppression properties	
Property	Description
Silence Suppression CN Level	The silence suppression comfort noise (CN) level in dB as defined by RFC3389. The default is minus (–) 127 dB. The range is minus (–) 127 dB to 0 dB.
Silence Suppression Interval (ms)	The number of milliseconds between successive 3389 RTP SS packets. The default is Disabled. The range is 0 to 2147483647 milliseconds.
Silence Suppression Threshold (ms)	The number of milliseconds before transmitted RTP silence is suppressed with 3389 SS packets. The default is 20 milliseconds. The range is 0 to 2147483647 milliseconds.

Configuring continuous STOUTCast streaming

About this task

Avaya MS supports continuous streaming of pre-transcoded audio. The audio must be in either MP3 or wav format.

Perform the following procedure to configure continuous audio streaming from a SHOUTCast source. See the Definitions for continuous SHOUTCast streaming properties table as an aid.

Procedure

1. Navigate to **EM > System Configuration > Media Processing > General Settings > Continuous Streaming Sources**.
2. Use application documentation as an aid to configure the following SHOUTCast configuration properties:
 - a. In the **SHOUTCast Primary URL** field, enter the audio source URL.
 - b. (Optional) In the **SHOUTCast Backup URL** field, enter an alternate audio source URL.
 - c. In the **SHOUTCast Channel Key** field, enter the channel key that is required by the application to attach to the streaming audio.
 - d. (Optional) In the **SHOUTCast HTTP Proxy Host** field, enter the address of the proxy server that is required to access SHOUTCast URLs.
 - e. (Optional) In the **SHOUTCast HTTP Proxy Port** field, enter the port on the internal proxy server that is required to access SHOUTCast URLs.

3. (Optional) Alter the value of **Audio Volume (dB)** to adjust the volume level of the streaming audio.
4. Click **Save**.

 Note:

For some of the changes to take effect, you must restart the media server.

Definitions for continuous SHOUTCast streaming properties	
Property	Description
Audio Volume (dB)	The volume level for the streaming audio is measured in decibels (dB). The default value is -10 dB. The range is from -24 dB to 24 dB.
SHOUTCast Backup URL	An optional backup URL is used to feed audio content to the streaming audio source when the primary SHOUTCast URL is out-of-service. If both the primary and backup servers are unavailable, streaming falls back to the Directory Provider. The maximum length of the URL is 1024 characters.
SHOUTCast Channel Key	A SHOUTCast channel key to attach to the streaming audio. The default is Audio. The length can be from 0 to 48. Changes take effect after the next Avaya MS restart.
SHOUTCast Primary URL	A SHOUTCast URL is used to feed audio content to the streaming audio source. The maximum length of the URL is 1024 characters. The audio stream specified must be in MP3 or wav format.
SHOUTCast HTTP Proxy Host	The FQDN or IP of the internal proxy server that is required to access the SHOUTCast URL.
SHOUTCast HTTP Proxy Port	The port of the internal proxy server that is required to access the SHOUTCast URL.

Configuring continuous RSS streaming

About this task

Avaya MS supports continuous streaming of pre-transcoded audio. The audio must be in either MP3 or wav format.

Perform the following procedure to configure continuous audio streaming from an RSS feed. See the Definitions for continuous RSS streaming Properties table as an aid.

Procedure

1. Navigate to **EM > System Configuration > Media Processing > General Settings > Continuous Streaming Sources**.
2. See the application documentation as an aid to configure the following RSS configuration properties:
 - a. Configure **Audio RSS URL** with the RSS URL of a document that contains MP3 or wav RSS audio.
 - b. Configure **Audio RSS Channel Key** with the channel key that is required by the application for the RSS feed.
 - c. Select **Allow one item per RSS channel** to stream only the first audio item in an RSS document when multiple items are found in the document.
3. (Optional) Alter the value of **Audio Volume (dB)** to adjust the volume level of the streaming audio.
4. Click **Save**.

Note:

For some of the changes to take effect, you must restart the media server.

Definitions for continuous RSS streaming properties	
Property	Description
Audio RSS URL	The RSS URL is used to feed audio content to the streaming audio source. The maximum length of the URL string is 1024 characters. The audio files specified in the RSS document must be in MP3 or wav format. Changes take effect after the next Avaya MS restart.
Audio Volume (dB)	The volume level for the streaming audio is measured in decibels (dB). The default value is -10 dB. The range is from -24 dB to 24 dB. Changes take effect after the next Avaya MS restart.

Definitions for continuous RSS streaming properties	
Property	Description
Audio RSS Channel Key	The channel name associated with the Real Simple Syndication (RSS) feed. This is the RSS feed channel key to attach to the audio streaming. The default is Audio. The maximum length is 48.
Allow one item per RSS channel	Select to stream only the first audio item in an RSS document when multiple items are found in the document. Changes take effect after the next Avaya MS restart.

Enabling and configuring audio codec settings

About this task

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

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

Procedure

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

Audio Codecs

Available:

- G.722

Enabled:

- G.711-ULAW
- G.711-ALAW
- G.729A

Buttons: Add, Add All, Remove, Up, Down

PTimes

	10	20	30	60	Default
G.722	☒	☒	☒	☒	20
G.729A	☒	☒	☒	☒	20
G.711-ALAW	☒	☒	☒	☒	20
G.711-ULAW	☒	☒	☒	☒	20

Warning: selecting 10ms as a default value degrades system capacity.

Buttons: Save, Cancel

2. On the **Audio Codecs** page, select one or more audio codecs from the **Available** list.
3. Click **Add** to move the codecs to the **Enabled** list.
4. To change the priority rank of a codec within the **Enabled** list, select a codec and use the **Up** or **Down** buttons to move the codec within the list.
5. For each codec, select **Default PTime** to use as the offered PTime for outgoing sessions.
6. Select **Silence Suppression** for each codec as required.
7. Click **Save**.

Removing an audio codec

About this task

Perform the following procedure to disable an audio codec that you no longer want to support on the Avaya MS:

Procedure

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

4. Click **Save**.

Enabling and configuring video codec settings

About this task

Perform the following procedure to enable and configure the video codecs you want to support on Avaya MS:

Procedure

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

	10	15	20	25	30	Default Frame Rate:	Preferred Format:	Annex Profile:
H.263	☒	☒	☒	☒	☒	15	CIF	2
H.263+	☒	☒	☒	☒	☒	15	CIF	2
H.263++	☒	☒	☒	☒	☒	15	CIF	2
H.264	☒	☒	☒	☒	☒	15	CIF	
NNVC	☒	☒	☒	☒	☒	15	LARGE	

Enforce Annex X Profiles: ☐

2. On the **Video Codecs** page, select one or more audio codecs from the **Available** list.
3. Click **Add** to move the codecs to the **Enabled** list.
4. To change the priority rank of a codec within the **Enabled** list, select a codec and use the **Up** or **Down** buttons to move it within the list.
5. Select **Allowed Frame Rates** for the codecs you enabled.
6. Choose the desired **Default Frame Rate**, for each added codec.
7. Select the **Preferred Format**, for each enabled codec.
8. Select the **Annex Profile**, for each enabled codec.

Selecting **Enforce Annex X Profiles** means that only prescribed sets of annexes, as described in the annex X profile list, will be accepted.

If you do not select **Enforce Annex X Profiles**, then Avaya MS negotiates arbitrary sets of annexes.

9. Click **Save**.
-

Removing a video codec

About this task

Perform the following procedure to disable a video codec that you no longer want to support on Avaya MS:

Procedure

1. Navigate to **EM > System Configuration > Media Processing > Video Codecs**.
 2. On the **Video Codecs** page, select the video codec from the **Enabled** list.
 3. Click **Remove** to move the codec to the **Available** list.
Repeat Step 2 to Step 3 to disable each video codec.
 4. Click **Save**.
-

Enabling and configuring digit relay settings

About this task

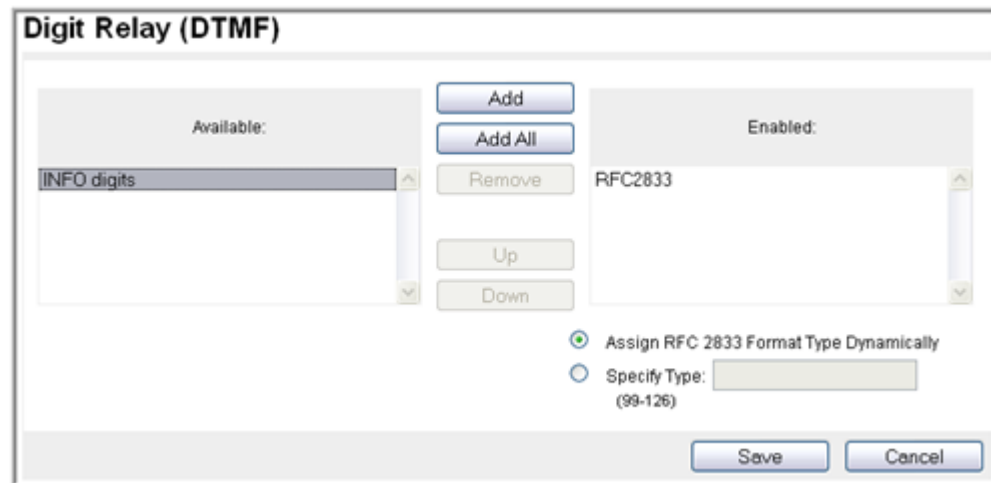
Avaya MS uses digit relay settings and the order of the enabled relay methods when Avaya MS negotiates digit relay with a client endpoint for an inbound or outbound session.

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

Perform the following procedure to enable and configure the digit relay support on Avaya MS:

Procedure

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



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

Removing a digit relay method

About this task

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

Procedure

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

Repeat Steps 2 and Step 3 to disable each video codec.

4. Click **Save**.

Media security configuration

Configure the media security policy to use for Session Description Protocol (SDP) negotiation.

The media security configuration provides the ability to secure media streams with cryptographic protection based on RFC 3711– The Secure Real-time Transport Protocol (SRTP). SRTP is a Real-time Transport Protocol (RTP) (RFC 3550) profile with symmetrical data encryption that provides the following security services: encryption, message integrity, and replay protection.

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

Selecting a media security policy

About this task

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

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

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

Definitions for security policy options		
Property	Description	
Best Effort Mode	The options include:	
	Capability	The SDP is formatted according to the Capability Negotiation format, using tcap/acap/pcap open parameters to negotiate AVP versus SAVP.
	Dual M-Line	The existing default SDP specification, containing both AVP and SAVP media stream offerings for each media type. This is the default.

Procedure

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

Media Security

[Security Policy](#) | [Crypto Suites](#)

Security Policy

Security Policy:

Best Effort Mode:

Enable SRTCP Encryption: ☒

Enable SRTP Encryption: ☒

Enable SRTP Authentication: ☒

Crypto Suites

	Priority	SRTCP Master Key Lifetime	Key Derive Rate	Master Key Index Length
☒ AES_CM_128_HMAC_SHA1_80	<input type="text" value="1"/>	☒ 2 ³¹	<input type="text" value="0"/>	<input type="text" value="0"/>
☐ AES_CM_128_HMAC_SHA1_32	<input type="text" value="1"/>	☒ 2 ³¹	<input type="text" value="0"/>	<input type="text" value="0"/>

2. On the **Media Security** page, in the **Security Policy** area, use the **Security Policy** list to select the required method.
3. In the **Best Effort Mode** list, select the required mode.
4. Click **Save**.

Negotiated parameters

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

- UNENCRYPTED_SRTCP
- UNENCRYPTED_SRTP
- UNAUTHENTICATED_SRTP

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

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

Configuring negotiated parameters

About this task

Perform the following procedure to configure the status of these negotiated parameters in outgoing offers initiated from Avaya MS. Use the *Definitions for Negotiated Parameters* table as an aid for the following procedure.

Procedure

1. Navigate to **EM > System Configuration > Media Processing > Media Security**.
2. Select or clear **Enable SRTCP Encryption**, **Enable SRTP Encryption**, and **Enable SRTP Authentication** as required.
3. Click **Save**.

Related topics:

[Negotiated parameters](#) on page 115

Configuring crypto suites

About this task

Perform the following procedure to configure cryptographic suites to provide message privacy:

Use the Definitions for Crypto Suite Options table as an aid for this procedure.

Definitions for crypto suite options	
Property	Description
AES_CM_128_HMAC_SHA1_80	The SRTP Advanced Encryption Standard (AES) Counter Mode (CM) cipher is used with Hash Message Authentication Code - Secure Hash Algorithm (HMACSHA1) message authentication having an 80-bit authentication.
AES_CM_128_HMAC_SHA1_32	The SRTP AES Counter Mode cipher is used with HMAC-SHA1 message authentication having a 32-bit authentication.
Priority	The preference ranking for Crypto Suites. The default is a priority of 1. A priority of 1 is the highest priority and 9 the lowest.
SRTP Master Key Lifetime	Select to enable SRTP Master Key Lifetime. Uncheck to omit the SRTP Master Key lifetime in outgoing offers. The exponent of the number of packets between key renegotiations. The default value is 2 ³¹ . The range is from 1 to 48.
Key Derive Rate	A value that sets the rate at which new keys are derived. The default value is 0. The default value omits the Key Derivation Rate from outgoing offers and indicates a single key derivation. The range is from 0 to 24.
Master Key Index Length	The number of bytes in the Master Key Index, which is transmitted with each packet, to identify which master key to use for decoding. The default value is 0. The default value omits the Master Key Index from outgoing offers. The range is from 0 to 4.

Procedure

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

Media Security

[Security Policy](#) | [Crypto Suites](#)

Security Policy

Security Policy:

Best Effort Mode:

Enable SRTCP Encryption: ☒

Enable SRTP Encryption: ☒

Enable SRTP Authentication: ☒

Crypto Suites

	Priority	SRTP Master Key Lifetime	Key Derive Rate	Master Key Index Length
☒ AES_CM_128_HMAC_SHA1_80	<input type="text" value="1"/>	☒ 2 ³¹	<input type="text" value="0"/>	<input type="text" value="0"/>
☐ AES_CM_128_HMAC_SHA1_32	<input type="text" value="1"/>	☒ 2 ³¹	<input type="text" value="0"/>	<input type="text" value="0"/>

Save Cancel Restore Defaults

2. On the **Media Security** page, in the **Crypto Suites** section, select the check boxes next to the crypto suites you want to configure.
3. For each selected crypto suite, in the **Priority** column, select a priority number.
4. In the **SRTP Master Key Lifetime** column, select the optional SRTP master key lifetime to include it in outgoing offers. Then, select a value for the SRTP master key lifetime.
5. In the **Key Derive Rate** column, select a key derivation rate.
6. In the **Master Key Index Length** column, select a value for the master key index length.
7. Click **Save**.

Security configuration

Configuring the System Manager settings

Procedure

1. Navigate to **EM > Security > General Settings > System Manager**.
 2. Enter the address of the System Manager in the **System Manager server address** field.
 3. Enter the port used by the System Manager in the **System Manager server port** field.
 4. Enter the enrollment password in the **System Manager trust management enrollment password** field.
 5. Click **Save**.
-

Creating a new certificate signed by System Manager in the Key Store

Procedure

1. Navigate to **EM > Security > Certificate Management > Key Store**.
 2. Select one of the service profiles listed on the **Key Store (Service Profiles)** page.
 3. Click **Edit...**
 4. Click **Create New...** on the **Edit Service Profile** page.
 5. Set the **Signing authority** field to **System Manager**.
 6. Set the remaining fields as required for your system.
 7. Click **Save**.
-

Creating a new certificate to be signed by other Certificate Authorities in the Key Store

Procedure

1. Navigate to **EM > Security > Certificate Management > Key Store**.
 2. Select one of the listed service profiles listed on the **Key Store (Service Profiles)** page.
 3. Click **Edit...**
 4. Click **Create New...** on the **Edit Service Profile** page.
 5. Set the **Signing authority** field to **Other Certificate Authorities**.
 6. Set the remaining fields as required for your system.
 7. Click **Save**.
The system displays a **File Save** dialog window and prompts you to save the file.
 8. Select a location for the file and then save the file.
-

Creating a new self-signed certificate in the Key Store

Procedure

1. Navigate to **EM > Security > Certificate Management > Key Store**.
 2. Select one of the listed service profiles listed on the **Key Store (Service Profiles)** page.
 3. Click **Edit...**
 4. Click **Create New...** on the **Edit Service Profile** page.
 5. Set the **Signing authority** field to **Self-Signed**.
 6. Set the remaining fields as required for your system.
 7. Click **Save**.
-

Processing a Certificate Signing Request Response in the Key Store

About this task

Perform the following procedure only to a certificate that is in pending state:

Procedure

1. Navigate to **EM > Security > Certificate Management > Key Store**.
 2. Select the service profile that the Certificate Signing Request response is for on the **Key Store (Service Profiles)** page.
 3. Click **Edit...**
 4. Click **Certificate Signing Request**.
 5. Click **Browse...** and select the file of the Certificate Signing Request response.
 6. Click **Process Request**.
-

Creating a renewal Certificate Signing Request to be signed by the original signing Certificate Authority

About this task

Perform the following procedure for certificates which are not self-signed:

Procedure

1. Navigate to **EM > Security > Certificate Management > Key Store**.
 2. Select the service profile that the Certificate Signing Request response is for on the **Key Store (Service Profiles)** page.
 3. Click **Edit...**
 4. Click **Certificate Signing Request**.
 5. Click **Renew**.
A **File Save** dialog window appears and prompts you to save the file.
 6. Select a location for the file and then save the file.
-

Deleting a pending Certificate Signing Request (new or renew)

About this task

This procedure is only applicable to a certificate that is in pending state.

Procedure

1. Navigate to **EM > Security > Certificate Management > Key Store**.
 2. Select the service profile that the Certificate Signing Request response is for on the **Key Store (Service Profiles)** page.
 3. Click **Edit...**
 4. Click **Certificate Signing Request**.
 5. Click **Delete Pending Request**.
-

Assigning a certificate for a Service Profile

Procedure

1. Navigate to **EM > Security > Certificate Management > Key Store**.
 2. Select one of the listed service profiles listed on the **Key Store (Service Profiles)** page.
 3. Click **Edit...**
 4. Click **Assign/Unassign...** on the **Edit Service Profile** page.
 5. Set the **Certificate** field using the drop-down list of certificates.
 6. Click **Save**.
-

Unassigning a certificate for a Service Profile

Procedure

1. Navigate to **EM > Security > Certificate Management > Key Store**.
2. Select one of the listed service profiles listed on the Key Store (Service Profiles) page.
3. Click **Edit**.

4. Click **Assign/Unassign...** on the Edit Service Profile page.
 5. Set the **Certificate** field to **None**.
 6. Click **Save**.
-

Importing a certificate for Service Profile

Procedure

1. Navigate to **EM > Security > Certificate Management > Key Store**.
 2. Select one of the listed service profiles listed on the **Key Store (Service Profiles)** page.
 3. Click **Edit...**
 4. Click **Import...** on the **Edit Service Profile** page.
 5. Enter the password or private key for the import in the **Password for certificate import** field.
The password is the same as the one used during the export.
 6. Click **Browse...** and select the certificate file to import.
 7. Click **Save** to import the certificate.
-

Exporting a Key Store certificate in PEM format

Procedure

1. Navigate to **EM > Security > Certificate Management > Key Store**.
 2. Select one of the listed service profiles listed on the **Key Store (Service Profiles)** page.
 3. Click **Edit...**
 4. Select **Export in PEM Format** for the **Type** field.
 5. Click **Export...**
The system displays a File Save dialog window and prompts you to save the file.
 6. Select a location for the file and then save the file.
-

Exporting a Key Store certificate with a key

Procedure

1. Navigate to **EM > Security > Certificate Management > Key Store**.
 2. Select one of the listed service profiles listed on the **Key Store (Service Profiles)** page.
 3. Click **Edit...**
 4. Select **Export with Key** for the **Type** field.
 5. Enter a key in the **Password for certificate export** field.
 6. Click **Export...**
The system displays the File Save dialog window and prompts you to save the file.
 7. Select a location for the file and then save the file.
-

Importing a trust certificate to the Trust Store

Procedure

1. Navigate to **EM > Security > Certificate Management > Trust Store**.
 2. Click **Import...** on the **Trust Store** page.
 3. Enter a name in the **Trust friendly name** field.
 4. Click **Browse...** and select a file to set the **Trust import file** field.
 5. Click **Save**.
-

Importing a Trust Certification Revocation List

Procedure

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

4. Click **Browse...** and select a file to set the **Trust certification revocation list import file** field.
 5. Click **Save**.
-

Downloading a Certification Revocation List

Procedure

1. Navigate to **EM > Security > Certificate Management > Trust Store**.
 2. Select a Certificate Authority from the list.
 3. Click **Download CRL...** on the **Trust Store** page.
The system displays a File Save dialog window and prompts you to save the file.
 4. Select a location for the file and then save the file.
-

Deleting Certificate Authorities from the Trust Store

Procedure

1. Navigate to **EM > Security > Certificate Management > Trust Store**.
 2. Select a Certificate Authority from the list.
 3. Click **Delete** on the **Trust Store** page.
 4. Click **Save**.
-

Content Store configuration

Configuring Content Store location

The Content Store component of Avaya MS stores media and other files for hosted applications on a disk. Avaya MS also uses the disk for SDR storage, persistent database store, and file manipulation that is unrelated to Content Store file management. As a result of the many

requirements Avaya MS has for the system disk, disk performance can be an issue for some applications.

The default installation places content storage in a directory within the main Avaya MS installation path. To improve the capacity and performance of the system, configure a dedicated disk for Content Store. Content Store uses this dedicated disk for applications that have large media file storage requirements.

 Note:

Changing the Content Store location is a commissioning task for new systems. If you change the Content Store location at a later time, files remain in the original location, and you need to remove these files manually.

Before you begin

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

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

About this task

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

Procedure

1. Navigate to **EM > System Configuration > Content Store > General Settings**.
 2. In the **File system location for content storage** field, enter the full pathname, starting from the file system root, to specify the disk that the system should use for Content Store.
For example, enter `F: /MediaFiles` for Windows, or `/mediafiles` for Linux.
Restore the default value or clear the **File system location for content storage** field to use the default location within the installation path.
 3. Click **Save**.
 4. Click **Confirm**.
Restart the server for the changes to take effect.
-

EM preferences configuration

Configuring time zone preferences

About this task

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

Avaya MS defaults to using the local time.

Procedure

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

Setting Login security warning text

About this task

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

Procedure

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

Chapter 5: Media file provisioning

Media file format

The audio files played by Avaya MS must be encoded as 16 bit, 8 kHz, single channel, LPCM files. However, you can use other sampling rates and codecs that are supported by Avaya MS. Avaya MS does not support multiple channels, like stereo.

Media storage in Avaya MS Content Store

The Content Store component of Avaya Media Server (MS) stores media and other files for hosted applications. Content Store provides a reliable, highly available, and persistent storage capability for Avaya MS. Any application with storage needs that align with the functionality of Content Store can use Content Store. However, not all applications need to use Content Store.

Content Store has an organized storage space consisting of Namespaces that include Content Groups which contain the actual content. Namespaces are the top level containers, under which Content Group containers exist. Namespaces and Content Groups can be considered analogous to folders. Actual content is stored by Content ID within each Content Group. A Content ID is analogous to a filename.

The following example shows the structure of Content Store:

```
Namespace_I
  ContentGroup_A
    Content_ID1
    Content_ID2
  ContentGroup_B
    Content_ID1
    Content_ID2
Namespace_II
  ContentGroup_A
    Content_ID1
    Content_ID2
```

To support capacity and high availability requirements of some installations, the Content Store is scaled automatically with the cluster. Content Stores are automatically enabled and configured on both the Primary and Secondary cluster servers or on the Primary and Backup server in High Availability pairs. The dual Content Store configuration provides full hardware

redundancy for critical applications. The application content in the Content Stores of a cluster is synchronized automatically.

Overview of the EM Media Management tool

Element Manager (EM) provides a Media Management tool that you can use to upload and manage media files in Content Store. Using the Media Management tool, you can perform the operations described in the following table to manage media files stored in Content Store.

Media management operations		
Scope	Operation	Description
Namespace	Add	Create a new namespace.
	Browse	View the content of a namespace.
	Rename	Give a new name to a namespace.
	Delete	Remove a namespace and its content.
Content Group	Add Content Group	Create new content groups under a namespace or another content group.
	Add Media	Upload media files to a content group.
	Delete	Remove the content group and its files.
	Rename	Give a new name to a content group.
	Batch File Provision	Upload multiple files contained in a zip archive file.
Content	Cut	Use Cut and paste together to move a media content file from one content group to another.
	Copy	Use Copy and Paste together to duplicate an existing content file.
	Paste	Use with Copy and Cut to move and duplicate media files.

Media management operations		
Scope	Operation	Description
	Rename	Give a new name to a media file.
	Download	Download a media file to the local computer running the browser that you use to gain access to the EM.

 Note:

Do not alter the default system namespaces.

 Important:

Do not use the file system to manually locate and change the media files managed by Content Store. Use appropriate interfaces such as the EM Media Management tool to make any changes.

The following procedures show you how to use each of these operations to organize and manage your media on Avaya MS.

Media Provisioning

Adding a content namespace

About this task

Perform the following procedure to add a content namespace to contain a group of related media files:

Procedure

1. Navigate to **EM > Tools > Media Management**.
2. On the **Media Management** page, click **Add...**
3. On the **Add Content Namespace** page, type a unique name for the new namespace in the **Name** field.

The name cannot begin with the ampersand (@) symbol, must be less than 128 characters, must not be case-sensitive, must not contain spaces, or any of the following symbols:

{ } ' * \

4. Click **Save**.
-

Renaming a content namespace

About this task

Perform the following procedure to rename a content namespace to describe what a namespace contains:

Procedure

1. Navigate to **EM > Tools > Media Management**
2. On the **Media Management** page, select the check box next to the namespace you want to rename.
3. Click **Rename**.
4. On the **Rename Content Namespace** page, type a unique name for the new namespace in the **Name** field.

Important:

The name cannot begin with the ampersand (@) symbol, must be less than 128 characters, is not case sensitive, and must not contain spaces or any of the following symbols:

{ } ' * \

5. Click **Save**.
-

Deleting a content namespace

About this task

Perform the following procedure to remove a content namespace from the system:

Procedure

1. Navigate to **EM > Tools > Media Management**.
2. On the **Media Management** page, select the check box next to the namespace you want to delete.
3. Click **Delete**.

4. On the **Delete Content Namespace** dialog box, click **Confirm**.
-

Viewing namespace content

About this task

Perform the following procedure to select a content namespace that you want to manage or browse:

Procedure

1. Navigate to **EM > Tools > Media Management**.
 2. On the **Media Management** page, select the check box next to the namespace that you want to manage or browse.
 3. Click **Browse**.
 4. From the left pane in the **Provision Media** page, select the namespace, which is the top item in the tree.
Navigate the namespace using the plus sign (+) and minus sign (-) to expand and hide the content.
-

Adding a content group

About this task

Perform the following procedure to add content groups and to organize the media in a content namespace into logical groups:

Procedure

1. Navigate to **EM > Tools > Media Management**.
2. On the **Media Management** page, select the check box next to the desired namespace.
3. Click **Browse**.
4. On the **Provision Media** page, in the left pane, select the name of the content namespace in which you want to add a new content group.
If applicable, navigate to a content group and click the content group to which you want to add the subcontent group.
5. Click **Add Content Group**.

6. In the **Name** field of the **New Content Group** dialog box, type a name for the new content group.

 Important:

The name cannot begin with the ampersand @ symbol, must be less than 128 characters, must not be case sensitive, and must not contain spaces or any of the following symbols:

{ } ' * \

 Tip:

You can use the forward slash (/) delimiter to specify sub-content groups in the tree structure. For example, typing `music/rock` in the **Name** field creates a `music` content group, with a sub-content group called `rock`, all in one step.

7. Click **Save**.

Adding media files on the server to a content group

About this task

Perform the following procedure to add media files to a content group, by uploading one media file at a time:

 Note:

Many browsers have a 2GB limit for file uploads.

 Note:

The audio files played by Avaya MS must be encoded as 16 bit, 8 kHz, single channel, LPCM files. However, you can use other sampling rates and codecs that are supported by Avaya MS. Avaya MS does not support multiple channels, like stereo.

Procedure

1. Using a browser on the same computer where your file resides, navigate to **EM > Tools > Media Management**.
2. On the **Media Management** page, select the check box next to the namespace.
3. Click **Browse**.
4. On the **Provision Media** page, select the content group to which you want to add a media file.
5. Click **Add Media**.

6. In the **Add Media** dialog box, click **Browse** and navigate to the media file you want to upload.
 7. Select **Always overwrite files with the same name** or **Do not overwrite files with the same name**.
 8. To remove the extension from the filename, select **Cut extension**.
 9. To use a different name for the media file that is uploaded, enter a new name in the **New Name** field.
 10. Click **Upload**.
-

Downloading media files to your computer

About this task

Perform the following procedure to download a media file stored on the media server to your computer:

Procedure

1. Using a browser on the computer where you want to download the file to, navigate to **EM > Tools > Media Management**.
 2. On the **Media Management** page, select the check box next to the namespace.
 3. Click **Browse**.
 4. On the **Provision Media** page, select the content group containing the media file you want to download.
 5. In the **Name** column in the right pane, select the media file you want to download.
 6. Right-click the file, and select **Download**, or use the **More Actions** drop-down menu, and select **Download**.
 7. In the **Download Media** dialog box, click **Download**.
The system displays a pop-up window.
 8. Click **Save**.
The procedure to save the file varies depending on the Web browser you use.
-

Renaming a content group

About this task

Perform the following procedure to rename a content group:

Procedure

1. Navigate to **EM > Tools > Media Management**.
2. On the **Media Management** page, select the check box next to the namespace.
3. Click **Browse**.
4. On the **Provision Media** page in the left pane, click the plus sign (+) next to the media namespace.
5. Select the content group that you want to rename.
6. Right-click the content group and select **Rename** or use the **More Actions** drop-down menu, and select **Rename**.
7. In the **New Name** field of the **Rename Content Group** dialog box, type a name for the new content group.

Important:

The name cannot begin with the ampersand (@) symbol, must be less than 128 characters, must not be case sensitive, and must not contain spaces or any of the following symbols:

{ } ' * \

8. Click **Save**.
-

Deleting a content group

About this task

Perform the following procedure to delete a content group:

Procedure

1. Navigate to **EM > Tools > Media Management**.
 2. On the **Media Management** page, select the check box next to the namespace.
 3. Click **Browse**.
 4. On the **Provision Media** page, in the left pane, click the plus sign (+) next to the media namespace.
 5. Select the content group that you want to delete.
 6. Click **Delete** or right-click the content group, and select **Delete**.
 7. In the **Confirm Content Group Delete** dialog box, click **Confirm**.
-

Batch provision media

Creating file structure for the zip file

About this task

You can batch provision media for a content namespace using a zip file that you create and upload.

Perform the following procedure to create a proper file structure on your local system for the zipped files:

Important:

When you create the zip file, remember the following naming conventions:

- The namespace and content group names cannot begin with the ampersand (@) symbol, must be less than 128 characters, must not be case-sensitive, and must not contain spaces or any of the following symbols: { } ' * \
- The media file names must be less than 128 characters, must not be case-sensitive, and must not contain any of the following symbols: { } ' * \

Note:

Many browsers have a 2GB limit for file uploads.

Note:

The audio files played by Avaya MS must be encoded as 16 bit, 8 kHz, single channel, LPCM files. However, you can use other sampling rates and codecs that are supported by Avaya MS. Avaya MS does not support multiple channels, like stereo.

Procedure

1. Select a target namespace already configured on Avaya MS, for example, MyNamespace.
2. Create a directory on your system with the same name as the target content namespace name.
The directory that you create is the root directory for your zip archive.
3. Create subdirectories in the namespace directory.
These represent the content groups that the system creates in the target namespace. The file structure in the uploaded zip file must match the Namespace and content group structure that you want on the Avaya MS. If the structure is not as described in the example, the upload fails.

For example, to upload media zip files to a namespace called MyNameSpace with a content group called MyContentGroup, the zip file structure must be as follows:

```
MyNameSpace\MyContentGroup\MyMediaFile1.wav  
MyNameSpace\MyContentGroup\MyMediaFile2.wav  
MyNameSpace\MyContentGroup\MyMediaFileX.wav
```

4. Follow the instructions of the zip archiving tool to zip up the entire MyNameSpace directory.
-

Uploading archived media

About this task

Perform the following procedure to provision the media on Avaya MS after the zip file is ready for upload:

Procedure

1. Using a browser on the same computer where your zip file resides, navigate to **EM > Tools > Media Management**.
 2. On the **Media Management** page, select the check box next to the namespace.
 3. Click **Browse**.
 4. On the **Provision Media** page, right-click the content namespace and select **Batch File Provision** on the **More Actions** drop-down menu.
 5. In the **Batch File Provision** dialog box, click **Browse** to navigate to the zip file to upload.
 6. Select **Always overwrite files with the same name** or **Do not overwrite files with the same name**.
 7. To remove the extension from the filename, select **Cut extension**.
 8. Click **Upload**.
 9. Verify that the media is uploaded by browsing the namespace and content groups with the Media Management tool.
-

Searching for a media file

About this task

Perform the following procedure to search for a stored media file on the system:

Procedure

1. Navigate to **EM > Tools > Media Management**.
 2. On the **Media Management** page, select the check box next to the namespace.
 3. Click **Browse**.
 4. On the **Provision Media** page, click **Search** in the upper-right corner.
 5. In the **File Name** field, type the full or partial file name.
 6. In the **Search In Content Group** list, select the name of the content group in which you want to search for media files.
 7. Click **Search**.
The content pane lists the result that matches.
 8. To perform media file operations, select the content and right-click or use the **More Actions** drop-down menu and select the required operation.
-

Renaming a media file

About this task

Perform the following procedure to rename a media file:

Procedure

1. Navigation to **EM > Tools > Media Management**.
2. On the **Media Management** page, select the check box next to the namespace.
3. Click **Browse**.
4. To locate the content to be removed, use the left pane of the **Provision Media** page to navigate the namespace and content groups.
Use the plus sign (+) and the minus sign (–) to expand and hide the content as needed. Alternatively, you can click **Search** in the upper-right corner of the page.
5. After you locate the file on the page, right-click the content name and select **Rename** or use the **More Actions** drop-down menu and select **Rename**.
6. In the **Rename Media** dialog box, type a new name for the file in the **New Name** field.

Tip:

The name must be less than 128 characters, must not be case sensitive and must not contain any of the following symbols: { } ' * \

7. Click **Save**.
-

Moving a media file

About this task

Perform the following procedure to move a media file to another content group:

Procedure

1. Navigate to **EM > Tools > Media Management**.
 2. On the **Media Management** page, select the check box next to the namespace.
 3. Click **Browse**.
 4. To locate the content to be moved, use the left pane of the **Provision Media** page to navigate the namespace and content groups.
Use the plus sign (+) and the minus sign (-) to expand and hide the content as needed.
 5. After you locate the file and the file on the page, right-click the content name and select **Cut** or use the **More Actions** drop-down menu and select **Cut**.
 6. In the left pane, go to the content group where you want to move the media file.
 7. Right-click the content group and select **Paste** from the menu or use the **More Actions** drop-down menu and select **Paste**.
-

Copying a media file

About this task

Perform the following procedure to copy a media file:

You can duplicate media content within the same content group or duplicate the media content to a different content group. The system creates the copy with the name **Copy of <filename>**. You must give the file an appropriate name using the rename procedure.

Procedure

1. Navigate to **EM > Tools > Media Management**.
2. On the **Media Management** page, select the check box next to the desired namespace.
3. Click **Browse**.

4. To locate the content to be copied, use the left pane of the **Provision Media** page to navigate the namespace and content groups.
Use the plus sign (+) and the minus sign (-) to expand and hide the content as needed.
 5. After you locate the file on the page, right-click the content name and select **Copy** or use the **More Actions** drop-down menu and select **Copy**.
 6. In the left pane, go to the content group where you want to copy the media file.
 7. Right-click on the content group and select **Paste** from the menu or use the **More Actions** drop-down menu and select **Paste**.
 8. To rename the copied file, right-click the new copy of the file with **Copy of <filename>** format and select **Rename** from the menu, or use the **More Actions** drop-down menu and select **Rename**.
-

Deleting a media file

About this task

Perform the following procedure to remove a media file from the system:

Procedure

1. Navigate to **EM > Tools > Media Management**.
 2. On the **Media Management** page, select the check box next to the namespace.
 3. Click **Browse**.
 4. To locate the content to be removed, use the left pane of the **Provision Media** page to navigate the namespace and content groups.
Use the plus sign (+) and the minus sign (-) to expand and hide the content.
Alternatively you can click **Search** in the upper-right corner.
 5. Select the content item that you want to remove and click **Delete** or right-click on the content item and select **Delete**.
 6. In the **Confirm Media Delete** dialog box, click **Confirm**.
-

Chapter 6: Application management

Enabling CCXML and VoiceXML applications

About this task

CCXML and VoiceXML applications are disabled by default on Avaya Media Server (MS).

Perform the following procedure to update the Server Profile to enable these application types:

Procedure

1. Navigate to **EM > System Configuration > Server Profile**.
 2. Select all the CCXML and VoiceXML related check boxes.
 3. Click **Save**.
-

Adding CCXML and VoiceXML custom applications

About this task

In addition to packaged applications, you can define custom CCXML and VoiceXML applications on Avaya MS.

Perform the following procedure to add a custom application and the SIP translations of the custom application:

Procedure

1. Navigate to **EM > Applications > Custom Applications**.
2. Click **Add...**
3. Select **URL** for the **Application Type**.
4. Enter a name for your application in the **Application Name** field.
5. In the **URL** field, specify the URL which each incoming call fetches.
6. Select the **Initial Interpreter Type** as **VoiceXML** or **CCXML**.

7. (Optional) Select **Add SIP Translation** to specify the SIP translation **Mode**, **Algorithm**, **Pattern**, and **Rank** for this application. You can configure the SIP translation later.

 Note:

Sip Account Association is currently not used.

8. Click **Save**.
-

Editing CCXML and VoiceXML custom applications

About this task

Perform the following procedure to edit an existing custom application:

Procedure

1. Navigate to **EM > Applications > Custom Applications**.
2. Click on the name of the application you want to edit, or select the check box next to the application and click **Edit...**
3. On the **Edit Custom Application** page, alter the fields for this application.

 Note:

Sip Account Association is currently not used.

4. Click **Save**.
-

Application interpreter configuration

Configuring RFC5707 (MSML) interpreter

About this task

Perform the following procedure to configure the RFC5707 Media Server Markup Language (MSML) settings:

Procedure

1. Navigate to **EM > System Configuration > Application Interpreters > RFC5707 (MSML) > General Settings**.
 2. Select **MSML Video Capability Negotiation** to enable video negotiation if offered by the SIP client endpoints.
 3. Select **MSML HA Event Notification** to enable MSML event notification when failover occur in High Availability mode.
 4. Enter the default announcement namespace in the **MSML Default Namespace** field.
 5. Click **Save**.
 6. Restart the system for the changes to take effect.
-

Configuring VoiceXML interpreter

About this task

Perform the following procedure to configure the Voice Markup Language (VoiceXML) default interpreter settings:

If the application defines the settings, then you do not need to change the settings.

Procedure

1. Navigate to **EM > System Configuration > Application Interpreters > VoiceXML > General Settings**.
 2. Alter the fields to change the default functionality for VoiceXML applications.
 3. Click **Save**.
 4. Restart the system for the changes to take effect.
-

Configuring CCXML interpreter

About this task

Perform the following procedure to configure the Call Control Markup Language (CCXML) default interpreter settings:

If the application defines the settings, then you do not need to change the settings.

Procedure

1. Navigate to **EM > System Configuration > Application Interpreters > CCXML**.
 2. Alter the fields to change the default output for CCXML applications.
 3. Click **Save**.
 4. Restart the system for the changes to take effect.
-

Viewing or changing application operational state

About this task

Perform the following procedure to manage the operational state of installed applications:

Procedure

1. Navigate to **EM > Applications > Operational State**.
 2. You can view the current state of each listed application in the **State** column.
 3. To change application states, select the check box next to one or more listed applications and then click **Lock**, **Unlock**, or **Pending Lock** from the **More Actions** drop-down menu.
-

Viewing or changing custom application operational state

About this task

Perform the following procedure to manage the operational state of custom applications:

Procedure

1. Navigate to **EM > Applications > Custom Applications**.
 2. You can view the current state of each listed application in the **State** column.
 3. To change application states, select the check box next to one or more listed applications and then click **Lock**, **Unlock**, or **Pending Lock** from the **More Actions** drop-down menu.
-

Configuring application signaling translations

About this task

Application signaling translations map incoming SIP INVITE requests to an application. Then the system invokes the application.

The system performs translations by using the configured comparison **Algorithm** to match a configured string **Pattern**. The configured **Mode** determines where in the SIP INVITE the system looks for the pattern.

If the **Pattern** field contains the same value for multiple translations, then the system uses the **Rank** of the translation to determine which application to invoke. Translations with the same **Pattern** must not be configured with the same **Rank**.

Perform the following procedure to add or modify application signaling translations:

Procedure

1. Navigate to **EM > Applications > Signaling Translations**.
2. Click **Add...** to create a new translation, or select an existing translation from the list and click **Edit...**
3. Select an existing application for **Application name**.
4. Select the translation **Mode**.
5. Select an **Algorithm** from the options.
6. Specify a match pattern in the **Pattern** field.
7. Enter a translation **Rank**.
The lower the number, the higher the priority of the translation.
8. Click **Save**.

Deleting application signaling translations

About this task

Perform the following procedure to remove defined translation from the application translations listed on the **Signaling Translations** page:

Procedure

1. Navigate to **EM > Applications > Signaling Translations**.

2. Select one or more translations from the list and click **Delete**.
-

Deleting a custom application

About this task

Perform the following procedure to remove a custom application from the system:

Procedure

1. Navigate to **EM > Applications > Custom Applications**.
 2. Select the check box next to one or more listed applications that you want to delete.
 3. Select **More Actions > Delete**.
-

Configuring packaged applications

About this task

Each installed packaged application can have unique settings which you need to configure. The packaged applications installer adds an EM plug-in to integrate the plug-in in the Avaya MS EM.

Perform the following procedure to gain access to the plug-ins:

Procedure

1. Navigate to **EM > Applications > Packaged Applications**.
 2. Modify the application configuration settings.
-

Chapter 7: Backup and restore

Backup and restore overview

Avaya Media Server (MS) can backup and restore system configuration data and application content stored in Content Store. You must maintain backups of your system to recover from hardware failure or to restore data to a previous point in time.

Using the Element Manager (EM), you can define, manage, and schedule backup and restore tasks. Use the Avaya MS command line backup and restore tool when you use a management interface other than EM.

 Important:

Storing the backup file locally on the same disk does not protect data from disk drive failure.

If you reimage your system or replace the disk drive, preserve the backup file if you have stored the backup file on the disk. Preserving the backup file ensures the backup is available for you to restore or upgrade the Avaya MS system.

 Important:

Backup data is not portable from one server to another. If you need to replace a server, you must configure the server with the same installation path, IP address, and hostname so that the data is compatible.

Configuring a backup task

About this task

EM organizes backups as tasks. These tasks contain your selected backup options and specify the location where the backup is stored.

You can create an automated backup task to create backups daily, weekly, monthly or at one particular time. You can store the backup in a local destination directory or in a remote server using File Transfer Protocol (FTP).

You cannot change Default Backup Destination, the predefined backup destination of Avaya MS. If the administrator chooses to create a backup using this destination, EM stores the backup files in the following predefined local directories for Linux or Windows on Avaya MS:

Linux: `<install path>/avaya/ma/MAS/platdata/EAM/Backups`

Windows: `<install path>\Avaya\Multimedia_Applications\MAS\platdata\EAM\Backups`

You can configure remote backup destinations and these destinations can be shared by multiple backup tasks. When you perform backups to remote destinations, EM uploads the backup files to the specified FTP server. If required, EM then deletes the local backup file from Avaya MS.

There are two types of content that you can include in your backups: System Configuration and Application Content. You can create one task for both the backup types or create separate tasks, each with independent schedules. Each backup type contains the following information:

Type of content	Description
System Configuration	Contains all the Avaya MS system settings that the Avaya MS management system has configured. For example, the settings you configure with the EM.
Application Content	Includes data that the Avaya MS Content Store manages. The data can either be the data that the applications generate or subscribers save. Examples of these data include subscriber preferences for a conferencing service or deposited voicemails and user preferences for a messaging service. The backup type does not include files stored on Avaya MS which are not stored in the Content Store.

Perform the following procedure to define or update backup tasks and destinations using EM:

Procedure

1. Navigate to **EM > Tools > Backup and Restore > Backup Tasks**.
2. Either create a new backup task by clicking **Add...** or select an existing task from the list and click **Edit...**

Edit Backup Task

[Option](#) | [Schedule](#)

Option

Backup Task Name:

Backup Type: ☒ System Configuration ☒ Application Content

Backup Destination:

	Destination Name	Path
1	Default Backup Destination	
2	RemoteBackupServer	ftp://135.60.68.12

Schedule

All times are based on the local server time

Run Backup: ☐ Manually, as needed. ☒ Schedule.

Schedule Task:

Start Time: :

3. Enter a name without spaces for this backup task in the **Backup Task Name** field.
4. For a complete backup, select both **System Configuration** and **Application Content** backup types.
5. Configure the destination for your backup files by selecting one of the following options:
 - Select the **Default Backup Destination** to store the backup on the local disk.
This option does not protect your system from Avaya MS disk drive failure.
 - Select **Add...** to define a new remote FTP location for your backup file.
 - Select an existing destination and click **Modify...** to alter the remote FTP properties.
6. If you choose to add or modify a backup task, then fill in the **Backup Destination Properties**:
 - a. Enter the server properties in the fields.
 - b. Click **Test** to verify whether your configuration can contact the server.
 - c. Click **Save**.

7. Select either **Manually, as needed**, or **Schedule** depending on how you want the backup to run.
 8. If you selected **Schedule**, then configure the **Schedule Task** either as Daily, Weekly, Monthly, or Once, and the date and time.
 9. Click **Save**.
The new backup task is included in the list of Backup Tasks.
-

Executing a backup task

About this task

Perform the following procedure to manually run a defined backup task:

Procedure

1. Navigate to **EM > Tools > Backup and Restore > Backup Tasks**.
 2. Select the check box next to the desired backup task in the list.
 3. Click **Run Now**.
 4. Click **Confirm** to execute the backup task.
 5. Monitor the Backup and Restore History Log at **Tools > Backup and Restore > History Log**.
After the backup is complete, the log shows a completed backup task entry.
 6. Confirm whether the backup files were saved to the desired FTP location or local default destination. If the backup files are saved to the local destination, the local backups are found in the following directories:
 - **Linux:** `<install path>/avaya/ma/MAS/platdata/EAM/Backups`
 - **Windows:** `<install path>\Avaya\Multimedia_Applications\MAS\platdata\EAM\Backups`
-

Deleting a backup task

About this task

Perform the following procedure to remove a defined backup task:

Procedure

1. Navigate to **EM > Tools > Backup and Restore > Backup Tasks**.

2. Select the check box next to the desired backup task in the list.
 3. Click **Delete**.
 4. Click **Confirm** to remove the backup task.
-

Editing a backup destination

About this task

Perform the following procedure to edit a backup destination to alter the FTP settings for storing backup files:

Procedure

1. Navigate to **EM > Tools > Backup and Restore > Backup Destinations**.
 2. Click on the name of the backup task you want to edit.
 3. Click **Edit...**
 4. Modify the fields on the **Backup Destination Properties** page.
 5. Click **Test** to verify your configuration can contact the server.
 6. Click **Save**.
-

Restoring from the local destination

About this task

Perform the following procedure to reconstruct data on Avaya MS by restoring data using a backup saved in the default backup destination:

The local backups that you are able to choose from are stored in:

Linux: <install path>/avaya/ma/MAS/platdata/EAM/Backups

Windows: <install path>\Avaya\Multimedia_Applications\MAS\platdata
\EAM\Backups

Procedure

1. Navigate to **EM > Tools > Backup and Restore > Restore**.
2. On the **Restore** page, in the **Restore Source** drop-down list, select **Default Backup Destination**.

3. In the **Restore Task List**, select the backups from the list which you want to use for the restore.
4. Click **Restore Now**.
5. On the **Confirm Restore** page, click **Confirm** to proceed with the restore.

 Important:

Restoring a backup archive might impact running applications. After you click **Confirm**, the system invokes the restore task, and EM and Avaya MS close the connections to all users until the system completes the restoration. You must restart the system after Avaya MS completes the restore. The administrator is responsible for informing users about the availability of EM after the servers complete the restore.

6. Restart the server to complete the restore.

Uploading a backup file for restore

About this task

Perform the following procedure to restore using an uploaded backup file to reconstruct data on your Avaya MS.

 Important:

Backup data is not portable from one server to another. If you need to replace a server, you must configure the server with the same installation path, IP address, and hostname so that the data is compatible.

Procedure

1. Navigate to **EM > Tools > Backup and Restore > Restore**.
2. On the **Restore** page, in the **Restore Source** drop-down list, select **Upload Backup Files**.
3. Click **Browse** to select the backup files.
You can upload a System Configuration and Application Content backup at the same time.
4. On the **Confirm Restore** page, click **Confirm** to proceed with the restore.

 Important:

Restoring a backup archive might impact running applications. After you click **Confirm**, the system invokes the restore task, and EM and Avaya MS close the connections to all users until the system completes the restoration. You must restart the system after Avaya MS completes the restore. The administrator is

responsible for informing users when EM is available after the servers complete the restore.

5. Restart the server to complete the restore.
-

Viewing the backup and restore history log

About this task

Each backup and restore operation, whether a success or a failure, is recorded in the backup and restore history log. You can use this log to see when the last backup and restore was executed, and to verify when a manually executed backup or restore was completed. The logs also report the elapsed time and size of each executed task.

Perform the following procedure to view the backup and restore history log:

Procedure

1. Navigate to **EM > Tools > Backup and Restore > History Log**.
 2. Use the **View** drop-down menu to select **All**, **Backup**, or **Restore** to filter the list of logs the system displays.
 3. Use the **Refresh Interval** to select the desired update frequency of the logs, in case you are monitoring backup or restore for completion.
 4. Click **Export** to save the log history.
 5. Click **Clear** to delete the current log history.
-

Configuring the history log

About this task

Perform the following procedure to configure the number of days for saving backup files and restoring history logs on the server before the files or logs are automatically removed:

Procedure

1. Navigate to **EM > Tools > Backup and Restore > General Settings**.
 2. Enter the number of days that you want to save backup and restore history log files on the server before the files are removed in the **Store history and log files for up to** field.
 3. Click **Save**.
-

Using the command-line backup and restore tool

About this task

The command-line backup restore tool backs up the same System Configuration and Application Content data as EM does when using task based system.

The executable file name is `backuprestore`. The following Backup and Restore tool description provides an overview of the options and the functionality.

Usage:

```
BackupRestore <-b | -r> <filename> -t <taskid> [-ftp server user
password destpath [-d]] [-c]
```

Backup Examples:

```
backuprestore -b /backup/AMS_CONFIG_BACKUP_HOSTNAME.zip -t config -
ftp ftpserver1 anonymous 1234 /export/home/anonymous/ -d
```

```
backuprestore -b /backup/AMS_SERVICE_BACKUP_HOSTNAME.zip -t service
```

Restore Examples:

```
backuprestore -r /backup/AMS_CONFIG_BACKUP_HOSTNAME.zip
```

Important:

- Quotation marks must be used if there are spaces in the filenames.
- The order of the parameters is important. Follow the earlier examples.
- You must include the .zip extension in your filename.

Backup Restore tool options	
Option	Description
-h	Display the Help message.
-b	Backup indicator followed by the <i><filename></i> .
-r	Restore indicator followed by the <i><filename></i> .
filename	Archive .zip file name including full path.
-t	Backup Task type: Defines what will be backed-up: config indicates System Configuration service indicates Application Content.
-ftp	FTP the resulting backup file. This is optional.

Backup Restore tool options	
Option	Description
-d	Delete the local file upon successful ftp transfer or restore. This is optional.
-c	The direct output that is sent to the console instead of the debug file. Make -c the last argument. This is optional.

Procedure

1. Open a Linux shell or Windows command-line console on Avaya MS.
2. Execute the **backuprestore** tool following the usage guidelines.

For example:

```
backuprestore -b backupfilename.zip -t config
```

or

```
backuprestore -r backupfilename.zip
```

Chapter 8: Avaya MS monitoring

Avaya MS monitoring overview

Element Manager (EM) provides ways to monitor the processing status of Avaya Media Server (MS). Administrators can view alarms, logs, protocol traces, and performance metrics of an individual element or an entire cluster using the available monitoring tasks.

In EM, the monitoring tasks are grouped under the System Status category in the left menu pane.

Element status viewing

The current operational status of a particular element, for example, the server you are administrating, is available on EM. For information on procedures to view and change the status of Avaya MS, see [Logging in to and navigating in EM](#).

Related topics:

[Logging in to and navigating in EM](#) on page 27

Viewing cluster status

About this task

The system displays the **Cluster Status** page with the operational state of the cluster and the member elements.

Procedure

1. Navigate to **EM > System Status > Cluster Status**.

Cluster Status

Select an element name to view the alarm viewer for that element.

[System Status](#) | [System Performance Summary](#)

System Status

Refresh every:

Element Name	UUID	Element Role	Element Status	Alarm Description
server3496.richlab	ac9905a0-80c5-11e0-8aa8-000d60d49a6c	Primary	Normal	No Alarm
server3497.richlab	e3cf0e20-80c5-11e0-8bdb-000d60d49748	Backup	Normal	No Alarm

System Performance Summary

Refresh every:

Name	Value (Aggregate)
Active Sessions	0
SIP Inbound Call Attempted	0
SIP Outbound Call Attempted	0

2. Scroll through the **System Status** pane to view the columns and the status of each element.

The **System Performance Summary** pane is present under the **System Status** pane. The **Key Performance Indicators** listed are an aggregate of all the cluster elements and represent the cluster as a whole.

The **System Performance Summary** pane is available only on Primary servers and displays only the operational measurements that are configured as **Key Performance Indicators** (KPIs).

3. Click the **Element Name** of an individual element in the **System Status** pane. The system displays the detailed alarm information for that particular element.

Monitoring alarms

About this task

Avaya MS generates an active alarm any time Avaya MS detects an operational error condition that requires corrective action by the administrator.

Avaya MS contains many individual system components that perform specific functions during operation. When a component detects an error condition the component raises an alarm. The component that raises the alarm automatically clears the alarm after the administrator resolves the error condition.

The system generates an event log each time a component raises or clears an alarm. The event log provides a clear record of all state changes on Avaya MS long after the error condition is resolved.

You can view the list of active alarms in the EM alarm viewer. The system updates the alarm viewer in real time. You do not need to refresh the alarm viewer manually.

EM displays the following information for each alarm:

Alarm field descriptions	
Field	Description
ID	A unique identifier assigned to the alarm.
Severity	A color represents the alarm severity. Red indicates Critical and Major alarms, and yellow represents all other alarms. The severity of the alarm from most severe to least severe are Critical, Major, Minor, and Warning.
Date and Time	The timestamp of the exact time the alarm is raised. You can configure timestamps display as either local time or Universal Time Coordinated (UTC) time. UTC time can be useful for correlating alarms with events in other time zones.
Description	A description of the type of error condition encountered.
Component	The name of Avaya MS software component reporting the alarm.
Probable Cause	A description of the probable cause of this alarm.
Corrective Action	A suggested corrective action that can be performed to resolve the error condition.

Perform the following procedure to view the active alarms on Avaya MS:

Procedure

1. Navigate to **EM > System Status > Alarms**.

You can set the refresh interval by using the **Refresh every** drop-down menu.

Alarms

Filter [Hide](#)

Customize... Clear

None

Active Alarms

Refresh every: 15 seconds

Id	Severity	Date and Time(CDT)	Description
318	Critical	2011-06-07 11:28:44	MAS instance is not licensed
390	Critical	2011-06-04 11:53:00	Missing License Key
323	Major	2011-06-07 11:28:47	All Configured SIP Routes Are Down

Alarm Details

[Hide](#)

Alarm Id: 390 Severity: Critical Component: MAS License Server

Date & Time: (CDT)2011-06-04 11:53:00

Description: Missing License Key

Probable Cause: There are no licenses keys configured.

Corrective Action: Configure a valid license key.

- Select an alarm that is listed.
The system displays the details at the bottom of the page.
Use the vertical and horizontal scroll bars to view information.
- Click one of the heading names, **Id**, **Severity**, **Date and Time**, or **Description**.
The system sorts and displays alarms in ascending or descending order.
- Click **Customize...** in the upper-right corner of the **Alarms** pane to create a filter for the displayed alarms.

Customize Filter

[Alarm Id](#) | [Severity](#)

Alarm Id

Alarm Ids to exclude: Add... Clear

☒ Id
☒ 323

Severity

Severities to filter out:

Available		Selected
Critical	Add	
Minor	Add All	Major
Warning	Remove	
	Remove All	

Apply Cancel

5. On the **Customize Filter** page, select the **Alarm ID** and the **Severity** types to include, using the **Add** button.
6. Click **Apply** to return to the **Alarms** page with the filtered results.
7. To clear the applied filter, click **Clear** in the upper-right corner of the **Alarms** pane.

Monitor event logs

Event logs provide a historical view of events that occurred in the system.

If required, you can configure Avaya MS to deliver event logs as SNMP traps or SysLog destinations. You need to perform the commissioning procedures for SNMP.

This section describes how to control the age of saved logs, enable or disable log throttling, and apply advanced filters based on log severity and class.

The system also sends a copy of the event logs to the Microsoft Event Viewer, if Avaya MS is on the Windows platform.

EM displays the following information for each alarm:

Event log field descriptions	
Field	Description
ID	A unique identifier assigned to the alarm.
Severity	The Severity color represents the alarm severity. Red indicates Critical and Major alarms and yellow represents all other alarms. The severity of the alarm and can be one of the following (listed from most severe to least) Critical, Major, Minor, and Warning.
Origin	The name of the server reporting the event.
Date and Time	Timestamp of the exact time that the alarm is raised. You can configure timestamps display as either local time or Universal Time Coordinated (UTC) time. UTC time can be useful for correlating alarms with events in other time zones.
Class	The type of information the log is reporting. Class values include Audit, Configuration, Data, Fault, Information, Maintenance, Metrics, Security, and State.

Event log field descriptions	
Field	Description
Category	Always reports a value of General in this release.
Instance Count	The number of times this event occurred when event throttling collects repeated events.
Description	Provides a description of the type of error condition encountered.
Component	The name of Avaya MS software component reporting the alarm.
Probable Cause	A description of what probably caused this event to be raised.
Corrective Action	Suggested corrective action that can be used to resolve the error condition.
Application Id	The application reporting the event.
Customer Id	A custom value set by an application.
Document Reference Link	An optional link to documentation related to the event.

Viewing event logs

About this task

The Event Logs reflect the alarm transitions and state of other system details.

Perform the following procedure to gain access to the saved Avaya MS Event Logs:

Procedure

1. Navigate to **EM > System Status > Logs > Event Logs**.
2. Select an event log.
The system displays the details in the lower part of the page.
Use the vertical and horizontal scroll bars to view information.

Event Logs

Filter [Hide](#)

None [Customize...](#) [Clear](#)

Events Refresh every: No Refresh ▼

[Remove All](#)

☐ Id	☐ Severity	☐ Date and Time(CDT) ▼	☐ Class	☐ Description
☐ 18913	Info	2011-05-17 13:32:50	Info	Element Manager [Status Monitoring
☐ 14600	Critical	2011-05-17 13:32:43	Info	Alarm Activated: Internal Component
☐ 8003	Info	2011-05-17 13:32:43	Info	ConfMP Shutdown Details: ConfMP Sha
☒ 14600	Major	2011-05-17 13:32:43	Info	Alarm Activated: ConfMP MSLINK Inac
☐ 8501	Warning	2011-05-17 13:32:43	Info	Connection Loss
☐ 8004	Info	2011-05-17 13:32:43	Info	Conference shutdown Details: confIc

Page: << < 1 > >> Of 1505

Event Details [Hide](#)

Event Id: 14600 Severity: Major Origin: server4835

Date & Time: (CDT)2011-05-17 13:32:43

Class: Info

Category: General

Instance Count: 1

Description:

- You can set the refresh interval by using the **Refresh every** drop-down menu. The displayed events are sorted in ascending or descending order when you click on one of the heading names: **Id**, **Severity**, **Date and Time (GMT)**, **Class** or **Description**.
- To go back in the history of the Event Logs, use the **Page** navigation buttons.
- Click **Customize...**, in the upper-right corner of the **Event Logs** page, to filter the logs which are displayed.

5. On the **Customize Filter** page, select the **Event Id**, **Date and Time**, **Severity**, and **Class** types to include, using the **Add** button.
6. Click **Apply** to return to the **Event Logs** page with the filtered results.
7. To clear the applied filter, click **Clear** in the upper-right corner of the **Event Logs** page.

Configuring event log throttling

About this task

You can enable and configure event log throttling for a particular event so that the system reports only the most recent event log and its contents. Log throttling prevents the event logs from being flooded with recurring identical events. When you enable throttling, the system

generates an event log and its occurrence count at the end of the interval specified by **Event Log Throttle Check Window (Secs)**.

Procedure

1. Navigate to **EM > System Configuration > Monitoring Settings > Event Logs > General Settings**.

2. Select **Event Log Throttling** to enable log throttling for events.
3. Configure **Event Log Throttle Check Window (Secs)** to set the interval in seconds to audit the throttled logs.
4. Configure **Event Log Archive Minimum Log Age (Days)** to set the minimum time in days to keep an event log before the system deletes the event log.
5. Click **Save**.

Configuring log filter settings

About this task

Each log destination you configure on Avaya MS, whether SNMP, SysLog, and Archive, has filter settings which you can customize independently.

You can filter logs based on the severity and the class where the logs are grouped, as described in the following tables.

Filter options by log severity	
Event type	Description
Emergency	An unusable system.
Alert	An action must be taken immediately.
Critical	An immediate corrective action that is required due to loss of service, loss of

Filter options by log severity	
Event type	Description
	bandwidth, outage, and loss of data or functionality.
Error	An error condition has occurred.
Major	An urgent corrective action that is required due to a pending loss of service, outage, and loss of data or functionality.
Minor	A corrective action is required to prevent an eventual degeneration of services.
Warning	A potential or impending service-affecting condition that is detected that requires some diagnostic action.
Notice	A normal but significant condition.
Indeterminate	A service-affecting condition that is detected whose impact is unknown.
Info	Audit-type information and configuration changes.
Debug	Diagnostic information.

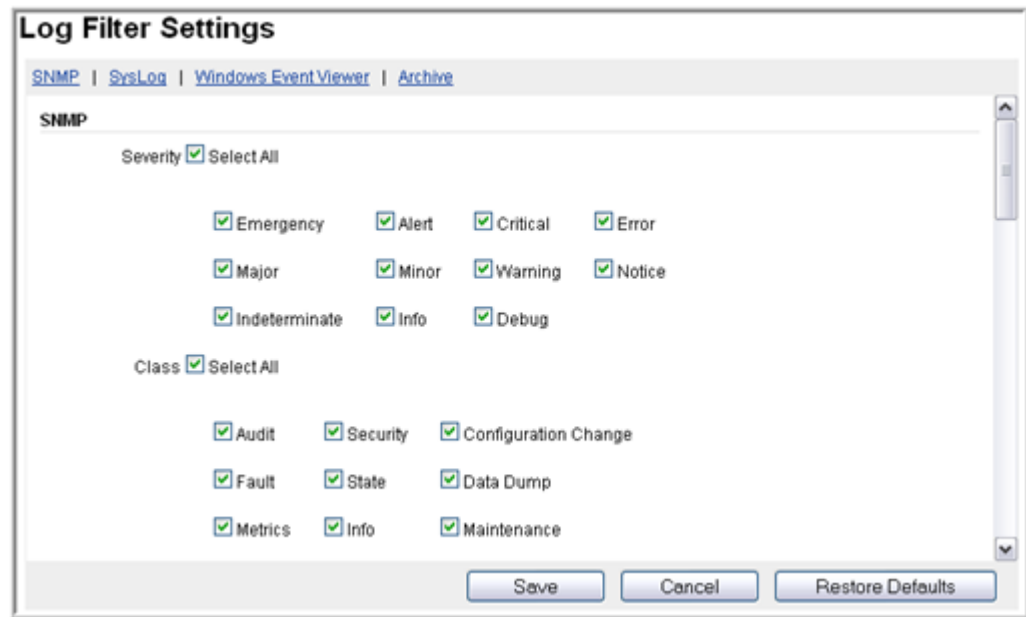
Filter options by log class	
Event type	Description
Audit	Audit events provide notification of very specific actions within a managed device. In isolation, an audit event provides limited data. However, a collection of audit information forms an audit trail.
Security	A security event happens in the interest of security. A security event occurs in the interest of security. A security event is often combined with other classes such as fault and audit to form a record or notification.
Configuration Change	A configuration event, also known as an inventory event, is used to notify the system that hardware, software, or a service has been added, changed, or removed.
Fault	The system generates a fault notification after a fault condition occurs. A fault notification can result in an alarm.
State	A state includes both administrative states that can be manually configured and

Filter options by log class	
Event type	Description
	operational states that are read-only and determined by the managed entity.
Data Dump	A data dump event is an asynchronous event that contains information about a system, such as the configuration and the state. The system generates these events as a result of a scheduled activity. Data dump events are not intended for a traditional poll-response type interaction.
Metrics	A metrics event contains a metric or a collection of metrics, including performance metrics, for an application, platform, or another device or network element. The record can be in a number of different formats, for example, XML, CSV.
Info	An event of interest which requires no action but can be used for troubleshooting purposes.
Maintenance	A maintenance event signals the beginning, process, or end of an action generated either by a manual or an automated maintenance action. Typically, the system reports the actual action initiation and the maintenance action.

Perform the following procedure to configure your log filters for each destination:

Procedure

1. Navigate to **EM > System Configuration > Monitoring Settings > Event Logs > Log Filter Settings**.



2. Scroll down in the window to configure the filters for each destination: **SNMP**, **SysLog**, and **Archive**.
3. Click **Save**.

Viewing security logs

About this task

Using security logs, you can track all configuration changes to the system. Security logs contain details about changes to the system including the exact configuration item that is changed, the old and the new value, the time of the change, and the IP address of the user who made the change.

Perform the following procedure to gain access to the saved Avaya MS Security Logs:

Procedure

1. Navigate to **EM > System Status > Logs > Security Logs**.
2. Select a security log.
The system displays details of the log in the lower part of the page.
Use the vertical and horizontal scroll bars to view information.

The screenshot shows the 'Security Logs' window. At the top right, there is a 'Refresh every:' dropdown menu set to '15 seconds'. Below this is a table with the following columns: 'Date and Time(CDT)', 'Effect', 'Action', 'Functional Task', and 'Item'. The table contains three rows of log entries. Below the table is a pagination bar showing 'Page: 1 of 3' with navigation buttons. At the bottom is a 'Details' pane for the selected event, showing fields like 'Event Id', 'Event Type', 'Origin', 'Date & Time', 'Effect', 'Action', 'Functional Task', and 'Task Path'.

Date and Time(CDT)	Effect	Action	Functional Task	Item
2011-05-17 11:04:08	Configuration Change	Delete	SystemConfig.Signaling.SIP.Nodes	TrustedN
2011-05-17 11:04:04	Configuration Change	Add	SystemConfig.Signaling.SIP.Nodes	TrustedN
2011-05-17 00:00:00	Configuration Change	Delete	Tools:Backup & Restore : History log	clear hist Date:Fri M 2011

Page: 1 of 3

Details

Event Id:18921 Event Type:Info Origin:server4835

Date & Time:2011-05-17 11:04:04

Effect:Configuration Change

Action:Add

Functional Task:SystemConfig.Signaling.SIP.Nodes&Routes:TrustedNodes

Task Path:SystemConfig.Signaling.SIP.Nodes&Routes:TrustedNodes

3. Use the **Refresh every** drop-down menu to refresh interval.
4. To move back further in the history of the **Security Logs**, use the **Page** navigation buttons.

Configuring SysLog settings

About this task

Perform the following procedure to enable the delivery of SysLog events and configure the destination server that receives the SysLog events:

Procedure

1. Navigate to **EM > System Configuration > Logging Settings > SysLog**.

Logging Settings

[SysLog](#) | [Session Logging](#) | [QMS](#)

SysLog

SYSLOG Delivery of Logs: ☒

SYSLOG Destination Server List:

Server Address	Port (0 - 65535)
135.60.66.12	514

2. Select **SYSLOG Delivery of Logs** to enable delivery of SysLogs.
3. Click **Add** to add destination server to **SYSLOG Destination Server List**.
4. Enter the IP address and the port of the destination server in text boxes in the **Server Address** and **Port** columns.
5. Click **Save**.
6. Click **Confirm**.
7. Restart the system for the changes to take effect.

Monitor active sessions

This section describes the procedures for monitoring Active Sessions on Avaya MS and for customizing the Active Sessions monitor display.

Viewing current active sessions

About this task

The active session display has several features you can use to find sessions of interest and to obtain detailed information related to each session, including the SIP messaging.

The default view of the **Active Sessions** pane in EM shows an unfiltered list of the active sessions. The unfiltered list can be a list of sessions only on one node or across the entire cluster. You can define a filter with very specific criteria to find sessions of interest. Additionally, you can specify a refresh interval to define how often the system updates the display with current sessions and whether the system needs to display timestamps in GMT time or local time.

Perform the following procedure to use all the features:

Procedure

1. Navigate to **EM > System Status > Monitoring > Active Sessions**.
If the system prompts, follow the onscreen instructions to download and install Microsoft Silverlight.

*** Note:**

You must install Microsoft Silverlight to use this feature.

2. On the **Active Sessions** page, you can see a summary of resources that any current active session is consuming.
Use the horizontal scroll bars to view information.

Remote Party	Start Timestamp	Application Name	Endpoint	QOS R-Factor	QOS Round Trip Time
"Paul"<slp:pd@avaya.com>	4/27/2011 10:45:18 AM	RFC4240	Nortel PCC 7.4.40	91	66
"David"<slp:dm@avaya.com>	4/27/2011 10:45:36 AM	RFC4240	Nortel PCC 7.4.40	91	62

3. Use the **Refresh** button and refresh interval drop-down menu to set the update frequency for the display.
4. To find a particular session, use the **Filter** drop-down menu to select a filter type, and then enter the matching criteria in the **Criteria** field under the selected filter.
5. To disable filtering and show all the active sessions, select **None** from the **Filter** drop-down list.
6. To display the active session timestamps using the local time, click **Select... > Display All Timestamps In Local Time**.
7. To display the active session timestamps using Greenwich Mean Time (GMT), clear **Display All Timestamps In Local Time** in the **Select...** drop-down menu.
8. To toggle the active sessions view between cluster-wide view and nodal view, click the **(Cluster)** toggle button on the upper-right corner of the **Active Sessions** pane.
The **(Cluster)** toggle button is present only if you have configured a cluster.

If you click **(Cluster)** to enter the cluster aggregated view, the button name changes to the host name of the local server.

Viewing details for a specific session

About this task

The **Active Sessions** page is a useful debugging tool when you encounter difficulties. There are options available to collect data for analysis. These options include graphical SIP message flows and SIP traces which show the details of the messages for a particular session.

Perform the following procedure to collect a message trace of a session:

Procedure

1. Setup trace monitoring by navigating to **EM > System Status > Monitoring > Active Sessions**.

In the content pane of EM, the system displays the Active Sessions page.

If prompted, follow the onscreen instructions to download and install Microsoft Silverlight.

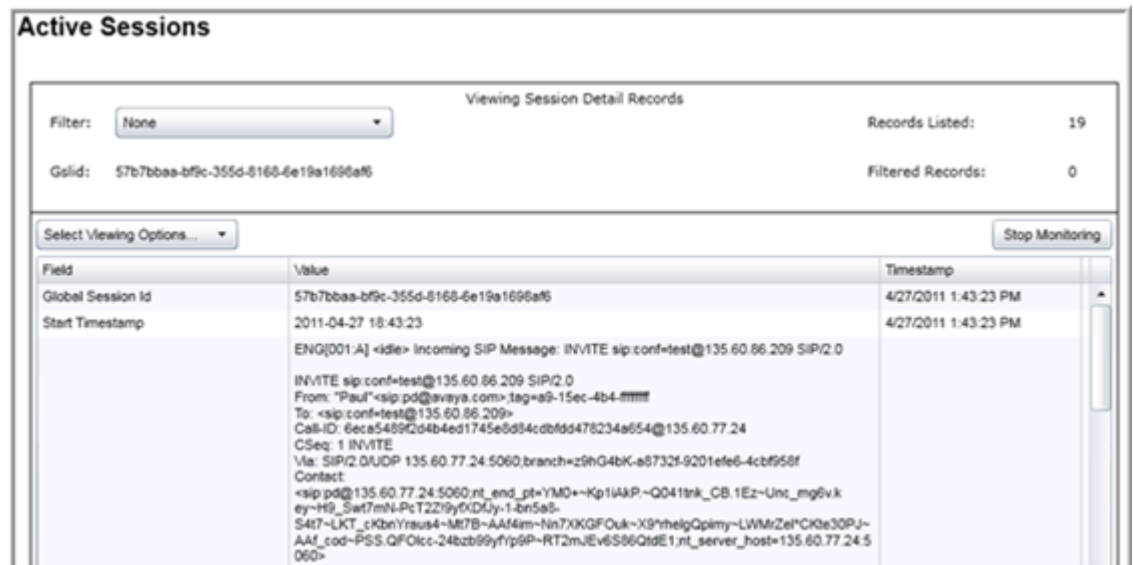
Note:

You must install Microsoft Silverlight to use this feature.

2. From the **Select...** drop-down menu, select **Monitor Next Session**.
The system displays a message that the system is waiting for a new session to start.
3. Ensure **Display Trace Records** is selected in the **Select...** drop-down menu.
After the next session begins, the system displays the **Active Sessions** window with a detail call performance summary.



4. To view session records of the call including SIP message content, select **Select Viewing Options... > View Session Detail Records**.



5. Change the view to a graphical, SIP message flow by selecting **Select Viewing Options... > View SIP Protocol Trace**.



6. Click **Stop Monitoring** to end tracing for this session.

Releasing one or more sessions

About this task

Perform the following procedure to release one or more active sessions on the server:

Procedure

1. Navigate to **EM > System Status > Monitoring > Active Sessions**.
If the system prompts, follow the onscreen instructions to download and install Microsoft Silverlight.

* Note:

You must install Microsoft Silverlight to use this feature.

2. As described in this section, apply filters to find the session you need to quit.
3. Select the session or sessions that you want to release from the list of **Active Sessions** that the system displays.

+ Tip:

To select multiple active sessions, hold down either the **Shift** key for multiple selections which are grouped together or the **Control** key for multiple selections which are separated and then click the sessions you want to end.

4. From the **Select...** drop-down menu, select **Release Selected Session**.

The sessions are removed from the **Active Sessions** list after the system releases the active sessions and refreshes the display.

Muting and unmuting sessions

About this task

Perform the following procedure to mute or unmute one or more active sessions listed on the Active Sessions display page:

 Note:

You can mute or unmute active sessions only if the current application supports this option otherwise the option is unavailable.

Procedure

1. Navigate to **EM > System Status > Monitoring > Active Sessions**.

If the system prompts, follow the onscreen instructions to download and install Microsoft Silverlight.

 Note:

You must install Microsoft Silverlight to use this feature.

2. As described in this section, apply filters to find the sessions you need to mute or unmute.
3. Select the session or sessions that you want to mute or unmute from the list of active sessions that the system displays.

 Tip:

To select multiple sessions, hold down either the `Shift` key for multiple selections which are grouped together or the `Control` key for multiple selections which are separated and then click the sessions you want to mute or unmute.

4. From the **Select...** drop-down menu, select **Mute Selected Session** or **Unmute**.
-

Monitoring system performance

About this task

You can monitor system performance by comparing the number of sessions with the CPU utilization.

The system displays a summary of the current system performance graphically on the **Performance** page of EM.

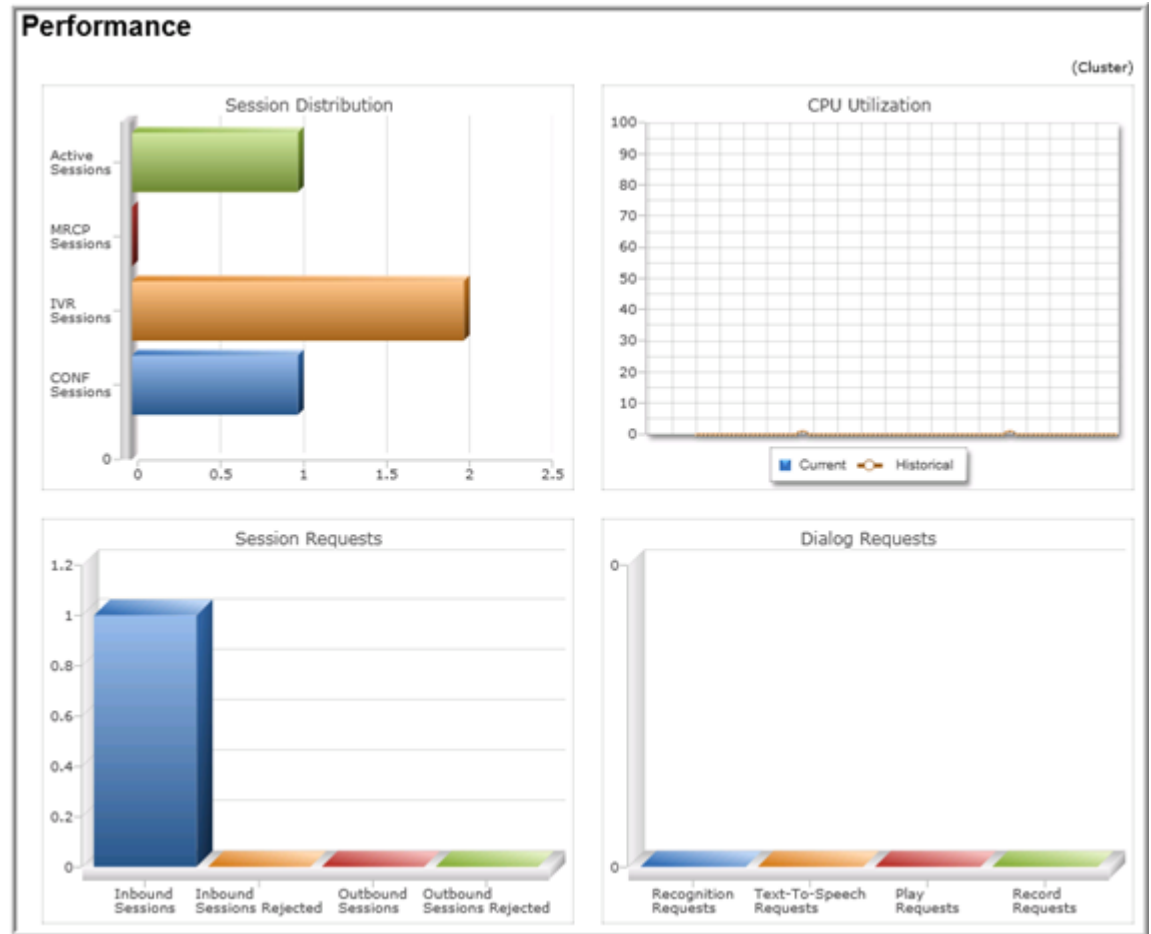
Procedure

1. Navigate to **EM > System Status > Monitoring > Performance**.

If the system prompts, follow the onscreen instructions to download and install Microsoft Silverlight.

Note:

You must install Microsoft Silverlight to use this feature.



- To monitor the aggregated performance of the cluster or the performance of only the current server, click **(Cluster)** on the upper-right corner of the **Active Sessions** pane.

This option is available only if you have configured a cluster.

OM monitoring

Configuring OM settings

About this task

Perform the following procedure to choose the Operational Measurements (OM) that are available for Archiving, Monitoring, Delivery and the OM that are used as Key Performance Indicators (KPI):

Procedure

1. Navigate to **EM > System Configuration > Monitoring Settings > Operational Measurements > Settings**.

Operational Measurements Settings

Category: MAS Conference Media Processor CmdUnjoin Find Next

Please enter OM's name and press find next to see this OM first in the table

Name	Archive	Monitor	KPI	Delivery
Processor CmdUnjoin	☐	☒	☐	☒
Processor Conference Cmd Error Unknown	☐	☒	☒	☒
Processor Conference VQMonCriticalEvents	☐	☒	☐	☐
Processor Conference VQMonSuppressedAlerts	☒	☒	☒	☒
Processor Conference VQMonWarningEvents	☒	☒	☒	☒
Processor ConfMP Number of dropped packets	☒	☒	☒	☒
Processor ConfMP NWTimer lost intervals, total	☒	☒	☒	☒
Processor ConfMP NWTimer lost single interval	☐	☒	☐	☐
Processor ConfMP NWTimer lost 2 intervals	☐	☒	☐	☐
Processor ConfMP NWTimer lost 3 intervals	☐	☒	☐	☐
Processor ConfMP NWTimer lost 4 intervals	☐	☒	☐	☐

Save Cancel

+ Tip:

- You can sort the columns by clicking on the column name.
- You can filter the displayed OMs by selecting a category from the **Category** drop-down menu.
- If you know the name of the OM to configure, type the name in the field to the left of the **Find Next** button and then press **Enter** or click **Find Next**.

- You can use the check box next to the column title to select or deselect all OMs listed in that column.
2. On the **Operational Measurement Settings** page, select the check box in the **Archive** column next to each OM to archive.
 3. Select check boxes in the **Monitor** column next to each OM that you want to monitor.
 4. Select the check boxes in the **KPI** column next to each OM that you want to appear in **System Performance Summary** which is located at **EM > System Status > Cluster Status > System Performance Summary**.
 5. Select the check box next to the OM in the **Delivery** column to indicate which OMs to deliver as periodic comma-separated values (CSV) reports.
 6. Click **Save**.
-

Configuring OM delivery

About this task

Perform the following procedure to configure how the system delivers OM reports using FTP (File Transfer Protocol) or SFTP (Secure FTP):

Procedure

1. Navigate to **EM > System Configuration > Monitoring Settings > Operational Measurements > Delivery**.

Delivery

This task allows administrators to view and modify operational measurements (OMs) delivery settings.

Periodic Performance Report Delivery: ☒

Report ZIP Compression: ☒

FTP Report Delivery: ☒

FTP Server Network Address: (1 - 256 characters)

FTP Remote Directory: (maximum: 256 characters)

FTP Account Username: (6 - 32 characters)

FTP Account Password: (6 - 32 characters)

Secure FTP (SFTP): ☒

Secure FTP Remote Server Fingerprint: (maximum: 2048 characters)

Secure FTP Key File Name: (maximum: 256 characters)

2. Select **Periodic Performance Report Delivery** to enable performance report delivery for FTP or SFTP.
3. Select **Report ZIP Compression** to create a .zip file of the OM reports.
4. Select **FTP Report Delivery** to deliver reports using FTP.
5. In the **FTP Server Network Address** field, enter the address of the destination FTP server.
6. In the **FTP Remote Directory**, enter the address of an optional remote directory to change to before uploading the report.
7. In the **FTP Account Username** field, enter the FTP user name to use at the destination FTP server.
8. In the **FTP Account Password** field, enter the FTP password to use at the destination FTP server.
9. (Optional) Select the **Secure FTP (SFTP)** check box and then configure the SFTP options:
 - a. In the **Secure FTP Remote Server Fingerprint** field, enter the fingerprint of the remote server.
 - b. In the **Secure FTP Key File Name** field, enter the file name to use as the optional SFTP key file.
10. Click **Save**.
11. Restart the system for the changes to take effect.

Configuring OM archiving

About this task

Perform the following procedure to archive OM and to configure OM retention options:

Procedure

1. Navigate to **EM > System Configuration > Logging Settings > OMs**.

Logging Settings

[SysLog](#) | [Session Logging](#) | [OMs](#)

OMs

Archive Operational Measurements: ☒

Operational Measurement Archive Minimum Record Age: (1 - 365 days)

Operational Measurement Archive Cleanup Threshold Size: (0 - 50,000,000 bytes)

Operational Measurements Reset Interval: (0 - 60 minutes)

2. Select **Archive Operational Measurements** to enable OM archiving.
3. In the **Operational Measurement Archive Minimum Record Age** field, specify the number of days after which the system needs to archive OMs.
When the system initiates a cleanup, the system deletes all archived OMs older than the specified days.
4. In the **Operational Measurement Archive Cleanup Threshold Size** field, enter the maximum space in bytes for OMs to use before the system initiates a cleanup.
5. In the **Operational Measurements Reset Interval** field, set the interval in minutes at which the system archives and resets OMs.
6. Click **Save**.
7. Click **Confirm**.
8. Restart the system for the changes to take effect.

Monitoring protocol connections

About this task

Perform the following procedure to view operational information about installed protocols:

Procedure

1. Navigate to **EM > System Status > Monitoring > Protocol Connections**.
2. You can set the refresh interval using the **Refresh every** drop-down menu.
View the information for the installed protocols using the vertical and horizontal scroll bars and by clicking the title of any column to change the ordering of the connection list. You cannot perform any action. The display is informational only.

Application Protocol	Transport Protocol	Type	IP Version	State	Status	Source Address
MRCPv1	TCP	Client	IPv4	Connected	Normal	135.60.77.150
MRCPv1	TCP	Client	IPv4	Connected	Normal	135.60.77.150

Advanced system monitoring

Viewing component status

About this task

Perform the following procedure to view the operational state of individual Avaya MS components:

Procedure

Navigate to **EM > System Status > Monitoring > Advanced > Component Status**.

In the content pane of EM, the **Component Status** page displays information about the operational state of individual components of Avaya MS.

You cannot perform any actions on the listed components. The information is useful for diagnosing and isolating system problems when working with Avaya support.

Component Status				
Component Name	Type	States	Status	TimeStamp(CDT)
MAS Resource Manager	SRP	Running	Healthy	2011-05-17 13:32:55
MAS SIP UserAgent	SRP	Running	Healthy	2011-05-17 13:32:53
MAS IVR Media Processor	SRP	Stopped	Failed Repeatedly	2011-05-17 13:32:55
MAS Conference Media Processor	SRP	Running	Healthy	2011-05-17 13:32:53
MAS Content Store	SRP	Running	Healthy	2011-05-17 13:32:53
MAS Streaming Source	SRP	Running	Healthy	2011-05-17 13:32:53
MAS Management SOAP Server	SRP	Running	Healthy	2011-05-17 13:32:53
MAS Reporting Agent	SRP	Running	Healthy	2011-05-17 13:32:53

Viewing advanced protocols

About this task

Perform the following procedure to view the status of various media server protocol interfaces:

Procedure

1. Navigate to **EM > System Status > Monitoring > Advanced > All Protocol Connections**.
The system displays information about the operational state of protocols on Avaya MS.
 2. You can set the refresh interval using the **Refresh every** drop-down menu.
 3. To restrict the display to certain protocols, select protocol from the **Display** drop-down list.
You cannot perform any action. The information is useful for diagnosing and isolating system problems when working with Avaya support.
-

System license monitoring

Monitoring License Server status

About this task

Perform the following procedure to start, stop, restart, or view the status of a License Server:

You can perform the procedure for systems that use License Server configurations and not for systems that use Nodal Licensing or WebLM licensing.

Procedure

1. Navigate to **EM > Licensing > Server Status**.
View the status of the primary license server.
If you have already configured the secondary license server, view the status of the server.
 2. Select a refresh rate for this page using the **Refresh every** drop-down menu.
 3. Change the state of the License Server as follows:
 - To start the License Server, click **Start**.
 - To stop the License Server, click **Stop**.
 - To restart the License Server, click **Restart**.
 4. Click **Confirm**.
-

SDR monitoring

Avaya MS sessions generate Session Detail Records (SDRs) which capture detailed information about each session. EM provides an SDR Browser which you can use to review the details of any session that the media server handles.

Perform the following procedures to filter and review SDRs, generate graphical reports of sessions for traffic pattern analysis, and view peak Avaya MS traffic:

Reviewing SDRs

About this task

Perform the following procedure to filter and review the details of any sessions archived by the media server:

Procedure

1. Navigate to **EM > Tools > Session Detail Record Browser** to browse SDRs.

Session Detail Record Browser

Query (NT1004002403)

Type: **Browse Records In Date Range** Limit: 100 6/9/2011 3:16:31 PM Central Standard Time

Start: 6/9/2011 12:00:00 AM ☒ Use Local Time

End: 6/9/2011 11:59:59 PM **Execute**

Global Session Id	Start Timestamp	End Timestamp	Server
-------------------	-----------------	---------------	--------

2. Select **Browse Records In Date Range** query type from the **Type** drop-down menu.
3. Use the **Start** and the **End** options in the **Query** panel to define a time range for a query.
4. Enter the maximum number of results in the **Limit** field.
5. Click **Execute** to run the query.
The system displays the list of sessions.
6. Click one of the rows in the list of sessions.
7. Scroll down to review the details of that session in the **Session Detail Records** panel.

Session Detail Record Browser

Query (server4803)

Type: Browse Records In Date Range Limit: 100 4/27/2011 11:27:34 AM Central Standard Time

Start: 4/26/2011 15 7:00:00 PM ☒ Use Local Time

End: 4/28/2011 15 11:59:59 PM Execute

Global Session Id	Start Timestamp	End Timestamp	Server
a638f32-2e9c-3bb7-af3e-b1cb0d80db5c	4/27/2011 10:45:18 AM	4/27/2011 10:56:34 AM	server4803
0f5061f5-374a-3b1b-97f5-860176c50a8b	4/27/2011 10:45:36 AM	4/27/2011 10:48:26 AM	server4803
a35ce6a7-a063-3627-860c-3164de7d57fb	4/27/2011 10:13:44 AM	4/27/2011 10:44:38 AM	server4803
ef7e39c5-a6e2-33cf-88c1-667c78d1f7f4	4/27/2011 9:20:04 AM	4/27/2011 9:20:04 AM	server4803

Result

Session Detail Records

Filter: None ☒ Display Trace Details

Field	Value	Timestamp
Global Session Id	0f5061f5-374a-3b1b-97f5-860176c50a8b	4/27/2011 10:45:36 AM
Start Timestamp	2011-04-27 15:45:36	4/27/2011 10:45:36 AM
Server	server4803	4/27/2011 10:45:36 AM
SiP Remote User Information	"David"<slp:dm@avaya.com>	4/27/2011 10:45:36.522 AM
Application Name	RFC4240	4/27/2011 10:45:36.523 AM

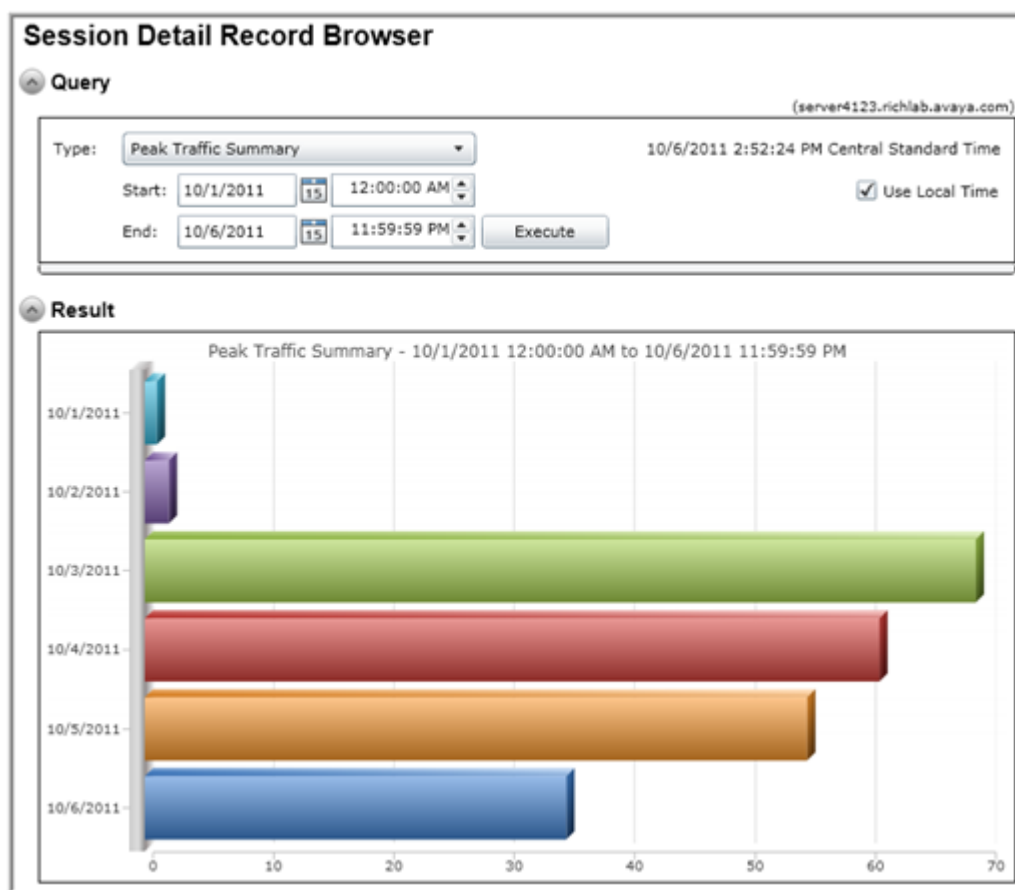
Determining peak session traffic

About this task

Perform the following procedure to generate a graphical report representing of the peak number of sessions Avaya MS processes each day:

Procedure

1. Navigate to **EM > Tools > Session Detail Record Browser**.
2. To run a query which reports the peak number of sessions on each day, select **Peak Traffic Summary** from the **Type** drop-down menu.
3. Use the **Start** and the **End** options in the **Query** panel to define a time range for the query.
4. Click **Execute** to run the new query and generate a graphical **Peak Traffic Summary**. Move your cursor over any bar graph element to see the peak number of sessions for each day.



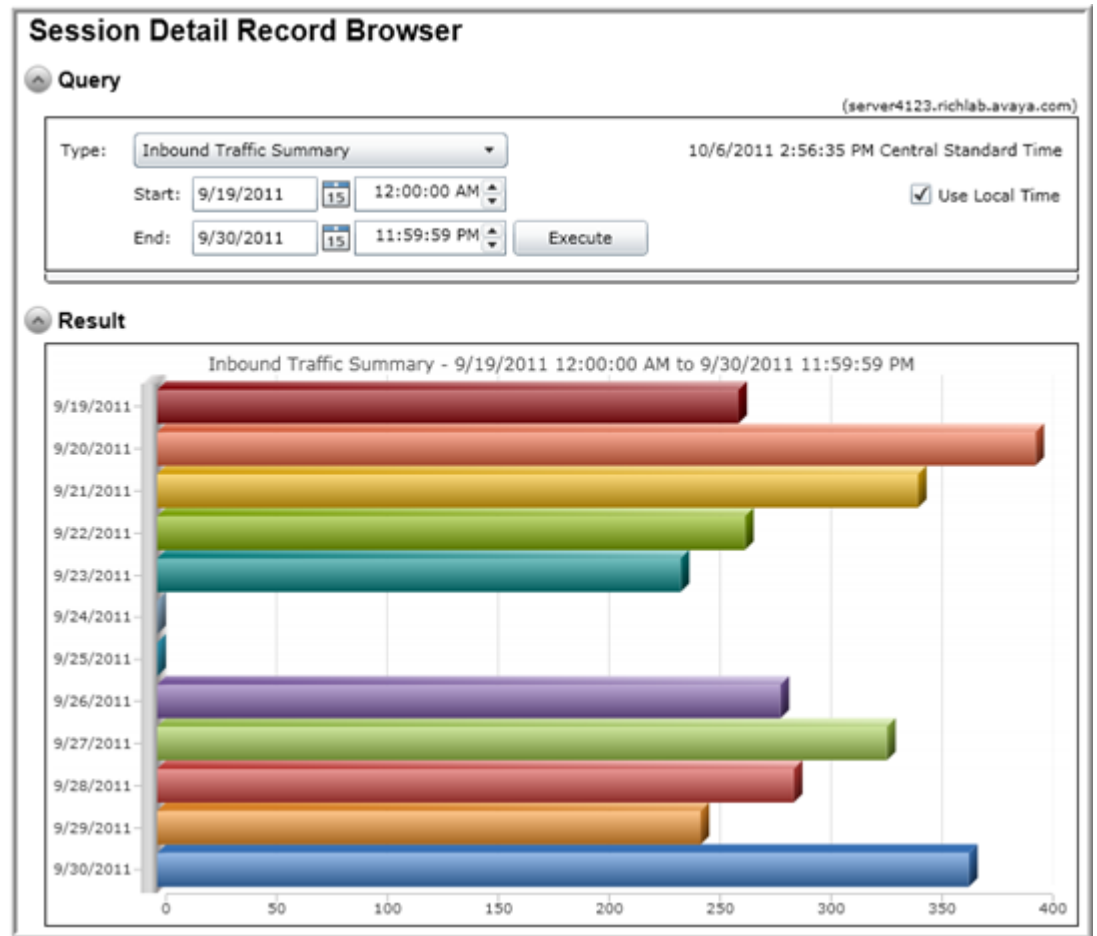
Summarizing daily inbound traffic

About this task

Perform the following procedure to generate graphical reports which summarize daily inbound traffic that Avaya MS processes:

Procedure

1. Navigate to **EM > Tools > Session Detail Record Browser**.
2. To run a query which reports the total number of sessions for each day, select **Inbound Traffic Summary** from the **Type** drop-down menu.
3. Use the **Start** and the **End** options in the **Query** panel to define a time range for the query.
4. Click **Execute** to run the new query and generate a graphical **Inbound Traffic Summary**. Move your cursor over any bar graph element to see the total number of sessions handled for each day.



Analyzing hourly inbound traffic details

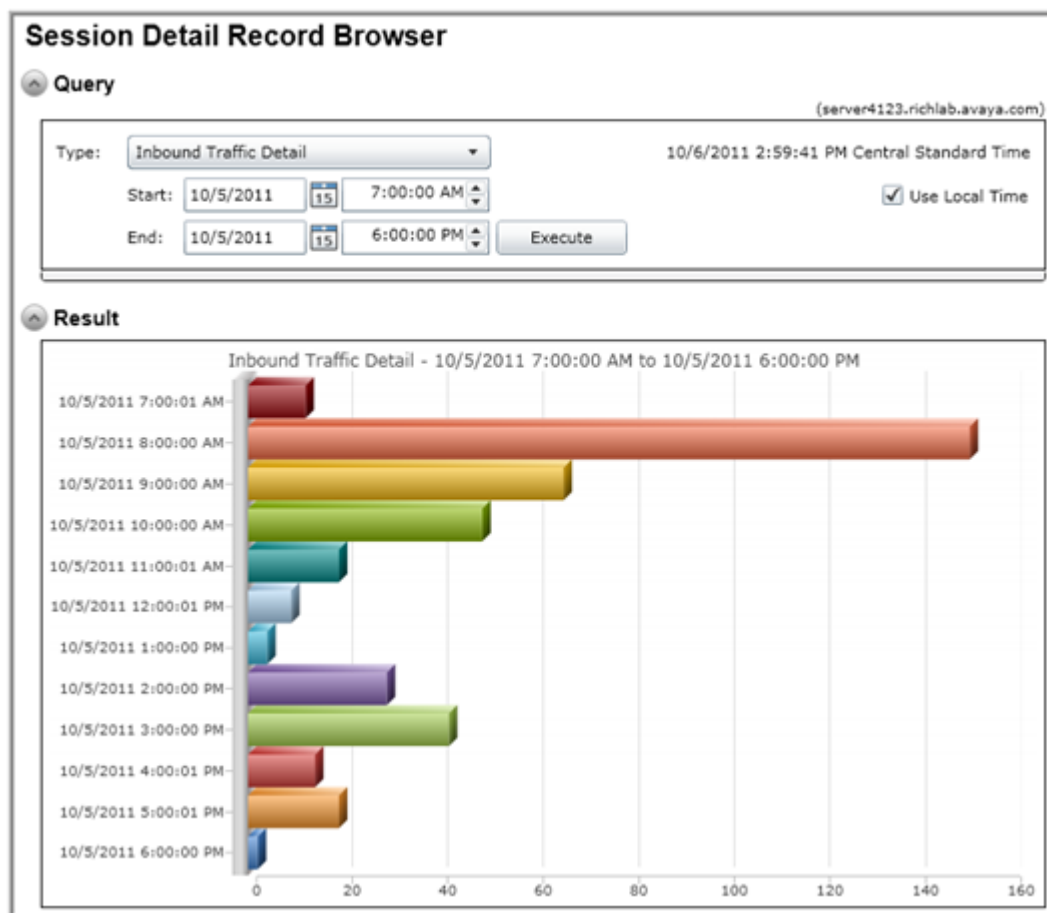
About this task

Perform the following procedure to generate graphical reports for determination of hourly traffic that Avaya MS processes:

Procedure

1. Navigate to **EM > Tools > Session Detail Record Browser**.
2. To run a query which details the total number of inbound sessions by hour, select **Inbound Traffic Detail** from the **Type** drop-down menu.
3. Use the **Start** and the **End** options in the **Query** panel to define a time range for the query.

- Click **Execute** to run the new query and generate a graph showing hourly inbound session totals. Move your cursor over any bar graph element to see the number of sessions recorded for that hour.



Reviewing a monitored SDR

Before you begin

Perform the procedure for Viewing details for a specific session to add a detailed SDR to the archive and then perform the following procedure:

About this task

A session which is traced using the session monitoring procedure produces a more detailed SDR. The SDR browser shows additional information for these monitored sessions which includes:

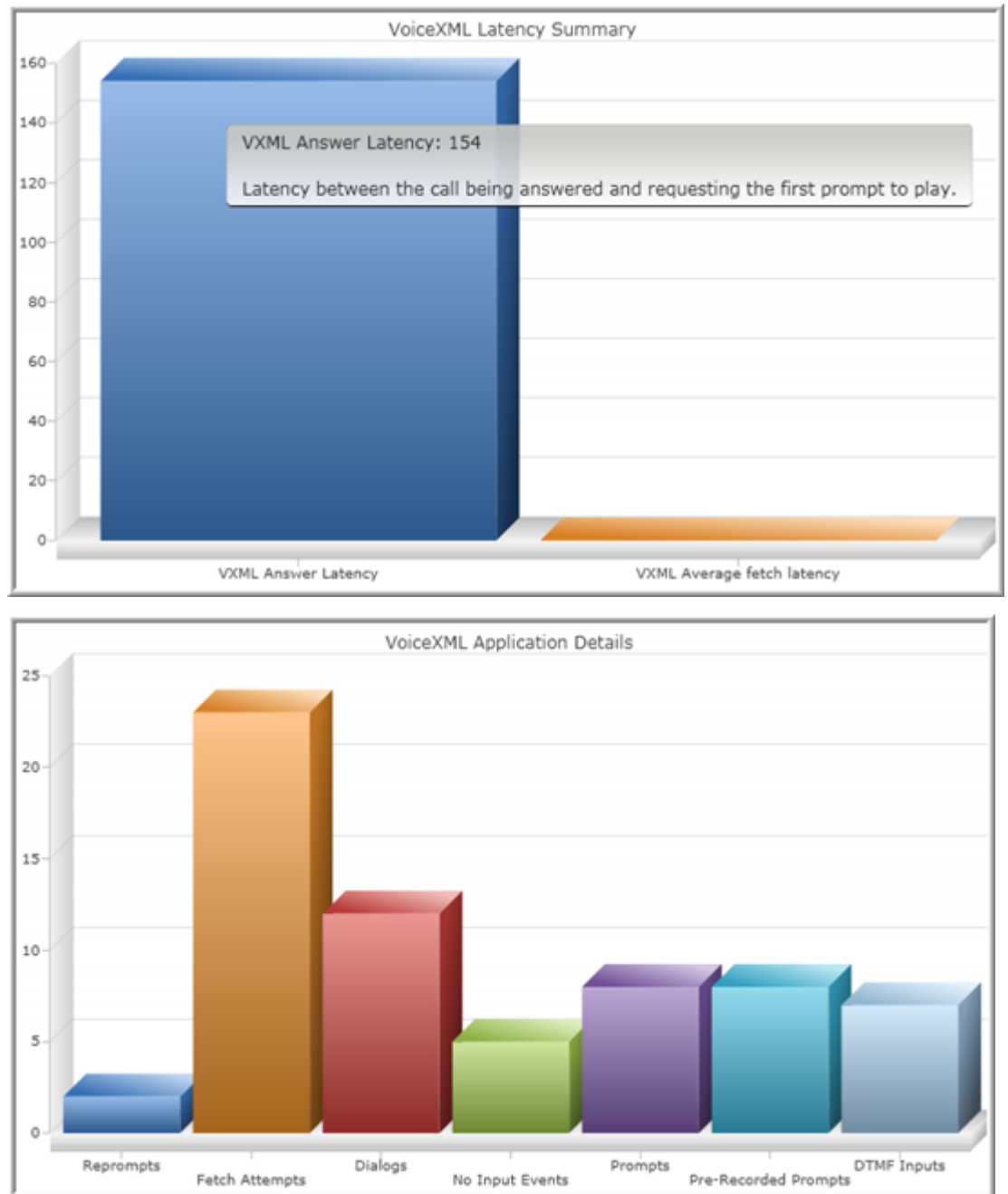
- Detailed SIP and Application log records.
- Operational measurement graphs specific to the session.
- A graphical SIP message flow.

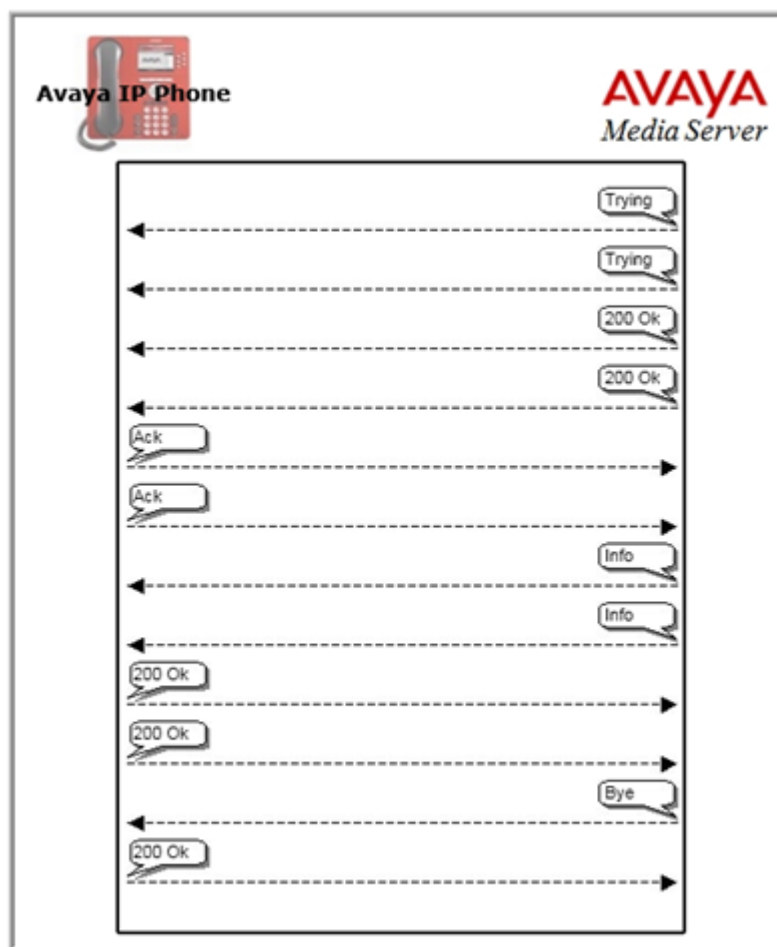
Perform the following procedure to review the detailed SDR of a monitored session.

Procedure

1. Navigate to **EM > Tools > Session Detail Record Browser** to browse SDRs.
2. Select **Browse Records In Date Range** as the query type, from the **Type** drop-down menu.
3. Use the **Start** and the **End** options in the **Query** panel to define a narrow time range for the query which includes the monitored session.
4. In the **Limit** field, enter the maximum number of results that you want to view.
5. Click **Execute** to run the query.
The system displays the list of sessions corresponding to the monitored session.
6. Click the result row in the list of sessions.
7. Scroll down to review the details of the session as shown in the following examples.

Session Detail Records		
Filter: None		☐ Display Trace Details
Field	Value	Timestamp
Global Session Id	55ade94b-3e52-4867-8aa7-dfef5ad0f46e	10/6/2011 3:47:47 PM
Start Timestamp	2011-10-06 20:47:47	10/6/2011 3:47:47 PM
Server	server4123.richlab.avaya.com	10/6/2011 3:47:47 PM
SIP Remote User Information	"Paul Divita"<sip.pdivita@avaya.com>	10/6/2011 3:47:47.315 PM
SIP Audio Remote IP Address	135.60.69.38	10/6/2011 3:47:47.315 PM
SIP Audio Remote IP Port	50014	10/6/2011 3:47:47.315 PM
Application Name	ucomm	10/6/2011 3:47:47.316 PM
Application URL	file:///var/mcp/ma/MAS/platedata/Applications/v/xml/ucomm/msg-route/ucomm.xml	10/6/2011 3:47:47.316 PM
SIP Remote User-Agent	Nortel IP Phone 11xx (SIP1140e.03.01.12.00)	10/6/2011 3:47:47.316 PM
SIP Locale	en_US	10/6/2011 3:47:47.316 PM
SIP Original Destination	<sip:4502@avaya.com>	10/6/2011 3:47:47.316 PM
SIP CALL ID	e6eedfad23bc74aa1745e8d8503ef29a181f45e16@135.60.77.24	10/6/2011 3:47:47.316 PM
SIP Audio Codec	PCMU	10/6/2011 3:47:47.319 PM
SIP Audio Packet Interval	20	10/6/2011 3:47:47.319 PM
SIP Audio Local IP Address	135.60.77.12	10/6/2011 3:47:47.319 PM
SIP Audio Local IP Port	6146	10/6/2011 3:47:47.319 PM
VXML Longest Fetch URL		10/6/2011 3:47:47.364 PM
VXML Worst Recognition URL		10/6/2011 3:47:47.364 PM
Application Log	Prepared Query: <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:urn="http://xml.avaya.com/ws/ams/oaam/v1_0/"> <soapenv:Header/> <soapenv:Body> <urn:ListConfiguration> <Gslid>55ade94b-3e52-4867-8aa7-dfef5ad0f46e</Gslid> <Group>Application</Group> <Locale>en_US</Locale> <CategoryOrKey>497091d6-b899-102a-97fb-541673fc9806</CategoryOrKey> </urn:ListConfiguration> </soapenv:Body> </soapenv:Envelope>	10/6/2011 3:47:47.399 PM
Application Log	configData.DEFAULT_LOCALE: en_us	10/6/2011 3:47:47.405 PM





Related topics:

[Viewing details for a specific session](#) on page 172

Configuring SDR archiving

About this task

The system creates SDRs for each session. You can review the archived SDRs using an SDR browser. You can also clear all the records in the current archive.

Perform the following procedure to enable the archiving of SDRs, configure the desired retention options, and clear all the records in the current archive:

Procedure

1. Navigate to **EM > System Configuration > Logging Settings > Session Logging**.

Logging Settings

[SysLog](#) | [Session Logging](#) | [QMS](#)

Session Logging

Session Detail Record Archiving: ☒

Session Detail Record Archive Minimum Record Age: (1 - 365 days)

Session Detail Record Archive Cleanup Threshold Size: (0 - 50,000,000 bytes)

Clear Session Detail Record Archive:

2. Select **Session Detail Record Archiving** to enable SDR archiving.
3. In the **Session Detail Record Archive Minimum Record Age** field, specify the number of days after which the system archives SDRs.
When the system initiates a cleanup, the system removes SDRs older than the configured number of days.
4. In the **Session Detail Record Archive Cleanup Threshold Size** field, enter the maximum space, in bytes, for SDRs to use before the system initiates a cleanup.
5. (Optional) Click **Clear** to delete all currently archived records.
6. Click **Save**.
7. Click **Confirm**.
8. Restart the system for the changes to take effect.

Configuring Field Promotion for SDR reports

About this task

Perform the following procedure to select the fields to include in SDRs:

Procedure

1. Navigate to **EM > Element Status** and select **Lock** from the **More Actions** drop-down menu and click **Confirm** to lock the system.
For more information on locking your system, see [Setting the operational state](#).

Important:

When you lock the media server, the system ends existing sessions, does not accept new requests, and redirects new traffic to other nodes in the cluster.

2. Navigate to **EM > System Configuration > Session Detail Records > Field Promotion**.

Field Promotion

Available Fields

Add
Add All
Remove
Remove All
Up
Down

Selected Fields

Field Name	Indexed	Field Definition	Definition Size

Save Cancel

3. Select the required fields from the **Available Fields** and then click **Add**.
The system displays the selected fields in the **Selected Fields** column and in the table on the lower part of the page.

+ Tip:

To select multiple items, press **Shift** key for multiple selections which are grouped together or **Control** key for multiple selections which are separated, and then click the required items.

Field Promotion

Available Fields

Add
Add All
Remove
Remove All
Up
Down

Selected Fields

Field Name	Indexed	Field Definition	Definition Size
QOS Mean Jitter (msec)	No	Integer	
QOS Round Trip Delay (msec)	No	Integer	
No Match Events	Yes	Operational Measurements	

Save Cancel

4. To reorder the fields in **Selected Fields**, select a field and then click **Up** or **Down**.
5. In the **Indexed** column, select **Yes** or **No** as required.
6. If you want to remove any selected field, click on the field in the **Selected Fields** and then click **Remove**.

Related topics:

[Setting the operational state](#) on page 29

Enabling enhanced SDRs for troubleshooting

About this task

You can enhance SDRs to capture additional detail to aid in system troubleshooting. When you select **Enable System Diagnostic Mode**, the system adds additional fields and full SIP message traces to the SDRs. The EM Active Sessions viewer and SDR browser display these additional details. Additional tracing is useful during trials and system commissioning.

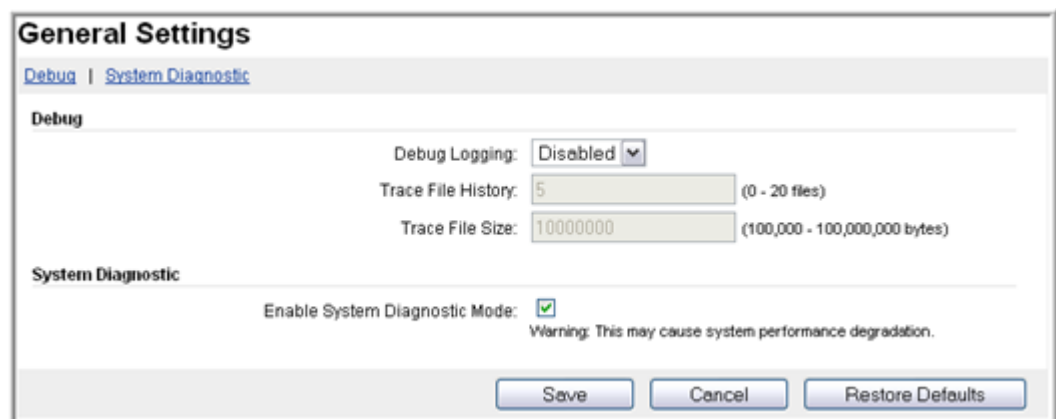
Important:

The collection of additional SDR data impacts system performance. Do not select **Enable System Diagnostic Mode** on live systems processing traffic. Ensure you clear **Enable System Diagnostic Mode** when you have finished troubleshooting.

Perform the following procedure to enable enhanced SDR tracing:

Procedure

1. Navigate to **EM > System Configuration > Debug Tracing > General Settings > > System Diagnostic**.
2. Select **Enable System Diagnostic Mode**.



The screenshot shows the 'General Settings' dialog box with the 'System Diagnostic' tab selected. Under the 'Debug' section, 'Debug Logging' is set to 'Disabled', 'Trace File History' is '5' (0 - 20 files), and 'Trace File Size' is '10000000' (100,000 - 100,000,000 bytes). Under the 'System Diagnostic' section, 'Enable System Diagnostic Mode' is checked. A warning message states: 'Warning: This may cause system performance degradation.' At the bottom are 'Save', 'Cancel', and 'Restore Defaults' buttons.

3. Click **Save**.

4. Click **Confirm**.

5. Restart the system for the changes to take effect.

To view an enhanced trace of sessions that Avaya MS processes after the restart, use the SDR browser as described in [Reviewing session detail records](#) or use the Active Sessions viewer as described in [Viewing current active sessions](#).

Related topics:

[Reviewing session detail records](#) on page 23

[Viewing current active sessions](#) on page 170

Chapter 9: Troubleshooting

Introduction to troubleshooting

By performing troubleshooting, you can provide possible solutions for common Avaya Media Server (MS) problems. Each troubleshooting topic provides the description of the problem, possible cause, and potential solution to the problem, using which you can solve the problem.

Element Manager troubleshooting

Cannot log in to EM after installation on Linux

After installation on a Linux system, you cannot log in to Element Manager (EM) using the system login account.

A possible cause is that you did not properly configure the local login settings for EM during the installation.

If you get the following EM login error message, then the **PasswordAuthentication** of the server in the SSH configuration might be disabled.

```
Login error. Could not authenticate through SSH server!
```

Another possible cause is that the firewall blocks the TCP ports the EM requires.

Proposed Solutions

Checking the user group

About this task

Perform the following procedure to ensure that the group the user belongs to is included in the authenticable groups list:

Procedure

1. Use a Linux shell on Avaya MS, and change to the following directory:
`cd $MASHOME/../../apache-tomcat/mas/conf`
2. Edit the `local-accounts.properties` file and check the `locallogin.authenticable.groups` settings.
 For example, if the group for the system login account is `root`, the settings is as follows:
`locallogin.authenticable.groups=root`
3. If the group to which the system login account belongs is not listed in the value, add the group.
 Use semicolons to separate multiple values.
4. Save the change.
5. Restart the Avaya EM Service after the change.

Checking PasswordAuthentication

Before you begin

Ensure PasswordAuthentication is enabled.

Procedure

1. Use a Linux shell on Avaya MS to change to root user by running the following command:
`su -`
2. Edit the appropriate file for your system:
`/etc/ssh/sshd_config` or `/etc/ssh/sshd_config`.
3. Change the value of PasswordAuthentication to `yes`.
4. Save the change to the file.
5. Restart SSHD using the appropriate command for your system:
`/etc/init.d/sshd restart` or `/etc/init.d/ssh restart`.

Checking firewall rules

About this task

Perform the following procedure to ensure that the Linux firewall is properly configured:

Procedure

1. See Configuring the Linux firewall in *Installing, Upgrading, and Patching Avaya Media Server 7.5*.

The default TCP ports required for EM are: 8009, 8443, 8080, and 80.

2. After you configure the firewall, you can verify whether the required ports are in the LISTEN state using the following command in a Linux shell:

```
netstat -tulpn
```

Cannot log in to EM after installation on Windows

You cannot gain access to EM after a successful installation and reboot.

A possible cause for this problem is the multiple JDK or JRE Java installations on the system.

Another possible cause is that the firewall is blocking the TCP ports which EM requires.

Proposed solution

About this task

Perform the following procedure to remove multiple JDK or JRE installations from the system:

Procedure

1. To open Windows Services, navigate to **Start > Run...** and then type `services.msc` in the **Open** field.
 2. Verify that Avaya EM Service is in the list and has a status of started.
If Avaya EM Service is not in the list, continue with the following steps. Otherwise, check the troubleshooting topics for another possible cause.
 3. To uninstall Avaya MS, follow your parent product documentation or see Uninstalling Avaya Media Server from Windows in *Installing, Upgrading, and Patching Avaya Media Server 7.5*.
 4. After you uninstall and restart the system, navigate to **Start > Control Panel > Programs and Features**.
 5. To uninstall any JDK or JRE installations, double-click the installation file and follow the onscreen instructions.
 6. Restart the server.
 7. To re-install Avaya MS, follow your parent product documentation or see Installing Avaya Media Server on Windows in *Installing, Upgrading, and Patching Avaya Media Server 7.5*.
If the problem still exists after reinstalling Avaya MS, contact Avaya Technical Support.
-

Cannot log in to EM using a new user account on Windows

You cannot log into EM with a newly created local user account which is a member of the Administrators group.

If the Microsoft User Account Control (UAC) feature is enabled it can cause this problem.

Proposed solution

About this task

Using the following procedure, you can disable the Microsoft User Account Control (UAC) feature so that new administrator users can log in. If the system does not accept the change in the security level in Windows, you must use only the primary Windows administrator login credentials for EM login.

Procedure

1. Open the **Local Security Policy** page by navigating to **Start > Run...** and entering `secpol.msc` in the **Open** field.
 2. In the **Local Security Policy** page, navigate to **Security Settings > Local Policies > Security Options**.
 3. Scroll down in the **Policy** list the system displays in the right pane and double-click **User Account Control: Run all administrators in Admin Approval Mode**.
 4. Select **Disabled**.
 5. Click **OK**.
 6. Restart the system.
-

Cannot log in to EM using the EM desktop shortcut with IE

Using the EM Windows desktop shortcut, you cannot log in to EM in the following conditions:

- Avaya System Manager Single Sign-On (SSO) settings are enabled on **EM > Security > General Settings** and **EM > Security > Certificate Management**.
- Internet Explorer is the default browser on the Windows system where you have installed Avaya MS.

This issue can happen when Internet Explorer validation fails for the certificates used by web servers, including the certificates served by Avaya System Manager web server and Avaya MS web server.

Proposed Solution

Procedure

1. Perform the following steps to obtain the Certificate Authority certificate for the Avaya System Manager:
 - a. Log on to the Windows Avaya MS server.
 - b. Open a browser and connect to the associated Avaya System Manager server that you use for Single Sign-On.
 - c. Log in to System Manager.
 - d. In the **Services** area on the **Home** tab, click the **Security** link.
 - e. On the **Security** tab, click **Certificates**.
 - f. Click **Authority** under **Security > Certificates**.
 - g. On the **Certificate Authority** page, click **Download to Internet Explorer**.
 - h. Save the `default.cacert.crt` file somewhere on the Avaya MS server.
This is the CA certificate that you import to Internet Explorer.
2. Perform the following steps to add the Certificate Authority certificate in Internet Explorer for Trusted Root Certification Authorities:
 - a. Log on to the Windows Avaya MS server.
 - b. Open Internet Explorer.
 - c. Go to **Tools > Internet Options**.
 - d. Click the **Content** tab.
 - e. In the **Certificates** section, click **Certificates**.
 - f. Click **Import...**
The system displays the Certificate Import Wizard window.
 - g. Click **Next**.
 - h. Click **Browse...** to select `default.cacert.crt`, the System Manager CA certificate file, that you have saved earlier on Avaya MS.
 - i. Click **Next**.
 - j. Select **Place all certificates in the following store**.
 - k. Click **Browse...**
 - l. Select **Trusted Root Certification Authorities**.
 - m. Click **OK**.
 - n. Click **Next**.
 - o. Click **Finish**.
The system displays the security warning message.
 - p. Click **Yes**.
The system displays `The import was successful`.
 - q. Click **OK**.
 - r. Go to the **Trusted Root Certification Authorities** tab by clicking on the small arrows in the top right corner.

- s. Ensure a certificate with `default` in the **Issued To** and **Issued By** fields is listed.
 - t. Click **Close**.
 - u. Click **OK**.
-

EM cannot download files when using IE

You are unable to download any files from EM. IE can block encrypted files from being downloaded.

Proposed solution

Perform the procedure to allow encrypted files to be saved in IE so that EM can download files.

Related topics:

[Adding EM to the trusted sites list in IE](#) on page 10

EM displays a blank page after login when using IE

After logging on to EM with valid credentials, you see a blank page. IE can block access to servers that are not in the trusted sites list. If the server you are connecting to is not in the trusted sites list, the browser does not display the EM pages.

Proposed solution

Perform the procedure to add Avaya MS to the trusted sites list in IE so that EM can display the pages.

Related topics:

[Adding EM to the trusted sites list in IE](#) on page 10

The EM Media Management tool is slow

You can experience slow system response times when browsing media using **EM > Tools > Media Management**.

A possible cause for this problem is that you have installed anti-virus software on the system and Avaya MS related directories are not in the scan exclusion list.

Proposed solution

If you install anti-virus software, ensure that you exclude the following directories from the scans:

- Linux:

```
$MASHOME/avaya/ma/MAS/common/log
```

```
$MASHOME/avaya/ma/MAS/platdata
```

- Windows:

```
%MASHOME%\Avaya\multimedia_applications\MAS\common\log
```

```
%MASHOME%\Avaya\multimedia_applications\MAS\platdata
```

Call completion troubleshooting

Avaya MS rejects incoming SIP sessions

Avaya MS rejects SIP sessions in the following manner:

- Avaya MS rejects incoming SIP sessions for one or more service types. Use the Log Viewer to identify attempts to launch an uninstalled or unlicensed service.
- Avaya MS rejects incoming SIP sessions and you see SIP failure responses such as 305 Use Proxy, or 403 Forbidden, in the message traces or logs.

The possible causes for these problems include:

- The calls to services on Avaya MS that are not licensed, receive a SIP final response indicating that the service is unavailable.
- The proxy configuration is incomplete.
- The target service application is not installed.
- Avaya MS is in the Pending Lock State.

Proposed solution

Checking the license

About this task

Perform the following procedure to ensure that the required licenses are configured:

Procedure

1. To check the number and variety of installed licenses, navigate to **EM > Licensing > General Settings > Licensing Details**.
Ensure the required licenses are installed and available.
If you need to alter the license configuration, see License configuration for detailed procedures.
2. Restart the system to activate any installed license.

Related topics:

[License configuration](#) on page 58

Checking proxy configuration

About this task

Perform the following procedure to verify whether the required SIP proxy nodes and routes are configured:

Procedure

1. Navigate to **EM > System Configuration > Signaling Protocols > SIP > Nodes and Routes**.
2. Ensure that you have configured the required **Trusted Nodes**.
3. Ensure that you have configured the required **SIP Routes**.
If you need to add trusted SIP nodes or SIP routes, see the procedures for SIP configuration.

Related topics:

[SIP configuration](#) on page 77

Checking application installation

About this task

If you have not installed a required application then the requests for that application fail.

Perform the following procedure to ensure that you have installed and unlocked the required applications:

Procedure

1. Navigate to **EM > Applications > Packaged Applications**, and ensure that the target service is installed.
If necessary, install the application using the application installer.

2. Navigate to **EM > Applications > Operational State** and ensure that the target service is unlocked.
If necessary, unlock the application by selecting the check box next to the desired application and then click **Unlock**.

Checking if Avaya MS is in Pending Lock state

About this task

Avaya MS in the Pending Lock state rejects new service requests. If this state is not required, then you can resolve the issue by unlocking Avaya MS as described in the following procedure:

Procedure

1. Navigate to **EM > System Status > Element Status** to check the state of Avaya MS.
 2. Set Avaya MS state to the Unlocked state by selecting **More Actions > Unlock**.
-

Unsupported codec response from Avaya MS

Avaya MS sends the following unsupported codec responses:

- Rejects incoming sessions and indicates there is no supported codec.
- Responds with a SIP 415, Unsupported Media Type.

The possible causes of these problems include:

- The session request does not offer a supported audio codec.
- When you configure Avaya MS with SECURITY ENFORCED security policy, Avaya MS does not accept sessions from clients offering insecure media.

Proposed solution

About this task

Perform the following procedure to set the security policy to **BEST EFFORT** so that Avaya MS can process sessions from clients offering insecure media:

Procedure

1. Navigate to **EM > System Configuration > Media Processing > Media Security**.
2. Select **BEST EFFORT** for the **Security Policy** mode, and adjust the **Best Effort Mode** and **Crypto Suites**.

For more detailed information, see Media settings configuration.

If the security settings are not the cause, then the session incoming to Avaya MS is not offering a supported audio codec.

Related topics:

[Media settings configuration](#) on page 102

TLS connection issues

Clients using Transport Layer Security (TLS) are unable to connect to Avaya MS.

The possible causes for TLS connection issues include:

- A backup file containing expired certificates, or incorrect TLS configuration settings is restored.
- All the nodes in a cluster are not TLS enabled.
- The certificates on either side of the attempted connection have expired.
- The configuration is incomplete or pending a restart.
- The IP address of the server is changed.
- The Trust Anchor configuration is incomplete.

Proposed solution

You require many configuration items for setting up TLS correctly in an Avaya MS cluster. See Security configuration documents and ensure that all settings are implemented correctly.

Some common solutions for these problems include:

- Ensure that certificates on either side of the attempted connection did not expire.
- Ensure that the Trust Anchor is in the Trust Store on all cluster nodes.
- Ensure that all nodes in a cluster are TLS enabled for every interface.
- When the IP address of a server changes, new certificates might be required if `subject alt name` is used.
- If a restoration, using a backup file containing expired certificates or outdated TLS configuration settings was used, then fix the TLS configuration.
- Some TLS changes require Avaya MS restart for the changes to take effect.
- Confirm that the media security settings meet the requirements. For more detailed information, see Media settings configuration.

Related topics:

[Media settings configuration](#) on page 102

Digit collection issues

Users are unable to log into Avaya MS services because of digit connection problems.

The possible reasons for digit collection issues include:

- If the client connects to Avaya MS through a PSTN or other form of internet gateway device, then you must configure the client to translate digits in the format that negotiates with Avaya MS. The following are the digit signaling formats:
 - In-band DTMF tones
 - RFC 2833 telephone events
 - SIP INFO digits
- To communicate digits, the client and the gateway device must use the same methodology indicated to Avaya MS and both must use only that methodology.
- Some gateways that translate in-band digits into events such as telephone-event or INFO digits fail to completely clamp the received tones. These tones can trigger unexpected behaviour in Avaya MS.
- If necessary, collect SIP messaging to resolve the nature of digit communication between the client, gateway, and Avaya MS.
- In some cases such as conferencing, clients unintentionally send digits in the conference through their microphone. The system detects these digits as conference controls in the conference. For example, a person near a conference user dials a number on a speakerphone and these digits are carried in the conference over the microphone of the active user.
- When users report digit collection issues, ask about the client type and surroundings to identify the cause of any unexpected conference behaviors.

Proposed solutions

- Configure the mode of digit transport from the clients or gateways or both for your installation. Digit translating gateway devices might require adjustments in order to fully clamp in-band DTMF tones.
- Analyze traces to ensure that clients and gateways are properly communicating digits to Avaya MS.
- Advise users in noisy surroundings to ensure minimal background noise as the background noise might impact digit collection.

Media playback troubleshooting

Unable to playback provisioned audio file

Proposed solution

The audio files played by Avaya MS must be encoded as 16 bit, 8 kHz, single channel, LPCM files. However, you can use other sampling rates and codecs that are supported by Avaya MS. Avaya MS does not support multiple channels, like stereo.

RSS and SHOUTCast troubleshooting

Users do not hear streaming SHOUTCast audio

The possible causes for the problem are:

- Improper configuration.
- Volume is too low.
- The configured SHOUTCast URL is unavailable or unreachable.
- The audio provided by the configured SHOUTCast URL is not in MP3 or wav audio format.

Proposed solution

Check the SHOUTCast configuration:

- Ensure that the SHOUTCast URL and channel key are correct.
- Ensure that the SHOUTCast proxy server host and port configuration are correct.
- Adjust the continuous streaming source volume level on the media server.
- Ensure that the streaming source is in either MP3 or wav audio format.
- Ensure that the SHOUTCast URL is reachable from the media server. To resolve the URL use wget or curl with the configured SHOUTCast URL.

The following is a successful wget example:

```
wget http://yp.shoutcast.com/sbin/tunein-station.pls?id=227567 --2014-01-06
18:52:59-- http://yp.shoutcast.com/sbin/tunein-station.pls?id=227567
Resolving webproxy.avaya.com... 8.28.150.65
Connecting to webproxy.avaya.com |8.28.150.65|: 80... connected.
Proxy request sent, awaiting response... 200 OK
Length: 5080 (5.0K) [audio/x-scpls]
Saving to: `tunein-station.pls?id=227567.2'
2014-01-06 18:53:00 (157 KB/s) - `tunein-station.pls?id=227567.2' saved [5080/5080]
```

The following is a successful cURL example:

```
curl http://yp.shoutcast.com/sbin/tunein-station.pls?id=227567 [playlist]
numberofentries=45
File1=http://95.141.24.96:80
Title1=(#1 - 44/1000) ChartHits.FM - Top 40 Radio - Mega Hot Music!
Length1=-1
File2=http://95.141.24.58:80
Title2=(#2 - 45/1000) ChartHits.FM - Top 40 Radio - Mega Hot Music!
Length2=-1
Version =2
```

Related topics:

[Configuring continuous STOUTCast streaming](#) on page 105

Users do not hear streaming RSS audio

The possible causes for this problem are:

- Improper configuration.
- Volume is too low.
- The configured RSS URL is unavailable or unreachable.
- The audio files specified in the RSS document not in MP3 or wav audio format.

Proposed solution

Check the RSS configuration:

- Ensure that the RSS URL and channel key are correct.
- Adjust the continuous streaming source volume level on the media server.
- Ensure that the audio files specified in the RSS document are in either MP3 or wav audio format.
- Ensure that the SHOUTCast URL is reachable from the media server. To resolve the URL use wget or cURL with the configured SHOUTCast URL.

The following is a successful wget example:

```
wget http://xyz.com/audio/rss/feed.xml
--2014-01-06 18:39:24-- http://xyz.com/audio/rss/feed.xml
Resolving webproxy.avaya.com... 8.28.150.65
```

```
Connecting to webproxy.avaya.com|8.28.150.65|:80... connected.  
Proxy request sent, awaiting response... 200 OK  
Length: 1025790 (1002K) [text/xml]  
Saving to: `feed.xml'  
2014-01-06 18:39:27 (2.85 MB/s) - `feed.xml' saved [1025790/1025790]
```

The following is a successful cURL example:

```
curl http://xyz.com/audio/rss/feed.xml  
<?xml version= "1.0" encoding= "UTF-8" ?>  
<rss xmlns:itunes= "http://www.itunes.com/DTDs/Podcast-1.0.dtd" version="2.0">  
<channel>  
...  
</channel>  
</rss>
```

Related topics:

[Configuring continuous RSS streaming](#) on page 107

High Availability troubleshooting

Cannot enable High Availability because it is disabled

When you navigate to **EM > Cluster Configuration > High Availability > General Settings**, you cannot select **Enable High Availability**.

You can select **Enable High Availability** only if the prerequisite High Availability configuration is complete, that is, a Primary and Backup server must be configured.

Proposed Solution

Perform the prerequisite High Availability configuration procedures in the correct order. For detailed information, see High Availability configuration.

Related topics:

[High Availability configuration](#) on page 48

Protocol troubleshooting

SNMP Traps are not getting posted on management consoles

The system cannot post SNMP traps to the monitoring system management servers.

The possible causes for this problem include:

- An incorrect SNMP network manager address.
- Network connectivity problems.
- SNMP Community string mismatch.
- SNMP Delivery is not enabled.
- SNMP Service is not started on Avaya MS.

Proposed solution

Incorrect SNMP network manager address

Procedure

1. Ensure **SNMP Network Manager Address** is configured with the correct address on Avaya MS by navigating to **EM > System Configuration > Network Settings > General Settings > SNMP Traps**.
2. If you change Avaya MS, then restart the system for the change to take effect.

Checking the network

About this task

Perform the following procedure to confirm there are no network problems between the monitoring system and Avaya MS:

Procedure

1. Verify that the monitoring system and Avaya MS can ping each other.
 2. If the ping test fails, troubleshoot the network connection between the monitoring system and Avaya MS.
-

Checking the SNMP community string

About this task

The following procedure verifies that the SNMP Community string on the monitoring system and on Avaya MS are the same.

Procedure

1. Check the configured community string on the monitoring system.
2. Check SNMP community string on Avaya MS by navigating to **EM > System Configuration > Network Settings > General Settings > SNMP Traps**.
If the community string on the monitoring system does not match the one on Avaya MS, then change one string to match the other.
3. If you change the community string on Avaya MS, restart the system for the change to take effect.

SNMP delivery is not enabled

Procedure

1. Ensure **Delivery of Alarms via Traps** is selected on Avaya MS by navigating to **EM > System Configuration > Network Settings > General Settings > SNMP Traps**.
2. If you change Avaya MS, then restart the system for the change to take effect.

Checking the SNMP service

About this task

Perform the following procedure to verify that you have installed the SNMP and the service is running:

Procedure

1. Navigate to **Start > Run...** and then type `services.msc` in the **Open** field to open the Windows Services.
 2. Verify **SNMP Service** is in the list and has a status of started.
 3. If SNMP Service is not running, then right-click and select **Properties**.
 4. Click **Start**, and set **Startup type** to **Automatic**.
-

SMTP mail delivery is not working

Avaya MS does not deliver recorded conferences or other e-mails sent by applications on the media server as expected, using Simple Mail Transport Protocol (SMTP).

Configuration, provisioning, or SMTP server availability are the typical causes for this problem. Sometimes, the network security settings prevent access to the SMTP server.

Proposed solution

- Ensure that an SMTP server address is configured for the service. You can configure these settings on the provisioning system connected to Avaya MS. In some cases, you need to provision and save a destination e-mail address for each user in Avaya MS.
- Ensure that the SMTP server address configured refers to a valid in service mail server.
- Ensure that the network settings are configured in such a way that Avaya MS can gain access to the SMTP server configured as the e-mail server.

SOAP connection is rejected

A provisioning or management system cannot connect to Avaya MS SOAP interface.

Possible causes for this problem include:

- The SOAP configuration is not complete.
- The remote server is not in the **SOAP Trusted Nodes** list when you enable the use of **Trusted SOAP Nodes** on Avaya MS.
- The SOAP server address or port used is incorrect or are changed in one of the endpoints.

Proposed solution

About this task

Perform the following procedure to verify SOAP configuration on Avaya MS as well as the provisioning or management system which is attempting to connect to Avaya MS.

Procedure

1. For basic SOAP configuration details, see *Configuring SOAP* and then perform the following checks:

- a. Verify that each setting of the SOAP configuration on Avaya MS is compatible with the settings of the system attempting to connect to Avaya MS.
 - b. Verify that the system which is attempting to connect to Avaya MS is in the **SOAP Trusted Nodes** list when you select **Enable Trusted SOAP Nodes**.
 2. Check that the ports configured for SOAP on Avaya MS match the SOAP ports configured on the system which is attempting to connect to Avaya MS.
 - a. Navigate to **EM > System Configuration > Network Settings > Advanced Settings**.
 - b. Scroll down to **MAS Management SOAP Server**.
 - c. Verify the `admin_soap_tls` port value.
 - d. Verify the `admin_soap` port value.
 3. If any of the values inspected in the preceding steps are not as required or not compatible with the settings on the remote system attempting the connection, then you must change the SOAP settings on either Avaya MS or on the remote server.
-

Related topics:

[Configuring SOAP](#) on page 68

Index

A

advanced settings	16
archived media	136
assigning certificate for service profile	121

B

backup and restore	147 , 150 – 154
Backup and Restore tool	154
configure backup task	147
configure history log	153
delete backup task	150
edit backup destination	151
execute backup task	150
history log	153
local destination	151
upload backup file	152

C

Call completion Troubleshoot	207
unsupported codec response from Avaya MS ...	207
Call completion troubleshooting	205 , 208 , 209
Avaya MS rejects incoming SIP sessions	205
digit collection issues	209
TLS connection issues	208
change	73
computer name	73
IP address	73
Change	144
application operational state	144
changing	74 – 76
computer name on Windows	74
IP address on Linux	75
IP address on Windows	76
cluster	47
change settings	47
cluster configuration	39
Configuration	39
overview	39
configure	19 , 44 , 45 , 48 , 52 , 58 , 61 , 63 , 69 , 70 , 77 , 102 , 113 , 118 , 125 , 126 , 146 , 165 , 178 , 181 , 193 , 194
Avaya MS using EM	19
connection security	69
Content Store	125

field promotion	194
HA cluster configuration	52
High Availability	48
license	58
license server	58
log filter settings	165
media security	113
media settings	102
nodal licensing	61
OM archiving	181
OM settings	178
packaged applications	146
replicate Content Store data	45
replication settings	44
SDR archiving	193
SIP	77
System Manager settings	118
time zone preference	126
transmit prioritization	70
WebLM License	63
Configure	107
configuring	142
RFC5707 interpreter	142
Configuring negotiated parameters	115
Configuring RSS streaming	107
content pane	15
refresh frequency	15
Content Store	127
media storage	127
create	118 – 120
a new certificate to be signed by other authorities in Key Store	119
a renewal certificate signing request	120
new certificate signed in Key Store	118
new self-signed certificate in Key Store	119

D

delete	145 , 146
application signaling translations	145
custom application	146
delete a pending certificate signing request	121
deleting certificate authorities from Trust Store	124
disable	46
replication of Content Store data	46
downloading certificate revocation list	124

E

Element Manager	9–11 , 13 , 27–29 , 31–36 , 128
change users for EM login on Linux	36
current operational status	27
debug tracing	34
download log capture	35
enable SSL file downloads in IE	10
High Availability state	31
install	9
interface	13
introduction	9
Log Capture tool	34
logging and navigating	27
Media management tool	128
operational state	29
overview	11
review PVI Checker results	33
start or stop media server	28
Trusted Sites	10
view software inventory	32
Web browser	9
Element Manager Troubleshoot	201 , 204
cannot access EM after installation on Windows	201
EM Media Management tool is slow	204
EM cannot download files when using IE	204
EM cannot download files when using Internet Explorer	204
EM displays a blank page after login when using IE	204
EM solution	199 , 200
check firewall rules	200
check PasswordAuthentication	200
check user group	199
enable	67
SNMP trap	67
enabling High Availability	49
primary server	49
engineering parameters	16
exporting a Key Store certificate	123
exporting a Key Store certificate in PEM format	122

H

High Availability	51 , 53 , 54 , 56 , 57
backup server	51
change service IP address	56
change setting	57
how to enable	53
review configuration	54

I

importing a Trust Certification Revocation List	123
---	---------------------

importing certificate for service profile	122
importing trust certificate to Trust Store	123

M

Media file format	127
Media playback	210
modify server profiles	66
monitor	176 , 181
protocol connections	181
system performance	176
monitor logs	161
monitoring	157 , 170 , 184
active sessions	170
session detail records	184
monitoring session	184 , 186–189
analyze traffic	188
determine traffic	186
review detail record	189
review SDRs	184
summarize traffic	187
mute	175

N

Negotiated parameters	115
-----------------------------	---------------------

P

process a certificate signing request in Key Store	120
Proposed solution	204 , 210
Protocol Troubleshoot	213 , 215
SMTP mail delivery not working	215
SNMP Traps are not on management consoles	213
SOAP connection rejected	215

Q

quick	17 , 18 , 20 , 21 , 23 , 24
call testing	20
monitoring	20
debugging	20
installation and configuration	17
installation on Linux	17
installation on Windows	18
make a test call	21
monitor active sessions	21
reviewing session detail records	23
view call traces for debugging	24
quick setup	17

R		
RSS streaming	107	
S		
select	71	
IP interface assignment	71	
session	175	
set	65	
alarm threshold	65	
license server alarm threshold	65	
nodal license alarm threshold	65	
setting	126	
login setting	126	
SHOUTCast troubleshooting	210	
Proposed solution	210	
streaming RSS audio	211	
Proposed solution	211	
Troubleshoot	211	
Streaming SHOUTCast audio	210	
Troubleshoot	210	
T		
troubleshoot	210 , 212	
		cannot enable High Availability 212
		Troubleshoot 202
		cannot log in to EM using a new user account on Windows 202
		cannot log in to EM with System Manager Single Sign-On using EM shortcut with IE 202
U		
		Unable to playback provisioned audio file 210
		unassigning a certificate for service profile 121
		unmute 175
		update 61 , 62
		license server key 61
		nodal license 62
		Users do not hear streaming RSS audio 211
		Users do not hear streaming SHOUTCast audio 210
V		
		view 170 , 182 , 183
		advanced protocols 183
		component status 182
		current active sessions 170
		View 157
		element status 157

