Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications

Release 7.1.2.3
Issue 1
August 2026

© 2015-2026, Avaya LLC
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

The Global Software License Terms (“Software License Terms”) are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

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

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction 13
Purpose 13
Intended audience 13
Related resources 13
Avaya Aura® Contact Center documentation 13
Viewing Avaya Mentor videos 17
Support 18
Chapter 2: Change in the release 19
Changes in this release 19
Chapter 3: Avaya Aura® Contact Center server commissioning 22
Prerequisites to Contact Center server commissioning 23
Commissioning tasks for SIP-enabled Contact Center 24
Chapter 4: Contact Center security certificates commissioning 29
Prerequisites 31
Contact Center certificate commissioning procedures for Unified Communications systems 32
Turning off Web Services security 35
Creating a new security store 36
Creating a security store with Subject Alternative Names 38
Copying the Certificate Signing Request file 39
Adding certificate files to the security store 41
Configuring the minimum TLS version 42
Exporting a root certificate from the security store 43
Importing the Contact Center root certificate into Avaya Aura® MS 44
Applying the root certificate to a Contact Center client 45
Configuring SMTP server details 46
Scheduling a security store inspection task 47
Verifying the scheduled security store inspection task 48
Chapter 5: Contact Center Manager Server commissioning 49
Contact Center Manager Server commissioning procedures 49
Verifying the success of the installation 51
Applying the local WebLM license file 51
Configuring remote WebLM server 52
Enabling Multiplicity 52
Scheduling weekly disk defragmentation 53
Configuring the Multicast controller 54
Enabling support for Third Line Appearance 55
Installing the third-party networking utility 56
Chapter 6: Network Control Center commissioning 57
Prerequisites for Network Control Center commissioning 57

Configuring the sites ... 57
Chapter 7: Avaya Aura® Media Server commissioning for non-HA deployments ... 59
Avaya Aura® Media Server non-HA commissioning checklist ... 60
Logging on to Avaya Aura® Media Server Element Manager ... 60
Configuring the primary Avaya Aura® Media Server for the cluster ... 61
Configuring a secondary Avaya Aura® Media Server for the cluster ... 62
Configuring a standard Avaya Aura® Media Server for the cluster ... 64
Chapter 8: Avaya Aura® Media Server commissioning for HA deployments ... 66
Prerequisites ... 67
Avaya Aura® Media Server High Availability commissioning procedures ... 68
Avaya Aura® Media Server HA commissioning checklist ... 69
Logging on to Avaya Aura® Media Server Element Manager ... 71
Obtaining the Universally Unique Identifier of the primary server ... 72
Configuring the High Availability pair primary Avaya Aura® Media Server ... 72
Configuring the High Availability pair backup Avaya Aura® Media Server ... 74
Enabling High Availability on the backup server ... 75
Completing High Availability pair configuration ... 76
Enabling High Availability on the primary Avaya Aura® Media Server ... 77
Reviewing High Availability configuration and status ... 79
Configuring Content Store replication across multiple Avaya Aura® Media Server High Availability pairs ... 79
Configuring the primary Avaya Aura® Media Server for the remote site ... 81
Configuring the secondary Avaya Aura® Media Server for the remote cluster ... 82
Configuring the standard Avaya Aura® Media Server for the remote cluster ... 83
Configuring the remote site to replicate from the campus site ... 84
Chapter 9: Avaya Aura® Media Server common commissioning ... 86
Configuring media on Avaya Aura® Media Server ... 86
Prerequisites for Avaya Aura® Media Server common commissioning ... 90
Avaya Aura® Media Server common commissioning procedures ... 90
Avaya Aura® Media Server common commissioning checklist ... 92
Logging on to Avaya Aura® Media Server Element Manager ... 93
Adding Contact Center Manager Server as a SIP trusted node ... 94
Adding Contact Center Manager Administration as a SOAP trusted node ... 95
Configuring a HTTP proxy for external music source access ... 95
Configuring **a streaming music source** ... 96
Adjusting the volume of the prompts ... 97
Configuring Avaya Aura® Media Server hostname verification ... 98
Configuring Avaya Aura® Media Server settings for SIP-enabled contact center ... 98
Chapter 10: Contact Center Manager Administration commissioning ... 100
Prerequisites for Contact Center Manager Administration commissioning ... 100
Contact Center Manager Administration commissioning procedures ... 100
Configuring Real-Time Reporting ... 104
Configuring domain accounts to allow scheduling Historical Reports to a Network Server ... 106

Creating a shared folder to export historical reports..... 106
Creating a shared folder on the client with read permissions for the domain..... 107
Creating a shared folder on the client with read permissions for a user..... 108
Creating a shared folder on the client PC with read permissions for the CCMA Administration account..... 109
Configuring Agent Desktop Display parameters on the server..... 110
Updating the CCMA Administration user password..... 112
Verifying web services..... 113
Configuring internet options..... 113
Accessing Contact Center Manager Administration from Microsoft Edge in Internet Explorer mode..... 115
Adding the Microsoft Edge administrative templates..... 116
Configuring integration with Internet Explorer..... 116
Configuring the Enterprise Mode Site List..... 117
Internet Explorer mode and Compatibility View configuration on the domain server..... 119
Adding the Microsoft Edge administrative templates to the domain server..... 120
Creating a configuration file for Internet Explorer mode..... 121
Uploading the configuration file for IE mode to the CCMA server..... 123
Enabling IE mode on the domain server..... 123
Completing IE mode configuration on a local computer..... 125
Configuring Compatibility View settings on the domain server..... 125
Disabling Internet Explorer 11 as a standalone browser..... 127
Logging in to Contact Center Manager Administration for the first time..... 127
Configuring Contact Center Manager Server global settings..... 129
Adding route points..... 130
Adding media servers..... 131
Adding media servers to the required services..... 133
Installing the Orchestration Designer client..... 134
Adding a Contact Center script or flow application..... 135
Chapter 11: Contact Center Manager Server certificate commissioning..... 137
Creating a new security store..... 138
Creating a security store with Subject Alternative Names 140
Copying the Certificate Signing Request file..... 141
Adding certificate files to the security store..... 143
Configuring the minimum TLS version..... 144
Exporting a root certificate from the security store..... 145
Manually applying the root certificate to AES..... 146
Importing the Contact Center root certificate into Avaya Aura® MS..... 147
Configuring SMTP server details..... 148
Scheduling a security store inspection task..... 149
Verifying the scheduled security store inspection task..... 150
Chapter 12: Avaya Aura® Media Server security and SRTP commissioning..... 151
Creating a new certificate signing request for Avaya Aura® Media Server..... 152

Adding signed certificate files to the Avaya Aura® MS key store ... 153
Assigning the server certificate to an Avaya Aura® MS service profile ... 154
Creating a Certificate Signing Request with multiple Subject Alternative Names for Avaya Aura® Media Server ... 155
Adding signed certificates generated in SMGR to the Avaya Aura® MS key store ... 156
Assigning the server certificate generated in SMGR to an Avaya Aura® MS service profile ... 157
Importing the Avaya Aura® MS root certificate into the Contact Center security store ... 157
Verifying the TLS configuration on Avaya Aura® Media Server ... 158
Configuring SRTP on Avaya Aura® Media Server ... 158
Verifying the Media Server configuration in CCMA ... 159
Chapter 13: Single sign-on commissioning ... 160
Prerequisites for single sign-on commissioning ... 160
Single sign-on commissioning procedures ... 160
Configuring communication between CCMA and System Manager ... 162
Mapping System Manager users to CCMA users ... 163
Starting the Contact Center Manager Administration client using a secure account ... 164
Configuring communication between CCMA and the backup System Manager ... 165
Configuring Agent Greeting properties for SSO ... 166
Chapter 14: High Availability single sign-on commissioning ... 168
Prerequisites for High Availability single sign-on commissioning ... 168
High Availability single sign-on commissioning procedures ... 169
Configuring communication between CCMA and System Manager on the primary Contact Center server ... 171
Configuring communication between CCMA and System Manager on the standby Contact Center server ... 172
Configuring communication between CCMA and System Manager on the geographic Contact Center server ... 174
Mapping System Manager users to CCMA users ... 175
Configuring internet options for SSO ... 176
Logging in to CCMA for the first time using a secure account ... 177
Chapter 15: Contact Center Manager Administration client commissioning ... 178
Prerequisites for client commissioning ... 178
Configuring the display settings ... 178
Configuring internet options on each client ... 179
Adding your browser to the firewall exceptions list ... 181
Installing ActiveX controls ... 181
Applying the ActiveX controls ... 182
Chapter 16: Communication Control Toolkit commissioning for SIP-enabled Contact Center ... 183
Prerequisites to CCT commissioning for SIP-enabled Contact Center ... 183
Confirming that the CCT services start ... 183
Adding Communication Control Toolkit to CCMA ... 184
Adding agents in CCMA for SIP-enabled Contact Centers ... 185

Verifying CCT using Reference Client 190
Chapter 17: Contact Center Multimedia commissioning 192
Contact Center Multimedia server commissioning prerequisites 192
Providing local users with the Log on as a service right 192
Verifying that Contact Center Multimedia services start 193
Adding the multimedia servers to Contact Center Manager Administration 194
Logging in to the Multimedia Administration tool for the first time 196
Configuring server settings 196
Configuring an LDAP server for Agent Desktop voice contacts 198
Configuring email recipient addresses 200
Configuring email attachment file locations 202
Configuring the multimedia skillsets 203
Creating an Orchestration Designer application to route from an IM route point to an IM skillset 205
Configuring the MIME types 206
Configuring the client OS setting for Citrix deployments 207
Adding an email address of an administrator in CCMM Dashboard 208
Chapter 18: Avaya Aura® Media Server Zoning commissioning 209
Avaya Aura® Media Server Zoning commissioning procedures 210
Enabling Avaya Aura® Media Server Zoning 212
Updating the Master Script for Avaya Aura® MS Zoning 212
Customizing the Master Script flow application for Zoning 214
Customizing the Media_Server_Selection flow application 215
Configuring the Avaya Aura® MS Zoning list 218
Chapter 19: Agent Greeting commissioning 221
Prerequisites for Agent Greeting commissioning 221
Agent Greeting commissioning checklist 221
Creating a SIP Entity for the Contact Center Agent Greeting endpoint 222
Creating a SIP Entity Link to the Contact Center Agent Greeting endpoint 224
Creating a routing policy from Session Manager to Contact Center 225
Creating a dial pattern to route calls to the Contact Center Agent Greeting endpoint 226
Creating a dial pattern to route calls to the Contact Center Announcement Recorder endpoint .. 227
Configuring the Voice XML Interpreter on Avaya Aura® Media Server 228
Enabling Agent Greeting on CCMS 228
Configuring Agent Greeting on CCMA 229
Enabling Agent Greeting for individual agents and supervisors 231
Performing an end-to-end test 231
Chapter 20: Microsoft instant messaging server commissioning 233
Microsoft instant messaging server prerequisites 234
Microsoft instant messaging server commissioning checklist 234
Creating a Trusted Application Pool for Contact Center 234
Creating a Trusted Application for Contact Center 235
Configuring the Contact Center Trusted Application server 236
Configuring a static route to Contact Center 238

Enabling the TCP port on the instant messaging server ... 240
Restarting the instant messaging service ... 241
Chapter 21: Avaya Aura® Presence Services Instant Messaging commissioning ... 242
Presence Services Instant Messaging commissioning prerequisites ... 242
Avaya Aura® Presence Services Instant Messaging commissioning checklist ... 242
Verifying the substitution rule to map the System Manager user login domain to the Presence Services domain ... 243
Creating a Presence Services user in System Manager for the route point ... 244
Adding an IM route point on CCMA for Presence Services ... 245
Creating a Presence Services user in System Manager for an agent ... 246
Adding the login ID to an agent's settings in CCMA ... 247
Creating a Presence Services user in System Manager for the IM web server ... 248
Creating an Orchestration Designer application to route from an IM route point to an IM skillset 249
Sending an Instant Message to the contact center and verifying the routing to an agent ... 250
Chapter 22: Mission Critical High Availability Voice and Multimedia Contact Server commissioning ... 251
Prerequisites ... 254
High Availability commissioning checklist ... 255
Resolving the Managed name to the Managed IP Address ... 256
Configuring CCMM General Administration ... 257
Verifying services are ready for High Availability ... 258
Configuring campus High Availability on the active server ... 259
Configuring email notification on the Active Server ... 261
Backing up the database on the Active Server ... 262
Restoring the database on the standby server ... 263
Configuring High Availability on the Standby Server ... 265
Verifying server details on the standby server ... 267
Starting the Active Server ... 270
Starting shadowing on the standby server ... 270
Verifying High Availability is running ... 271
Changing server details in Contact Center Manager Administration ... 274
Using the Contact Center Manager Administration managed name ... 275
Testing switchovers ... 276
Chapter 23: Remote Geographic Node High Availability Voice and Multimedia Contact Server commissioning ... 278
Prerequisites ... 280
High Availability commissioning checklist ... 281
Resolving the Managed name to the Managed IP Address ... 282
Verifying services are ready for configuring High Availability ... 283
Configuring geographical redundancy on the active server ... 283
Backing up the database on the active server ... 285
Configuring RGN CCMM General Administration ... 285
Configuring the Remote Geographic Node local resources ... 287

Configuring High Availability on the Remote Geographic Node server 288
Restoring the database on the Remote Geographic Node server 290
Configuring server details on the Remote Geographic Node 292
Starting the active server 294
Starting shadowing on the standby server 295
Starting shadowing on the Remote Geographic Node Server 296
Verifying the Voice and Multimedia Contact Server RGN settings 296
Verifying Voice and Multimedia High Availability is running 297
Chapter 24: Mission Critical High Availability Voice Contact Server commissioning 301
Prerequisites 304
High Availability commissioning checklist 304
Resolving the Managed name to the Managed IP Address 306
Configuring CCMM General Administration 307
Verifying services are ready for High Availability 308
Configuring campus High Availability on the active server 308
Configuring email notification on the Active Server 311
Backing up the database on the Active Server 312
Restoring the database on the standby server 313
Configuring High Availability on the Standby Server 315
Verifying server details on the standby server 317
Starting the Active Server 320
Starting shadowing on the standby server 320
Verifying High Availability is running 321
Changing server details in Contact Center Manager Administration 324
Using the Contact Center Manager Administration managed name 325
Testing switchovers 326
Chapter 25: Remote Geographic Node High Availability Voice Contact Server commissioning 328
Prerequisites 330
High Availability commissioning checklist 331
Resolving the Managed name to the Managed IP Address 332
Verifying services are ready for configuring High Availability 333
Configuring geographical redundancy on the active server 333
Backing up the database on the active server 335
Configuring the Remote Geographic Node local resources 336
Configuring High Availability on the Remote Geographic Node server 337
Restoring the database on the Remote Geographic Node server 339
Configuring server details on the Remote Geographic Node 341
Starting the active server 343
Starting shadowing on the standby server 344
Starting shadowing on the Remote Geographic Node Server 345
Verifying the Multimedia Contact Server RGN settings 345
Verifying High Availability is running 346

Chapter 26: High Availability Multimedia Contact Server commissioning 351
Prerequisites 352
High Availability commissioning checklist 352
Resolving the Managed name to the Managed IP address 354
Installing a third-party utility to support High Availability 355
Configuring CCMM General Administration 355
Configuring the Active Server 357
Backing up the Active Server database 359
Restoring the database on the Standby Server 360
Configuring the Standby Server 361
Starting the Active Server 362
Starting shadowing on the Standby Server 362
Verifying shadowing is running on the Active Server 363
Testing a switchover 364
Chapter 27: Geographic High Availability Multimedia Contact Server commissioning 365
Prerequisites 365
High Availability commissioning checklist 366
Resolving the Managed name to the Managed IP address 367
Installing a third-party utility to support High Availability 368
Configuring the active server 369
Backing up the active server database 370
Configuring RGN CCMM General Administration 371
Configuring the Remote Geographic Node server 373
Restoring the database on the Remote Geographic Node server 374
Starting the active server 375
Starting shadowing on the Remote Geographic Node server 375
Verifying shadowing is running on the active server 376
Chapter 28: High Availability Network Control Center commissioning 377
Prerequisites for High Availability Network Control Center commissioning 379
High Availability Network Control Center commissioning procedures 379
Resolving the Managed name to the Managed IP Address 381
Installing a third-party utility to support High Availability 381
Verifying services are ready for High Availability 382
Configuring High Availability on the Active Server 382
Variable definitions 383
Configuring email notification on the Active Server 384
Variable definitions 385
Backing up the database on the Active server 385
Restoring the database on the Standby server 386
Configuring server details on the Standby server 387
Configuring High Availability on the Standby server 388
Starting the Active server 389
Procedure job aid 389

Starting shadowing on the Standby server ... 390
Verifying shadowing is running on the Active Server ... 391
Changing server details in Contact Center Manager Administration ... 391
Testing switchovers ... 392
Reinstating High Availability after a switchover ... 393
Chapter 29: Contact Center Manager Server web service configuration ... 394
Contact Center Manager Server Web service commissioning checklist ... 395
Generating a Certificate Signing Request for a non-HA server ... 395
Generating a Certificate Signing Request for a High Availability CCMS server pair ... 396
Importing the CSR-Related Certificates ... 397
Configuring SOA OpenQueue and OpenNetworking Web Services ... 398
Removing Certificate Configuration ... 399
Chapter 30: Communication Control Toolkit web service configuration ... 400
Communication Control Toolkit Web service commissioning checklist ... 401
Configuring SIP Call Recording ... 401
Generating a Certificate Signing Request ... 402
Generating a Certificate Signing Request for a High Availability CCT server pair ... 403
Importing CSR-related Certificates ... 405
Importing CSR-related Certificates on Standby and RGN servers ... 405
Configuring SOA CCT Web services ... 406
Removing Certificate Configuration ... 408

Chapter 1: Introduction

Purpose

Use this document when commissioning your Contact Center. It contains information about preparation, initial configuration, and verification of the installation on the Avaya Aura® Unified Communications platform.

Intended audience

This document is intended for people who commission the Avaya Aura® Contact Center solution.

Related resources

Avaya Aura® Contact Center documentation

The following table lists the documents related to Avaya Aura® Contact Center. Download the documents from the Avaya Support website at https://support.avaya.com.

Title	Document purpose	Audience
Overview		

Table continues…

Title	Document purpose	Audience
Avaya Aura® Contact Center Overview and Specification	This document provides the high-level technical details you need to set up your Contact Center suite. The document contains background planning and engineering information, including server preparation information, routing options, licensing configurations, and hardware configuration information. It also contains the background information you require to install all software components that are part of and work with Contact Center. General information about considerations for upgrading your existing Contact Center is also included. This document contains strategies and requirements to plan your network configuration and prepare your servers for Contact Center software installations.	Customers and sales, services, and support personnel
Avaya Aura® Contact Center and Avaya Aura® Unified Communications Solution Description	This document describes the solution architecture, suggested topologies, and capacities for the Avaya Aura® Unified Communications (UC) platform. This document also describes the features and functional limitations of certain configurations.	Customers and sales, services, and support personnel
Avaya Aura® Contact Center and Avaya Communication Server 1000 Solution Description	This document describes the solution architecture, suggested topologies, and capacities for the Avaya Communication Server 1000 platform. This document also describes the features and functional limitations of certain configurations.	Customers and sales, services, and support personnel
Avaya Aura® Contact Center Documentation Catalog	This document contains high-level information about Avaya Aura® Contact Center documentation resources and the type of information in each document.	Customers and sales, services, and support personnel
Avaya Aura® Contact Center Terminology	This document contains definitions for the technical terms specific to Contact Center.	Customers and sales, services, and support personnel
Contact Center Performance Management Data Dictionary	This document contains reference tables that describe statistics and data in historical and real-time reports generated in Contact Center.	System administrators and contact center supervisors

Table continues…

Title	Document purpose	Audience
Implementing		
Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration	This document contains information and procedures to integrate the Avaya Aura® UC platform with Contact Center.	Implementation personnel
Avaya Aura® Contact Center and Avaya Communication Server 1000 Integration	This document contains information and procedures to integrate the Avaya Communication Server 1000 platform with Contact Center.	Implementation personnel
Deploying Avaya Aura® Contact Center DVD for Avaya Aura® Unified Communications	This document contains information about Contact Center DVD installation, initial configuration, and verification for the Avaya Aura® UC platform.	Implementation personnel
Deploying Avaya Aura® Contact Center DVD for Avaya Communication Server 1000	This document contains information about Contact Center DVD installation, initial configuration, and verification for the Avaya Communication Server 1000 platform.	Implementation personnel
Deploying Avaya Aura® Contact Center Software Appliance for Avaya Aura® Unified Communications	This document describes how to deploy the Avaya Aura® Contact Center Software Appliance for the Avaya Aura® UC platform.	Implementation personnel
Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications	This document describes Contact Center preparation, initial configuration, and verification of the installation on the Avaya Aura® UC platform.	Implementation personnel
Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000	This document describes Contact Center preparation, initial configuration, and verification of the installation on the Avaya Communication Server 1000 platform.	Implementation personnel
Avaya Aura® Contact Center and Proactive Outreach Manager Integration	This document provides conceptual and procedural information on the integration between Avaya Aura® Contact Center (AACC) and Avaya Proactive Outreach Manager (POM). It describes the tasks required for AACC and POM integration.	Implementation personnel
Upgrading and Patching Avaya Aura® Contact Center	This document contains information and procedures to upgrade from previous releases to Contact Center, migrating the databases, and information and procedures to download and install service packs.	Implementation personnel and system administrators

Table continues…

Title	Document purpose	Audience
Administering		
Avaya Aura® Contact Center Server Administration	This document contains information and procedures for day-to-day maintenance of all servers in the Contact Center suite, including server maintenance tasks, administrative tasks, managing data, configuring data routing, performing archives, and backing up data. It also describes optional configuration procedures.	System administrators
Avaya Aura® Contact Center Client Administration	This document contains information and procedures to configure users and user access, skillsets, server management, and configuration data in the Contact Center database.	System administrators and contact center supervisors
Using Contact Center Orchestration Designer	This document contains information and procedures to configure script and flow applications in Orchestration Designer.	System administrators
Maintaining		
Maintaining Avaya Aura® Contact Center	This document contains routine maintenance procedures, such as installing service packs and maintaining the databases for the Contact Center system.	System administrators and support personnel
Troubleshooting Avaya Aura® Contact Center	This document contains system-wide troubleshooting information and procedures for Contact Center hardware, software, and network.	System administrators and support personnel
Contact Center Event Codes	This Microsoft Excel spreadsheet contains a list of errors in the Contact Center suite and recommendations to resolve them.	System administrators and support personnel
Using		
Using Avaya Aura® Contact Center Reports and Displays	This document contains procedures to generate performance reports, and to monitor and analyze performance data and performance measurements.	System administrators and contact center supervisors
Using Agent Desktop for Avaya Aura® Contact Center	This document provides information and procedures for agents who use the Agent Desktop application to accept, manage, and close contacts of all media types in Contact Center.	Contact center agents and supervisors

Table continues…

Title	Document purpose	Audience
Using the Contact Center Agent Browser application	This document provides information and procedures for agents who use the Agent Browser application to log on to Contact Center and perform basic tasks.	Contact center agents
Using Avaya Workspaces for AACC and ACCS	This document describes the tasks that Contact Center agents can perform using Avaya Workspaces.	Contact center agents and supervisors
Release Notes		
Avaya Aura® Contact Center Release Notes	The Release Notes contain information about known issues, patches, and workarounds.	System administrators and support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click to display the search results.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: Change in the release

Changes in this release

Changes in the release 7.1.2.3

The following are the changes or updates introduced in the release 7.1.2.3:

Workspaces Operating System Migration from CentOS 7.9 to RHEL 9.6

Avaya Workspaces infrastructure migrated from CentOS 7.9 to Red Hat Enterprise Linux (RHEL) 9.6.

Third-Party Component Version Upgrades

This release includes upgrades to several third-party software components used by the Avaya Aura® Contact Center and Avaya Workspaces environments. The updated versions provide improved platform compatibility, security, stability, and alignment with supported software versions.

The following table lists the software components and their versions included in release 7.1.2.3:

Software Component	Version in 7.1.2.3
Operating System	RHEL 9.6
Java (Avaya Aura® Contact Center)	8.94.0.18 (OpenJDK 1.8.0_492)
Java (Avaya Workspaces)	17.60.17
.NET	4.8
Spring Boot	3.5.6
Log4j	2.25.3
SLF4J	2.0.17, 1.7.36
Jetty	9.4.58
ActiveMQ	5.16.7
Tomcat (Avaya Aura® Contact Center)	9.0.111
Tomcat (Avaya Workspaces)	10.1.54
Istio	1.28.1
Kafka Broker (Confluent)	7.2.1
Apache Kafka	3.2
Kubernetes	1.35.2
Container Runtime	Containerd 2.2.1

Table continues…

Software Component	Version in 7.1.2.3
Fluent Bit	4.0.7
Helm	3.18.6
Metrics Server	3.13.0
VMware ESXi	8.0.2 and 9.0.2

Interoperability

Supported features	Versions Tested
Avaya Aura® Contact Center and Avaya Contact Center Select interoperability with latest WebLM 8.x release	WebLM 10.2
Avaya Aura® Contact Center and Avaya Contact Center Select interoperability with Avaya IX Workplace softphone	IX Workplace 3.40 or 3.41
Avaya Aura® Contact Center and Avaya Contact Center Select support for the latest AAMS release	AMS 10.1 or 10.2
Avaya Aura® Contact Center interoperability with Avaya Aura UC current and previous releases	Aura 10.1 or 10.2
Avaya Aura® Contact Center and Avaya Contact Center Select interoperability with the latest and previous AAEP releases	AAEP 8.1.2.2
Avaya Contact Center Select interoperability with the latest and previous Avaya IP Office releases	IPO 12.2 or 12.3
Avaya Aura® Contact Center interoperability with current and previous releases of POM	POM 4.1
Avaya Aura® Contact Center interoperability with current release of CBA	Callback Assist 5.2

Hyper-V Host Requirement for Workspaces

As part of AACC 7.1.2.3 Service Pack, the Workspaces operating system has been migrated from CentOS to Red Hat Enterprise Linux (RHEL) 9.6.

Customers deploying or upgrading the Workspaces Virtual Machine (VM) on Microsoft Hyper-V running on Windows Server 2016 must migrate the Hyper-V host to Windows Server 2019 before deploying or upgrading to AACC 7.1.2.3 Service Pack.

This is a mandatory prerequisite. Due to a known compatibility issue affecting RHEL 9.4 and later kernels on Windows Server 2016 Hyper-V, the Workspaces VM may fail to boot, preventing successful deployment or upgrade of the Workspaces solution.

Deployment Scenario	Action
Workspaces VM hosted on Microsoft Hyper-V running on Windows Server 2016.	Migrate the Hyper-V host to Windows Server 2019 before deploying or upgrading to AACC 7.1.2.3 Service Pack.

Table continues…

Deployment Scenario	Action
Workspaces VM hosted on Microsoft Hyper-V running on Windows Server 2019.	No Action Required.
Workspaces VM hosted on VMware.	No Action Required.
Deployments that do not host the Workspaces VM on Windows Server 2016 Hyper-V.	No Action Required.

Avaya Aura Media Server 8.x Support Change

Avaya Aura Media Server (AAMS) 8.x software bundle and co-resident deployment with Avaya Aura® Contact Center (AACC) or Avaya Contact Center Select (ACCS) 7.1.2.x is no longer supported. The following are the updates:

- The upgrade process removes the AAMS co-resident virtual machine (VM) and the associated AAMS resources and artifacts from the AACC installation.
- Existing AACC or ACCS deployments on physical hardware using AAMS 8.x are no longer supported.
- Customers using AAMS 8.x are required to migrate to a supported AAMS version.
- AACC or ACCS supports AAMS 10.x as an independent deployment.
- For supported AAMS 10.x deployment configurations, refer to the applicable Avaya Aura Media Server 10.x documentation.
- For information about configuring an independent AAMS deployment with AACC or ACCS, refer to the *Avaya Aura Contact Center Server Administration* or *Avaya Contact Center Select Advanced Administration* guides.

Chapter 3: Avaya Aura® Contact Center server commissioning

Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications describes how to prepare the Avaya Aura® Contact Center Release 7.1 server and client software to handle inbound and outbound voice and multimedia contacts. Commissioning the server and client software prepares the hardware to run the contact center. If you want to make additional changes to the contact center server configuration, see *Avaya Aura® Contact Center Server Administration*.

Commission each Avaya Aura® Contact Center application according to your Contact Center configuration. Each Contact Center server type provides different functionalities and installs a different set of Contact Center applications.

The following SIP-enabled Contact Center server types are available in Avaya Aura® Contact Center Release 7.1:

Voice and Multimedia Contact Server — This server provides context sensitive and skill-based routing for customer voice and multimedia contacts. This server also provides routed contact support for email messages, web communications, voice mail messages, scanned documents, fax messages, and SMS text messages. Each SIP-enabled Voice and Multimedia Contact Server requires one or more Avaya Aura® Media Server in the contact center solution. Avaya Aura® Media Server supports SIP-enabled voice contact routing, and it provides conferencing and Agent Greeting capabilities in SIP-enabled contact centers. A Voice and Multimedia Contact Server has the following components:

- Contact Center Manager Server
- Contact Center License Manager
- Contact Center Manager Server Utility
- Contact Center Manager Administration
- Communication Control Toolkit
- Contact Center Multimedia
- Optional Avaya Aura® Media Server

Voice Contact Server Only — This server provides context sensitive and skill-based routing for customer voice contacts. Each SIP-enabled Voice Contact Server requires one or more Avaya Aura® Media Server in the contact center solution. Avaya Aura® Media Server supports SIP-enabled

voice contact routing, and it provides conferencing and Agent Greeting capabilities in SIP-enabled contact centers. A Voice Contact Server has the following components:

- Contact Center Manager Server
- Contact Center License Manager
- Contact Center Manager Server Utility
- Contact Center Manager Administration
- Communication Control Toolkit

Multimedia Contact Server Only — This server increases the number of contact center agents in your enterprise solution. When installed, this server provides the multimedia contact processing capabilities, and the Voice Contact Server processes only voice contacts. A Multimedia Contact Server has the following components:

- Contact Center Multimedia

Network Control Center Server Only — This server adds networking, network skill-based routing, and consolidated reporting support for a number of Voice and Multimedia Contact Servers operating as a single distributed contact center. Use this server to configure contact routing between the Voice and Multimedia Contact Server nodes of a distributed contact center solution. A Network Control Center Server has the following components:

- Contact Center Manager Server — Network Control Center
- Contact Center Manager Administration
- Contact Center License Manager

Avaya Aura® Media Server on Linux — This server provides additional media processing capabilities, and to support Avaya Aura® Media Server High Availability. Avaya Aura® Media Server supports SIP-enabled voice contact routing, and it provides conferencing and Agent Greeting capabilities in SIP-enabled contact centers. Each SIP-enabled Contact Center requires one or more Avaya Aura® Media Server. For large contact centers, or contact centers requiring High Availability, install one or more standalone Avaya Aura® Media Server Linux-based servers.

Prerequisites to Contact Center server commissioning

Install or migrate your Contact Center software. For more information, see *Deploying Avaya Aura® Contact Center DVD for Avaya Aura® Unified Communications* or *Upgrading and Patching Avaya Aura® Contact Center*.

Commissioning tasks for SIP-enabled Contact Center

About this task

This work flow shows you the sequence of tasks you perform to commission the Contact Center software in your SIP-enabled contact center.

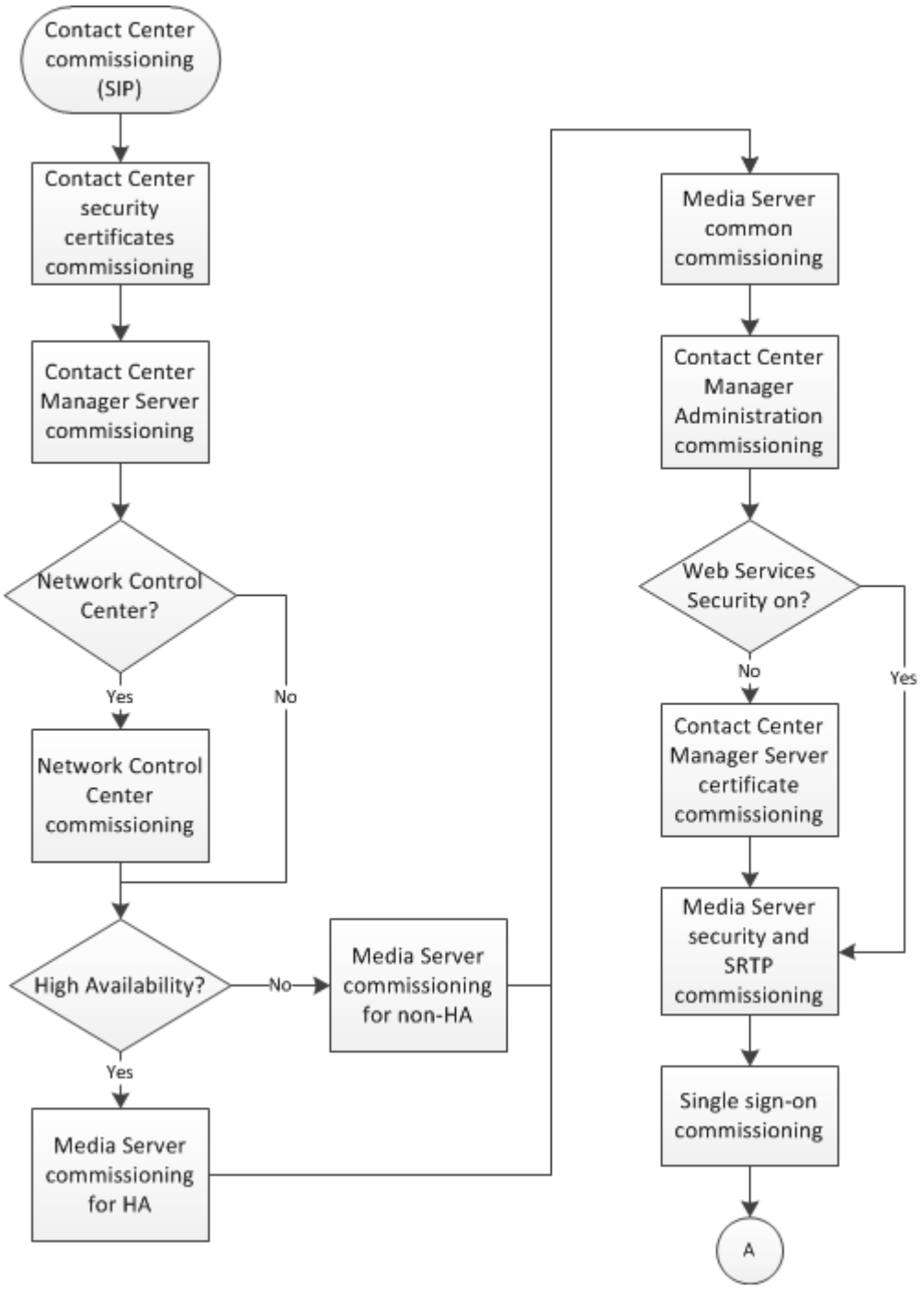


Figure 1: SIP-enabled Contact Center commissioning work flow

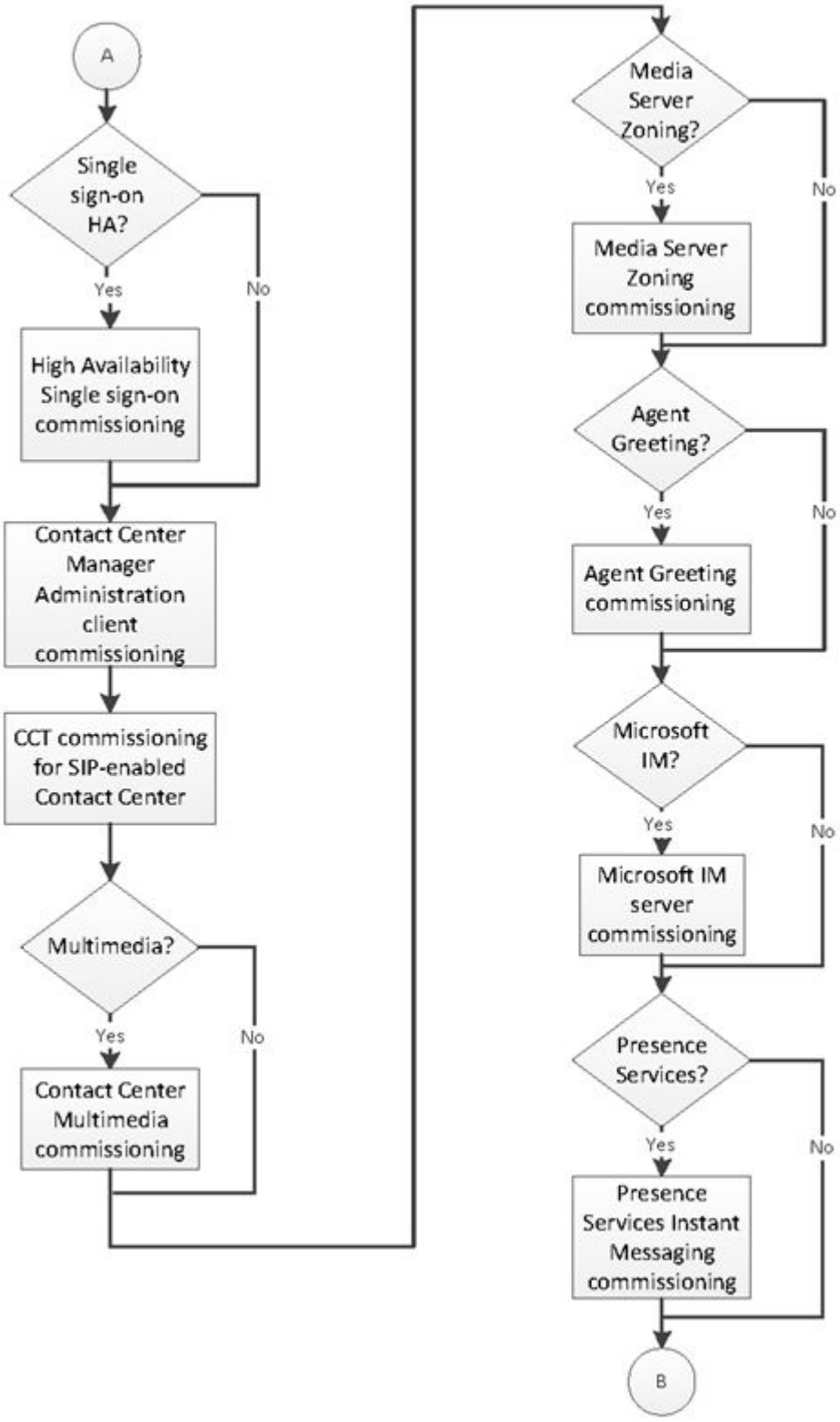


Figure 2: SIP-enabled Contact Center commissioning work flow continued

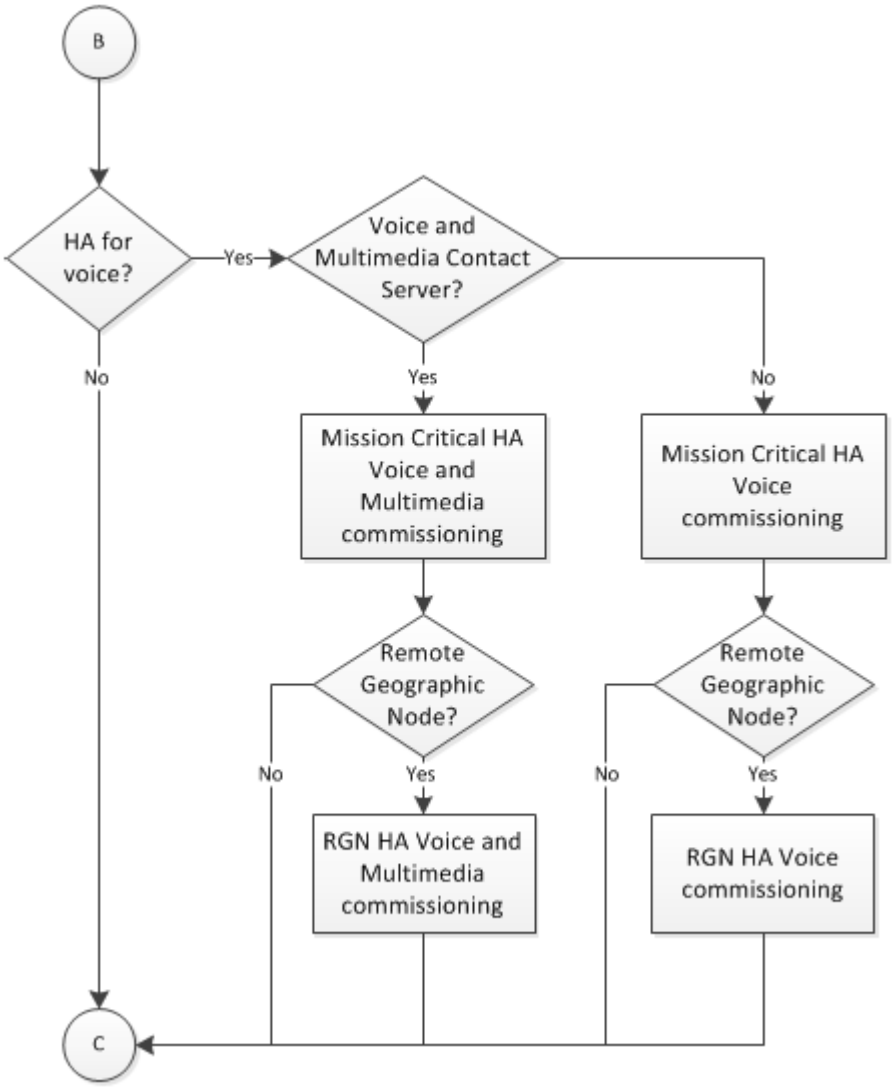


Figure 3: SIP-enabled Contact Center commissioning work flow continued

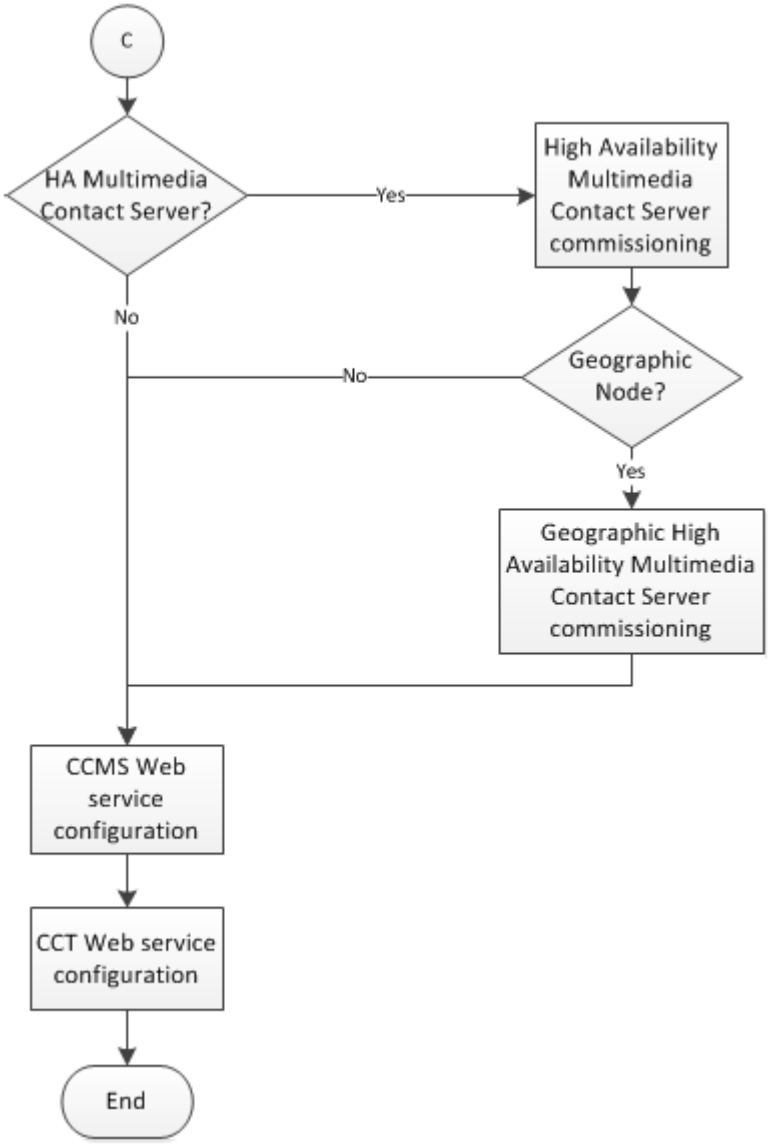


Figure 4: SIP-enabled Contact Center commissioning work flow continued

Chapter 4: Contact Center security certificates commissioning

Contact Center includes a number of services and connections that you can secure using TLS. You can install Contact Center with security enabled for commonly-used web services and CTI connections. Use the Ignition Wizard to create a security store, generate a Certificate Signing Request (CSR), and import a Certificate Authority (CA) root certificate. Use the procedures in this chapter to disable security, or to create and configure a new security store for secure services and connections.

On a new Contact Center installation, you can configure the following connections and services to use TLS:

- Application Enablement Services (AES) CTI call control. TLS is required for AES communication.
- Contact Center Manager Administration (CCMA)
- Contact Center Multimedia (CCMM) Administration
- Agent Desktop
- Multimedia Services
- Orchestration Designer
- Outbound Campaign Management Tool
- Agent Browser application

Contact Center security store

Contact Center includes a security store to enable secure communications over TLS, both between Contact Center applications and with external clients or third party applications. You can create a new security store using Security Manager, including a new signed server certificate and root certificate from a CA, before putting Contact Center into production. Contact Center also uses the Internet Information Services (IIS) security store for some services. In addition, the Contact Center Open Interfaces have unique security stores.

Important:

If you change the Contact Center server name, you must create a new security store and new server certificates. If you plan to change the server name before final production, avoid configuring Contact Center security certificates at this point. Turn off Web Services security and configure the security certificates after changing the server name. For more information about configuring security certificates after commissioning, see *Avaya Aura® Contact Center Server Administration*.

Contact Center automatically backs up a new security store when you create it. This enables you to recover from situations where the store is damaged or deleted before you make a manual backup of the store.

Contact Center Security Manager

Contact Center Security Manager provides an interface for managing the security certificates in the Contact Center security store and the IIS security store. Contact Center supports the management of the IIS security store through Security Manager only. Do not use IIS functions to manage the IIS security store on a Contact Center server. Security Manager supports importing chained certificates and it places these certificates in the Contact Center security store for distribution across the solution.

Supported TLS versions

Contact Center defaults to using TLS 1.2 for secured services and connections. For backward compatibility, Contact Center supports changing the minimum TLS version that Contact Center can negotiate with other systems. This is to interoperate with legacy systems that do not support TLS 1.2. You can set minimum TLS versions separately for the following connections:

- SIP signaling
- CCMA and CCMM administration
- Event Broker Web service (this setting also sets the minimum TLS version used for Web Statistics)

If you change the CCMA and CCMM administration setting, the configuration applies the Windows Server TLS settings, and affects all applications on the server that use Windows Server secure communications technology.

When the Contact Center configuration is for a TLS version lower than 1.2, Contact Center still attempts to negotiate the highest (and most secure) version first, before stepping down to a lower (and less secure) version.

Avaya recommends that you maintain the TLS version settings at the highest possible TLS version, and that you change these settings only when it is certain that parts of your overall contact center solution do not work with the higher TLS version.

Contact Center High Availability

In a High Availability (HA) system, the security stores must use Subject Alternative Names (SANs). Include a SAN for the managed name and the server name. This ensures clients connecting to Contact Center with the managed name do not get warnings that the server certificate name does not match the server name.

Some commercial CAs charge more for signed certificates that use SANs. Plan your HA managed and standby names in advance of creating a new security store.

Multimedia Contact Server deployments

Where you are deploying Contact Center to use both a Voice Contact Server and a Multimedia Contact Server, you must configure security on both servers.

Certificate Authority root certificates

When a client initiates a secure connection with a server, it must have a root certificate from the CA that provided the signed server certificate. If the client does not have a matching root certificate, it does not complete the connection. If the client has a root certificate from a CA, it can trust any

server certificate signed by that CA. You can import a Certificate Authority root certificate at install time using Ignition Wizard or later in the deployment using Security Manager.

If possible, use a single CA to sign all the certificates in your contact center. This simplifies the deployment process because you only need to distribute a single root certificate to all the clients. If you use different CAs to sign certificates for your different servers, you must copy the root certificate from each CA to all the clients in your contact center.

For some Contact Center web services, Contact Center servers can act as clients of other servers. Therefore, you must ensure that the Contact Center servers also have the required CA root certificate(s).

Offline Store

You can create an offline store using Security Manager, which minimizes downtime if you replace your current security store. When your offline store is created, you can swap between the active store and the offline store. You can make the offline store the active store at any point using Security Manager. Stop Contact Center services before making the offline store active. For more information about working with an offline store, see *Avaya Aura® Contact Center Server Administration*.

Security store notifications

Security certificates contain an expiration date and they are not valid after this date. If the security certificates expire, the Contact Center loses call control and stops functioning.

Security Manager provides a security store inspection utility to help you monitor and maintain valid security certificates. You can use Security Manager to schedule a security store inspection task. Security Manager adds the scheduled task to the underlying Windows Task Scheduler. The scheduled task runs the security store inspection utility once a week. The inspection utility checks the status of the security certificates in the Contact Center security store. If any of the security certificates are due to expire within a month, the inspection utility sends a notification email so the Contact Center administrator can refresh the security certificates.

Security Manager provides the notification email; it cannot renew expired security certificates. For uninterrupted contact center functionality, if you receive an email about upcoming certificate expiration dates, you must renew the security certificates before they expire.

Security Manager uses the Microsoft Windows Task Scheduler to schedule the weekly security store inspection. You must ensure that there is a Microsoft Windows user account that has the necessary privileges from which Security Manager can schedule a task on Windows Task Scheduler. You can use the Windows administrator account that you used to install Contact Center to add a task to Windows Task Scheduler.

Security Manager uses a specified SMTP server to send the notification emails. Contact Center does not provide this SMTP server. You must provision the SMTP server and ensure that the Contact Center server can communicate with it at all times. Contact Center does not support SSL connectivity to this SMTP server.

Prerequisites

- Read the security content in *Avaya Aura® Contact Center Overview and Specification*.
- Have a good understanding of security certificates and secure communications.

- Identify the Certificate Authority (CA) that your organization uses to sign security certificates.

Contact Center certificate commissioning procedures for Unified Communications systems

About this task

This task flow shows you the sequence of procedures you perform to commission Contact Center security certificates on Unified Communications based systems.

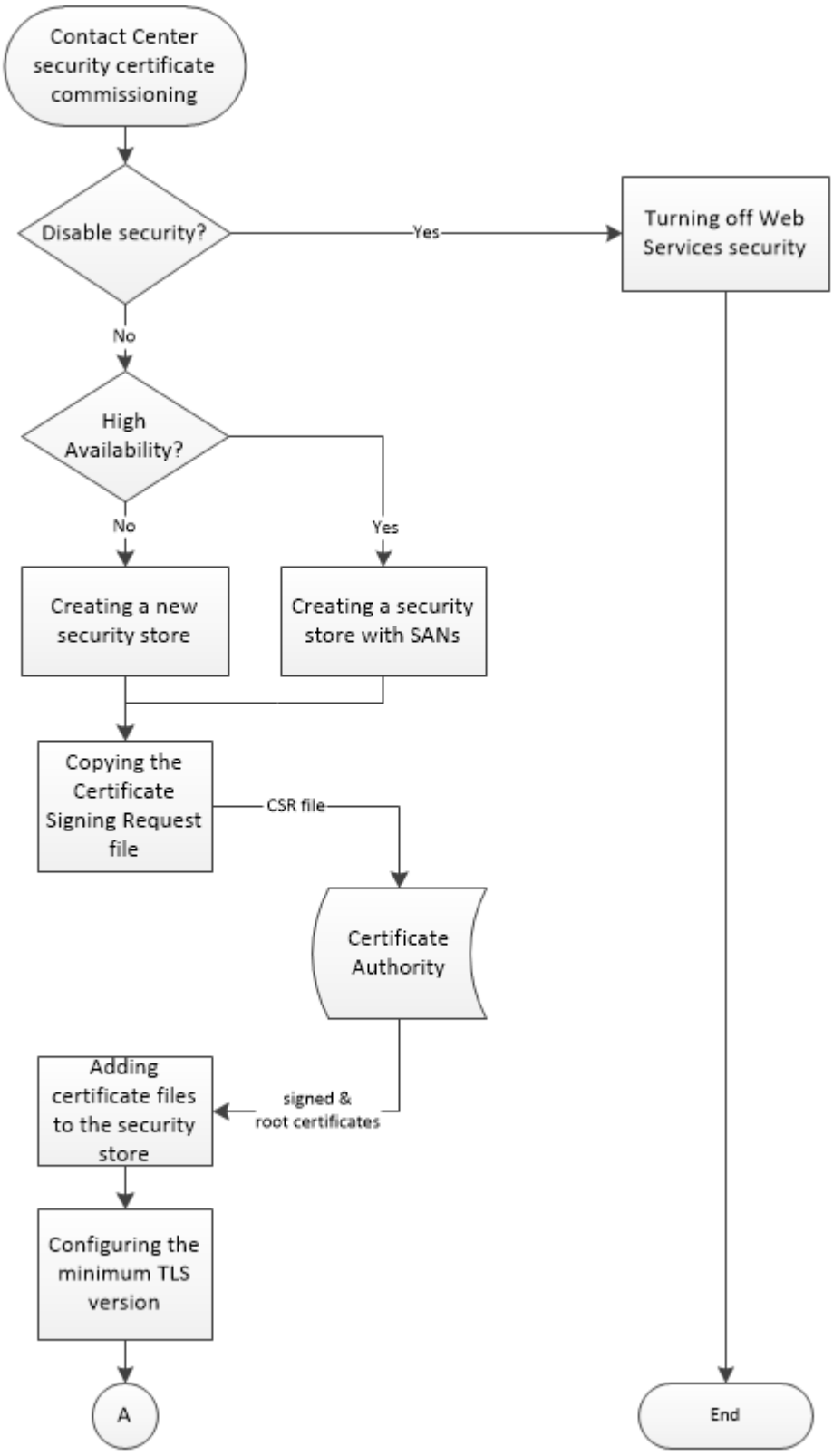


Figure 5: Contact Center certificate commissioning procedures

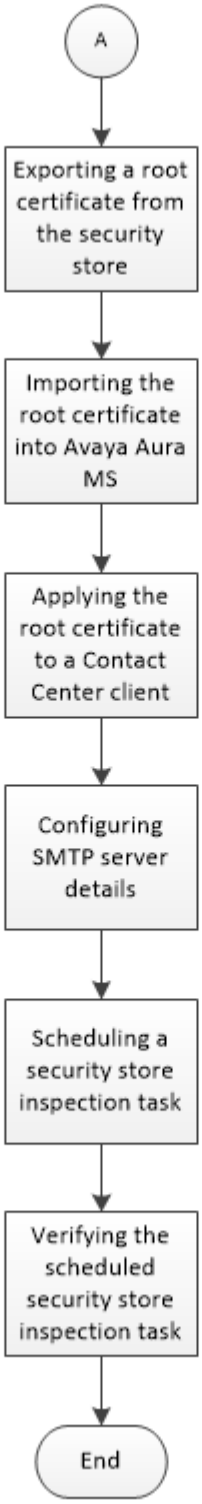


Figure 6: Contact Center certificate commissioning procedures continued

Turning off Web Services security

About this task

Turn off Web Services security if you do not want to use the feature, or if you want to complete Contact Center commissioning without Web Services security enabled.

Before you begin

- Read the security section of *Avaya Aura® Contact Center Overview and Specification*.

Procedure

1. Log on to the Contact Center server as a local administrator.

   Important:

   If you log on to the server as a domain administrator, this procedure does not complete successfully.

2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. On the Store Access dialog, type the password for the security store, and click **OK**.

   If this is the first time you logged on to Security Manager, use the password set at install time. Security Manager prompts you to change the security store password.

4. On the Security Manager screen, select the **Security Configuration** tab.
5. Click **Security Off**.
6. Click **Apply**.
7. On the Security Change Confirmation dialog, click **Confirm**.
8. Click **Log Out**.
9. Restart the Contact Center server.
10. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Next steps

Skip the rest of this chapter and continue with Contact Center commissioning.

With Web Services security disabled, you still must use certificates to secure AES and Agent Browser application communications. Tasks for configuring certificates for these components come later in the commissioning process.

Creating a new security store

About this task

The Security Manager uses a store to hold Certificate Authority root certificates and signed certificates. Create the security store if you plan to use a Certificate Authority and generate signed certificates.

The default encryption setting is SHA2 with a key size of 2048. For backward compatibility, you can choose SHA1 or a key size 1024. However, neither SHA1 nor 1024 provide the industry-recommended level of encryption. If you select one of these values, Contact Center displays a warning message.

If you created a security store at install time using the Ignition Wizard, skip this procedure.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. In the **Security Manager** window, select the **Security Store** tab.
4. In the **Security Store** tab, in the **Full Computer Name (FQDN)** box, type the full FQDN of the server on which you are creating the security store.

   Important:

   The FQDN must be the full machine name of the server that the Security Store resides on. The FQDN name is case-sensitive.
5. In the **Name of Organizational unit** box, type the name of the department or division within the company.
6. In the **Name of Organization** box, type the company name.
7. In the **City or Locality** box, type the name of the city or district in which the contact center is located.
8. In the **State or Province** box, type the state or province in which the contact center is located.
9. In the **Two Letter Country Code** box, type the country code in which the contact center is located.
10. In the **Security Store password** box, type a password for accessing the new security store.
11. In the **Confirm Store password** box, confirm the password for accessing the new security store.

    Important:

    Ensure you remember this password, because you need it the next time you log on to Security Manager. If you forget the password, you are not able to access Security Manager.

12. If you want to change the encryption setting, select the required encryption settings from the **Encryption Algorithm** and **Key Size** drop-down lists.

    The default value for **Encryption Algorithm** is SHA2 and the default value for **Key Size** is 2048.

    Contact Center displays a warning message if you select SHA1 or 1024. Contact Center includes these values for backward-compatibility only, because these settings do not meet the industry-recommended level of encryption.

13. Click **Create Store**.

    Contact Center creates the private key required for private-public key encryption.

    Security Manager automatically displays the Certificate Request tab, showing the newly created Certificate Signing Request file contents.

    Contact Center automatically backs up the new security store to the folder `D:\Avaya\Contact Center\autoBackUpCertStore`. Do not overwrite or delete this backup location.

14. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Variable definitions

Name	Description
Full Computer Name (FQDN)	The host name and parent domain which fully qualifies the computer where the security store is to be created. The FQDN name is case sensitive. The Security Manager auto-populates the FQDN field by reading the name from the operating system. You can modify this field if required. Example FQDN format: computerX.DomainY.com
Name of Organizational unit	The department or division within a company.
Name of Organization	The company name.
City or Locality	The city or district in which the system is located.
State or Province	The state or province in which the system is located.
Two Letter Country Code	The country code in which the system is located.

Creating a security store with Subject Alternative Names

About this task

If you are implementing High Availability in the contact center, generate the security store using Subject Alternative Names (SANs). Include the Managed name and the current server name as SANs.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. In the **Security Manager** window, select the **Security Store** tab.
4. In the **Security Store** tab, in the **Full Computer Name (FQDN)** box, type the full FQDN of the server on which you are creating the security store.

   Important:

   The FQDN must be the full machine name of the server that the Security Store resides on. The FQDN name is case-sensitive.
5. In the **Name of Organizational unit** box, type the name of the department or division within the company.
6. In the **Name of Organization** box, type the company name.
7. In the **City or Locality** box, type the name of the city or district in which the contact center is located.
8. In the **State or Province** box, type the state or province in which the contact center is located.
9. In the **Two Letter Country Code** box, type the country code in which the contact center is located.
10. Under **Subject Alternative Name (SAN)**, for each SAN you want to add:
    a. From the **Type** drop-down list, select DNS.
    b. In the **Value** field, type the FQDN for the server.
    c. Click **Add SAN**.

    For a High Availability system, add the current server name and the Managed name for the HA pair.
11. On the Security Store tab, in the **Security Store password** box, type a password for accessing the new security store.
12. In the **Confirm Store password** box, confirm the password for accessing the new security store.

Important:

Ensure you remember this password, because you need it the next time you log on to Security Manager. If you forget the password, you are not able to access Security Manager.

13. If you want to change the encryption setting, select the required encryption settings from the **Encryption Algorithm** and **Key Size** drop-down lists.

    The default value for **Encryption Algorithm** is SHA2 and the default value for **Key Size** is 2048.

    Contact Center displays a warning message if you select SHA1 or 1024. Contact Center includes these values for backward-compatibility only, because these settings do not meet the industry-recommended level of encryption.

14. Click **Create Store**.

    Contact Center creates the private key required for private-public key encryption.

    Security Manager automatically displays the Certificate Request tab, showing the newly created Certificate Signing Request file contents.

    Contact Center automatically backs up the new security store to the folder `D:\Avaya\Contact Center\autoBackUpCertStore`. Do not overwrite or delete this backup location.

15. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Next steps

Send the Certificate Signing Request file to the Certificate Authority, and receive a signed certificate, so that you can import the signed certificate to the security store.

Copying the Certificate Signing Request file

Before you begin

- Speak with your System Administrator to identify a Certificate Authority.

About this task

Security Manager automatically generates a Certificate Signing Request (CSR) when it creates a new security store. The Security Manager—Certificate Request tab displays the name, location, and contents of the Certificate Signing Request (CSR) file on the server. A Certificate Authority uses this Certificate Signing Request (CSR) file to generate a signed security certificate. Contact Center uses the signed security certificate to establish secure communication links with Application Enablement Services (AES) servers, the Agent Browser application, and Web Services clients.

Until you add a signed certificate, the Signing Request Status field shows the CSR status as Pending. When the CSR is signed, and you add it to the security store using the “Add Certificate Tab”, the status changes to “Signed” to indicate that this CSR has been signed.

Procedure

1. Log on to the Contact Center server containing the security store.
2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. Select the **Certificate Request** tab.
4. Check the **Signing Request Status** value. If this value is **Pending**, you must have the CSR signed by a Certificate Authority.
5. Note the location of the Certificate Signing Request file from **File location**.
6. Select **Logout**.
7. Copy the Certificate Signing Request file from the directory referenced in **File location**, to send to a Certificate Authority.
8. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Next steps

After you perform this procedure, the certificate must be signed by a Certificate Authority. Contact your System Administrator for the preferred method of processing the signed certificate request file to obtain a signed certificate. Send the Certificate Signing Request file to a Certificate Authority and receive a signed certificate and root certificate to import to the security store.

Variable definitions

Name	Description
Security Store Status	Indicates if the Security Store is created.
Signing Request Status	Indicates if the generated Certificate Signing Request that appears is signed and added back into the store. Pending: Security Manager is waiting for a signed certificate to be added back into the store. Signed: Security Manager added the certificate signed by a specific Certificate Authority into the store.
File Location	Location of the Certificate Signing Request file.
Contents	Displays the contents of the Certificate Signing Request file. You can copy this directly from the field and have it signed.

Adding certificate files to the security store

Before you begin

- Use the CSR file from the Contact Center Security Manager to obtain a Certificate Authority signed certificate and root certificate.
- Save the certificate files on the Contact Center server.

About this task

Contact Center Security Manager can add both Certificate Authority root certificates and signed certificates to the security store. Contact Center requires a signed certificate and a corresponding Certificate Authority root certificate to communicate using secure services.

There are two options when adding CA root and signed certificates.

Automatically adding certificates :

You can select a folder that contains signed and root certificates. Security Manager accesses this folder and automatically determines which are signed certificates and which are root certificate and then adds them to the security store accordingly.

Important:

Security Manager attempts to import all files and certificates it finds in the certificate folder. Ensure that the certificate folder contains only Certificate Authority root certificates and signed certificates.

Manually adding certificates :

For manually added certificates, you can browse for individual signed and root CA certificates and add them to the security store, one at a time. Security Manager checks the certificates and does not add signed certificates as root CA certificates.

Procedure

1. Log on to the Contact Center server containing the security store.
2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. On the **Store Access** dialog, type the security store password.
4. Click **OK**.
5. In the Security Manager window, select the **Add Certificate** tab.
6. To add certificates automatically:
    a. Click **Browse**.
    b. On the Select Directory dialog, browse to the directory where you saved the certificate files, and click **Select Directory**.

       Security Manager displays the certificates in the **Certificates** field.
    c. Click **Add all Certificates**.

7. To add certificates manually:
    a. Select **Add Certificates Manually**.
    b. To manually add a Certificate Authority root certificate, click **Browse**.
    c. Browse to the Certificate Authority root certificate, and click **Select File**.
    d. Click **Add CA Certificate**.
    e. To manually add a signed certificate, click **Browse**.
    f. Browse to the Certificate Authority signed certificate, and click **Select File**.
    g. Click **Add Signed Certificate**.
8. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Variable definitions

Name	Description
Security Store password	Password to access the security store.
Add Certificates Automatically	Security Manager automatically determines which certificates are signed and which are root certificate and then adds them to the security store accordingly.
Select folder	The folder from which Security Manager automatically loads certificates.
Add Certificates Manually	Manually add certificates, one at a time.
Add Root Certificate	The name and location of the root certificate. Root Certificate Authority certificates must be in Base64 format.
Add Signed Certificate	The name and location of the signed certificate. Signed certificates must be in DER format.

Procedure job aid

The same root certificate must be applied to the Application Enablement Services so that Contact Center Manager Server (CCMS) can communicate securely with it using TLS. For more information about configuring Application Enablement Services certificates, see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.

Configuring the minimum TLS version

About this task

Configure minimum TLS versions that Contact Center can negotiate for secure connections. This enables third-party and legacy systems that do not support TLS 1.2 to communicate securely with

Contact Center. If you do not change these settings, Contact Center uses only TLS 1.2, and does not connect to systems that support only lower versions of TLS.

You can set minimum TLS versions separately for the following communications:

- SIP and CTI signaling
- CCMA and CCMM administration
- Event Broker Web service (this setting also sets the minimum TLS version used for Web Statistics)

Procedure

1. Log on to the server as a local administrator.

   Important:

   If you log on to the server as a domain administrator, this procedure does not complete successfully.

2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. On the Store Access dialog, type the password for the security store, and click **OK**.
4. On the Security Manager screen, select the **Security Configuration** tab.
5. In the **SIP and CTI Signaling Level** box, select the lowest version of TLS for SIP signaling communication.
6. In the **CCMA — Multimedia Web Service Level** box, select the lowest version of TLS for CCMA and Multimedia Web service communication.

   This changes the setting for IIS, and for Windows Server generally.
7. In the **Event Broker Web Service Level** box, select the lowest version of TLS for Event Broker Web Service communication.
8. In the **Current TLS Level for Cache Database** box, select the lowest version of TLS for Cache Database Level communication.
9. Click **Apply**.
10. Click **Log Out**.
11. Reboot the Contact Center server to complete the procedure.
12. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Exporting a root certificate from the security store

About this task

Export the certificate authority root certificate from the Contact Center security store so that clients using secured services can trust the public key for encryption. Avaya recommends that you

always export the root certificate from the security store, so that it is consistent with the current signed certificate.

Before you begin

- Add a signed certificate and root certificate to the security store.

Procedure

1. Log on to the Contact Center server containing the store.
2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. On the **Store Access** dialog, type the security store password, and click **OK**.
4. In the Security Manager window, select the **Store Maintenance** tab.
5. In the **Root Certificates** field, select the root certificate that you want to export.
6. Click **Export**.
7. On the Select Directory To Export To dialog, select or create a directory to which you want to export the root certificate.
8. Click **Export To**.

   Security Manager exports two files to the directory. The PEM file is for AES and Avaya Aura® MS; the Security Certificate file is for all other clients.
9. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Next steps

Apply the root certificate to all Contact Center clients.

Importing the Contact Center root certificate into Avaya Aura® MS

Before you begin

- Export the root certificate from the Contact Center Security Store, and save the PEM file to a location on the Avaya Aura® MS server.

About this task

Import the Contact Center root certificate into the Avaya Aura® MS trust store to support Transport Layer Security (TLS) communications. You perform this procedure on the Avaya Aura® MS server. If you have multiple Avaya Aura® MS servers, repeat this procedure on each server. Avaya Aura® MS supports importing only the PEM format root certificate file.

Procedure

1. Log on to Avaya Aura® MS Element Manager.
2. Navigate to **EM** > **Security** > **Certificate Management** > **Trust Store**.

3. Click **Import**.
4. In the **Trust friendly name** field, type a friendly name for the CA root certificate.
5. Click **Browse**.
6. Select the root certificate file that you exported from the Contact Center Security Store.
7. Click **Save**.
8. If you have multiple Avaya Aura® MS servers, repeat this procedure on each server.

Applying the root certificate to a Contact Center client

About this task

Copy the root certificate exported from the Contact Center security store to the Contact Center clients and servers that use secure services. If you have a large number of clients, you can use automated methods to distribute and apply the root certificates. For example, you can use a Group Policy to distribute root certificates to clients using supported Microsoft Windows operating systems.

This procedure shows how to manually apply a root certificate on a Microsoft Windows operating system.

Before you begin

- Add a signed certificate and root certificate to the security store.
- Export the root certificate from the security store.

Procedure

1. On the client operating system Desktop, click **Start** > **Run**.
2. Type `MMC`, and click **OK**.
3. Click **File** > **Add/Remove Snap In**.
4. From the **Available snap ins** list, select **Certificates**, and click **Add**.
5. On the Certificates Snap in dialog, select **Computer account**, and click **Next**.
6. Click **Finish**.
7. On the Add or Remove Snap-ins dialog, click **OK**.
8. In the console root, expand **Certificates (Local Computer)** and then expand **Trusted Root Certification Authorities**.
9. Right-click the **Certificates** folder.
10. Select **All Tasks** > **Import**.
11. On the Certificate Import Wizard dialog, click **Next**.
12. Click **Browse**, and browse to the location where you copied the root certificate file.

13. Select the root certificate file and click **Open**.
14. On the Certificate Import Wizard dialog, click **Next**.
15. Click **Next**.
16. When the Certificate Import Wizard finishes importing the certificate, click **Finish**.

Configuring SMTP server details

Before you begin

- Provision, configure, and maintain a Simple Mail Transport Protocol (SMTP) server. Contact Center Security Manager supports Microsoft Exchange Server.
- Know the authentication logon account and password details for the SMTP server.
- Ensure that the Contact Center server can access the SMTP server at all times.
- On the SMTP server, configure an email address for the contact center administrator. Security Manager sends the notification emails to this address. Ensure the contact center administrator monitors this email address.
- On the SMTP server, configure an email address for Avaya Aura® Contact Center Security Manager. Security Manager can then use this email address to send notification emails.

About this task

Configure the details of the SMTP server and accounts used to send the Security Manager status report email.

Procedure

1. On the **Security Manager** screen, select the **Expiration Alerts** tab.
2. Select **SMTP Configuration**.
3. From the **Outgoing e-mail server (SMTP)** list, select **IP** or **Address**. The Contact Center server must be able to communicate with the SMTP server by IP address or SMTP address.
4. In the **Outgoing e-mail server (SMTP)** box, enter the IP address or SMTP address of the SMTP server.
5. In the **Port number** box, enter the TCP port number for the SMTP server. The default port number is 25.
6. In the **Sender e-mail address** box, enter the email address to be used by Security Manager to send notification emails. Ensure this email address is registered with the SMTP server.
7. In the **Recipient e-mail address** box, enter the email address to which Security Manager is to send the notification emails. Ensure this email address is registered with the SMTP server. This is typically the contact center administrator’s email address. You must monitor this email address for notifications about the status of Contact Center security certificates.

8. If your SMTP server requires authentication, select **SMTP server requires authentication**. If your SMTP server does not require authentication, clear this check box.
9. In the **User name** box, enter the user account name used to authenticate with the SMTP server.
10. In the **Password** box, enter the password of the user account used to authenticate with the SMTP server.
11. Click **Save Configuration**.
12. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Scheduling a security store inspection task

Before you begin

- Configure the SMTP server and email account details.

About this task

Schedule a security store inspection task. Security Manager adds the scheduled task to the underlying Windows Task Scheduler. The scheduled task runs the security store inspection utility once a week. You can select the time and day of the week that the security store inspection task runs during the week.

Procedure

1. Log on to the Avaya Aura® Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. Select **Expiration Alerts** > **Schedule Alerts**.
4. From the **Day of week** list, select the day on which to schedule the weekly inspection task.
5. In the **Time (24 hr)** section, enter the time of day on which to schedule the weekly inspection task. Use twenty four hour format time.
6. In the **User** box, enter the name of a Windows user account that has the privileges necessary to access the Windows Task scheduler and schedule the task.
7. In the **Password** box, enter the password of the Windows user account that has the privileges necessary to access the Windows Task scheduler and schedule the task.
8. Click **Apply Schedule**.

   Security Manager then schedules this task on the underlying Microsoft Windows Task Scheduler. After successfully scheduling the task, the name on the **Apply Schedule** button changes to **Modify Schedule** and the button is disabled. To enable the **Modify Schedule** button, select a new time. You can then update the scheduled task time by clicking **Modify Schedule**.

9. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Verifying the scheduled security store inspection task

Before you begin

- Configure the scheduled task.

About this task

Verify that the Windows Task Scheduler lists the Security Manager scheduled inspection task. Do not modify the scheduled task in Task Scheduler. Use only Security Manager to modify the scheduled inspection task.

Procedure

1. Log on to the Contact Center server.
2. On the **Start** screen, under **Administrative Tools**, click **Task Scheduler**.
3. In the left pane, click **Task Scheduler Library**.
4. In the middle pane, confirm that there is a task named **aaccSentinel**.
5. Confirm that the task **Status** is **Ready**.
6. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Chapter 5: Contact Center Manager Server commissioning

Use the procedures in this section to configure the Contact Center Manager Server software in your Avaya Aura® Contact Center. The procedures outlined include configuring your passwords, configuring features and verifying the success of your installation to prepare your server for Contact Center operations.

Contact Center Manager Server commissioning procedures

About this task

This task flow shows you the sequence of procedures you perform to configure Contact Center Manager Server.

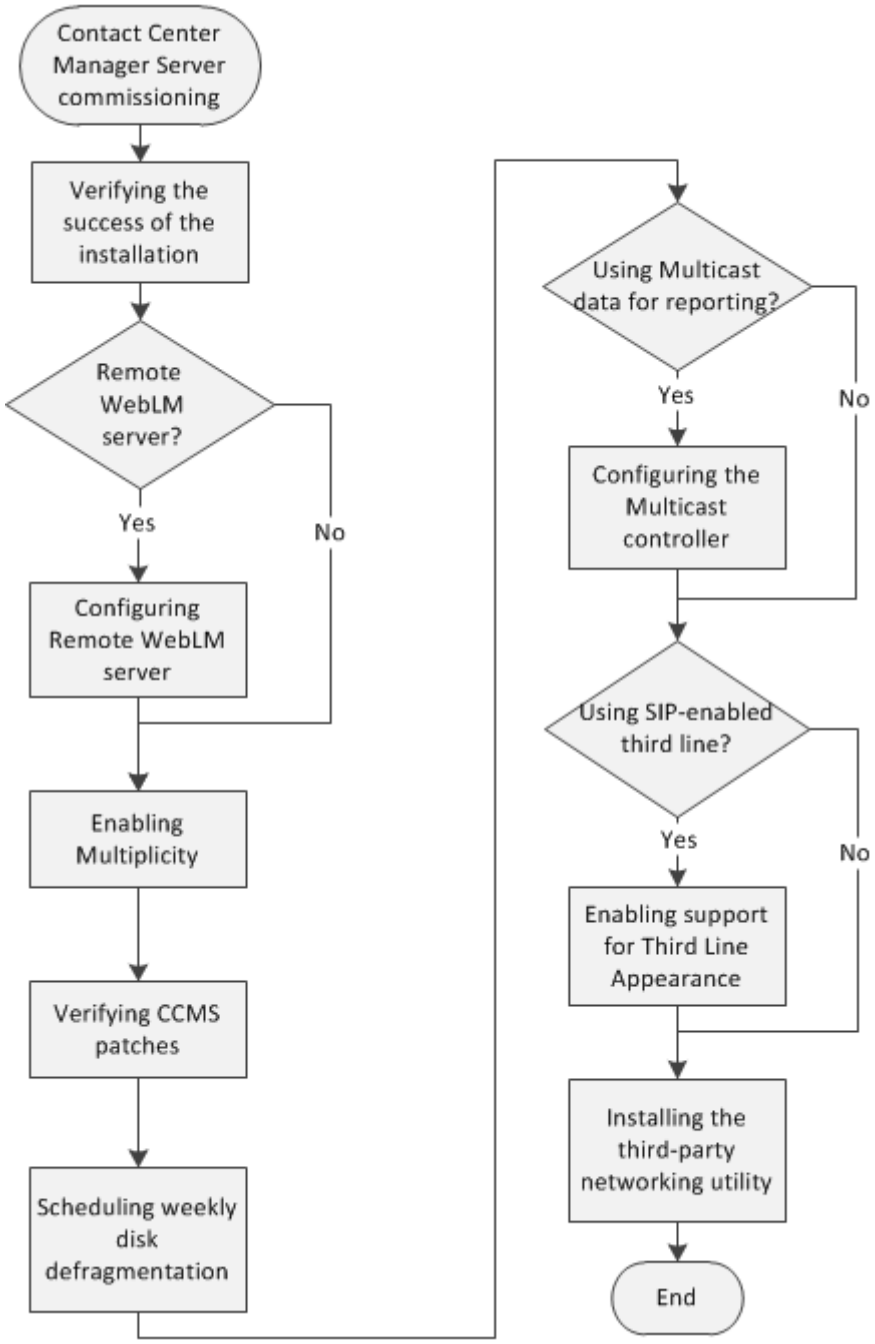


Figure 7: Contact Center Manager Server commissioning procedures

Verifying the success of the installation

Before you begin

- Install the Contact Center software.

About this task

Verify the success of your installation to ensure that all components are installed. To verify the success of the installation, ensure that the Contact Center services are running.

Procedure

1. Log on to the Contact Center server as an administrator.
2. From the **Start** menu, in the Avaya area, click **System Control and Monitor Utility**.
3. On the **LM**, **CCMS**, **CCMA**, **CCT**, and **CCMM** tabs, check that all relevant services are in the **Up** state.

   The **CCMM** tab is not present on a Voice Contact Server.
4. Close the System Control and Monitor Utility window.

Applying the local WebLM license file

About this task

If you have a virtualized solution, you cannot apply your local WebLM license during the installation process. Use the License Manager Configuration Tool to apply your local WebLM license file.

Procedure

1. Log on to the server where the Contact Center License Manager software is installed.
2. From the **Start** menu, in the Avaya area, click **License Manager Configuration**.
3. Select the **Configuration** tab.
4. Under **License Type**, select **Local WebLM**.
5. Under **License Location**, click **Browse File**.
6. Navigate the file system and locate the new license file.
7. Click **Open**.
8. On the License Manager Configuration Tool window, click **Apply**.
9. On the pop-up dialog, click **Yes** to restart Contact Center License Manager.
10. Click **Close** to close the window.

Configuring remote WebLM server

About this task

Configure Contact Center License Manager to use a remote Avaya WebLM server. Contact Center License Manager can obtain licenses from a remote Avaya WebLM server, and then use these licenses to control Avaya Aura® Contact Center licensed features.

Refer to the Avaya WebLM documentation for instructions on applying your updated license file on the remote Avaya WebLM server.

Procedure

1. Log on to the server where the Contact Center License Manager software is installed.
2. From the **Start** menu, in the Avaya area, click **License Manager Configuration**.
3. Select the **Configuration** tab.
4. From the **License Type** list, select **Remote WebLM**.
5. Under **WebLM Configuration**, in the **Host** box, type the IP address or FQDN of the remote Avaya WebLM server.
6. In the **Port** box, type the port number to use for the remote Avaya WebLM server. The default port number is 52233.
7. Click **Apply**.

   Contact Center applies the license and updates the WebLM URL.
8. On the **LMConfig** dialog, click **Yes** to restart the Contact Center License Manager server.
9. Click **OK** to close the window.
10. Click **Exit**.

Enabling Multiplicity

Before you begin

- Ensure that the Contact Center License Manager is licensed to provide Multiplicity.
- Ensure that the Contact Center License Manager is licensed to provide agent licenses for the required contact types.

Important:

You must restart your server at the end of this procedure.

About this task

Enable Multiplicity to allow agents manage multiple contact types at the one time. Configure multiplicity presentation classes (MPC) in Contact Center Manager Administration (CCMA). Each

agent is assigned either the default MPC or a customized MPC. Enable multiplicity in the licensing tab of the Server Configuration utility.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Server Configuration**.
3. Click the **Licensing** tab.
4. From the **Features** list, select **Multiplicity.**
5. Click **Apply All**.
6. On the **Restart Required** dialog, click **Yes** to restart the server.

Procedure job aid

After you restart Contact Center Manager Server, Multiplicity is enabled. Configure contact center agents for multiplicity in Contact Center Manager Administration using Multiplicity Presentation Classes. For more information, see the *Avaya Aura® Contact Center Client Administration*.

Scheduling weekly disk defragmentation

About this task

Schedule daily disk defragmentation for all drives to optimize performance and avoid potential outages.

Procedure

1. Log on to the Contact Center server.
2. On the **Start** screen, select **This PC**.
3. Right-click drive C and select **Properties**.
4. Click the **Tools** tab.
5. Select **Optimize**.
6. Click **Change settings**.
7. Select **Run on a schedule (recommended)**.
8. Under **Frequency**, select **Weekly**.
9. Click **Choose**.
10. On the **Optimize Drives** window, click **Select all**.
11. Click **OK**.
12. Click **OK**.

13. Click **Close**.

Configuring the Multicast controller

About this task

Configure the Multicast controller if you plan to use the IP Multicast delivery method to send Real Time Reporting data. Multicast is a network addressing method for delivering information to a group of destinations in a one-to-many distribution.

If you plan to use the unicast delivery method, no configuration of Contact Center Manager Server is required and you can skip this procedure. For Unicast delivery, only one user can log on at a time and you must ensure that you disconnect all terminal services sessions.

For more information about multicast and unicast, see *Avaya Aura® Contact Center Overview and Specification*.

You can enable compression of multicast data to conserve network bandwidth. For example, enable RTD Compression to reduce the bandwidth usage between the CCMS server and any CCMA server from which it is managed. Use RSM compression only if you use a third-party or custom application to provide real time displays. Enabling RSM compression disables both the CCMA Real Time Displays feature and POM integration.

Procedure

1. Log on to the Contact Center server as an administrator.
2. From the **Start** menu, in the Avaya area, click **Multicast Stream Control**.
3. In the **RTD Multicast Controller** dialog box, select the check boxes for the Real Time data to enable.
4. If you want to conserve bandwidth between the CCMS server and CCMA servers, in the **Compression** section of the window, select the **RTD Compression** check box.
5. If you are using a third-party or custom real time display application, to conserve bandwidth, select the **RSM Compression** check box.

   The third-party or custom application must be capable of processing a compressed data stream. For more details, see the SDK documentation.
6. Click **Apply**.
7. Click **OK**.
8. From the **Start** menu, in the Avaya area, click **Multicast Address and Port Configuration**.
9. In the **RTD Multicast Configuration** dialog box, in the **Multicast IP group** box, type the multicast IP address for Contact Center Manager Server to use to transmit the RTD.

   This is the same address as the Contact Center Manager Administration server receiving IP multicast address.

10. In the **Multicast Time To Live (TTL)** box, accept the default setting for the number of network hops packets can transition

    OR

    Type a new value.

    Important:

    Do not change the ports.

11. For the **Interval to Date**, **Moving Window IP Port**, and **Multicast Rate** boxes, accept the default values.
12. Click **Apply**.
13. Click **OK**.
14. From the **Start** menu, in the Avaya area, click **System Control and Monitor Utility**.
15. Click the **CCMS** tab.
16. In the **Enter password** box, type the Process Monitor – Common Utilities password.
17. Right-click **SDP_Service**.
18. Click **Restart**.

Enabling support for Third Line Appearance

About this task

Enable Avaya Aura® Contact Center support for the third Call Appearance button on Communication Manager agent stations.

Note:

You must restart Avaya Aura® Contact Center at the end of this procedure.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Server Configuration**.
3. In the **Server Configuration** dialog box, under **SIP**, click the **Local Subscriber** tab.
4. From the **SIP Server Version** list, select **6.2 or Greater**.
5. Select **Third Line Enabled**.
6. Click **Apply All**.
7. On the **Restart Required** dialog, click **Yes**.

Installing the third-party networking utility

About this task

Install a third-party utility required by Avaya Aura® Contact Center to support managed IP addresses and to monitor for High Availability switchovers.

Procedure

1. Log on to the Contact Center server.
2. Using Windows Explorer, navigate to <installation drive>:\Avaya\Contact Center\Manager Server\CCSMMC\thirdparty\winpcap.
3. Double-click **WinPcap_4_1_3.exe**.
4. On the WinPcap installer dialog, click **Next**.
5. On the WinPcap installer **Setup Wizard** dialog box, click **Next**.
6. On the WinPcap installer **License Agreement** dialog box, click **I Agree**.
7. On the WinPcap installer **Installation options** dialog box, click **Install**.
8. On the WinPcap installer dialog, click **Finish**.

Chapter 6: Network Control Center commissioning

Configure the communications database to enable the distribution of information from the Network Control Center (NCC) database to all servers on the network and to enable communication and network skill-based routing (NSBR) among multiple sites. The communications database lists all servers in the network, including each IP addresses and status.

Prerequisites for Network Control Center commissioning

- Install the Network Control Center server software.
- Install a Contact Center Manager Server at each site.
- Install and commission the Contact Center License Manager software.
- Install and commission Contact Center Manager Administration.
- If you use an Avaya Communication Server 1000, configure the following elements:
  - NACD (not required for Universal Networking)
  - a CDN for the server to use as an MCDN Network CDN (not required for Universal Networking)
  - Landing Pads (required for Universal Networking only)
  - a dialing plan to facilitate call routing between the telephony switches
- Ensure that all site names and the CLAN IP addresses are unique.

Configuring the sites

About this task

Configure the sites on the networked Avaya Aura® Contact Center on the Network Control Center server to designate the site names and locations.

Procedure

1. On the Network Control Center server, on the **Desktop** screen, right-click on the Windows icon and select **Run**.
2. In the **Open** box, type `nbconfig -admin`.
3. Click **OK**.
4. Click the **Site Table** tab.

   Important:

   Do not select the **Force Synchronization** check box. When you force synchronization, you force each site in the network to request address table information from every other site in the network. This can result in unnecessary use of network bandwidth. (Normally, servers request address table updates only when the NCC notifies them that the site list changed.) Use the **Force Synchronization** option if information at a site is not updated.
5. Click **Add**.
6. In the **CLAN IP Address** box, enter the CLAN IP address of the server.

   Important:

   Each server must have a unique CLAN IP address. You must ensure that you use the correct IP address. You can check the server IP address on the Local Settings tab of the Server Configuration utility.
7. Click **OK**.
8. Repeat step 5 on page 58 to step 7 on page 58 for each server on your network.
9. After you add the servers, click **Verify** to validate the connection to the nodal servers.
10. If all site names are correct, click **Apply** to update the database and synchronize the site table.

    The **Flags** column shows the progress of synchronization.
11. Click **Refresh** to update the status of the flags.

    Synchronization is complete when an **N** appears in the **Flags** column beside the NCC, and an **S** appears beside each server.
12. Click the **Address Table** tab.

    The communication addresses of the new servers appear on the Address Table page.
13. Click the **OK** button on the Nbconfig window.

Chapter 7: Avaya Aura® Media Server commissioning for non-HA deployments

Perform the procedures in this chapter in sequential order. Only use this chapter to commission Avaya Aura® Media Server if your Contact Center deployment does *not* include High Availability. For a deployment with High Availability, see Avaya Aura Media Server commissioning for HA deployments on page 66.

Avaya Aura® Media Server is only supported in SIP-enabled contact centers. It provides media processing for Avaya Aura® Contact Center.

In a non-HA deployment of Avaya Aura® Media Server, the following configuration options are available:

- A single standalone Avaya Aura® Media Server on a Red Hat Enterprise Linux (RHEL) 64-bit operating system. RHEL must be installed with the English language selected.
- Multiple Avaya Aura® Media Server systems, each installed on a server with the RHEL 64- bit operating system. RHEL must be installed with the English language selected.

The servers in an Avaya Aura® Media Server cluster must all use the same RHEL operating system. Avaya Aura® Media Server does not support clusters with mixed operating systems.

WebLM licensing

When you configure Avaya Aura® Media Server as a Media Server in Contact Center Manager Administration, Contact Center License Manager pushes the license keys to that Avaya Aura® Media Server. Restart the Avaya Aura® Media Server so it can acquire the licenses.

Avaya Aura® Media Server cluster replication

An Avaya Aura® Media Server cluster is a collection of nodes that work together closely. Avaya Aura® Media Server clusters offer improved redundancy and performance. A cluster has one primary Avaya Aura® Media Server, one secondary Avaya Aura® Media Server, and up to six standard Avaya Aura® Media Serversystems. The cluster performs automatic Content Store replication of system and application configuration data from the primary Avaya Aura® Media Server to the secondary and standard Avaya Aura® Media Servers.

Avaya Aura® Media Server uses a custom password-protected account to secure Content Store replication. Each Avaya Aura® Media Server in the cluster must be configured with the same replication account username and password details. The replication account is a custom account used to secure the Avaya Aura® Media Server Content Store during replication. It is not a Linux operating system account.

Avaya Aura® Media Server non-HA commissioning checklist

The following is a list of key configuration items required for non-High Availability (HA) commissioning.

Item	Your value	Description
Standalone Avaya Aura® Media Server name		The server name of your standalone Avaya Aura® Media Server.
Standalone Avaya Aura® Media Server IP address		The IP address of your standalone Avaya Aura® Media Server.
Element Manager – User ID		The User ID used to log on to Avaya Aura® Media Server Element Manager.
Element Manager – Password		The password used to log on to Avaya Aura® Media Server Element Manager.
Primary Avaya Aura® Media Server IP address		The IP address of your primary Avaya Aura® Media Server.
Primary Avaya Aura® Media Server Universally Unique Identifier (UUID)		The UUID of the primary Avaya Aura® Media Server. The UUID is required for cluster replication.
Cluster replication account Username		The username of the Avaya Aura® Media Server replication account.
Cluster replication account Password		The password of the Avaya Aura® Media Server replication account.
Secondary Avaya Aura® Media Server IP address		The IP address of your secondary Avaya Aura® Media Server.
Standard 1 Avaya Aura® Media Server IP address		The IP address of the first standard Avaya Aura® Media Server in the cluster.
Standard 2 Avaya Aura® Media Server IP address		The IP address of the second standard Avaya Aura® Media Server in the cluster.
Standard 3 Avaya Aura® Media Server IP address		The IP address of the third standard Avaya Aura® Media Server in the cluster.
Standard 4 Avaya Aura® Media Server IP address		The IP address of the fourth standard Avaya Aura® Media Server in the cluster.

Logging on to Avaya Aura® Media Server Element Manager

Before you begin

- Obtain a valid user name and password to access Avaya Aura® Media Server Element Manager.

About this task

Log on to the Avaya Aura® Media Server Element Manager to configure Avaya Aura® Media Server.

Element Manager (EM) is a web-based administration tool that facilitates the Operation, Administration, and Maintenance (OAM) of Avaya Aura® Media Server. A SIP-enabled Contact Center solution must contain one or more Avaya Aura® Media Server servers.

Note:

You must have more than one Avaya Aura® Media Server account managed by separate users. If one account is disabled or lost, another account can perform critical tasks, backups or recovery. For more information, see *Implementing and Administering Avaya Aura® Media Server*.

Procedure

1. Start a Web browser.
2. In the address box, type the following URL:

   `https://SERVER_IP_ADDRESS:8443/em`

   Where SERVER_IP_ADDRESS is the IP address of the Avaya Aura® Media Server.
3. In the **User ID** box, type the Avaya Aura® Media Server User ID log on account name. The default user account name is `Admin`.
4. In the **Password** box, type the Element Manager password. Use the `Admin` account password. The default password is `Admin123$`.
5. Click **Sign In**.

Configuring the primary Avaya Aura® Media Server for the cluster

About this task

Designate an Avaya Aura® Media Server as the primary server for a cluster, and create a replication username and password.

Avaya Aura® Media Server uses a custom password protected account to secure Avaya Aura® Media Server Content Store replication. Each Avaya Aura® Media Server in the cluster must be configured with the same replication account username and password details.

Procedure

1. Log on to the Element Manager for the primary Avaya Aura® Media Server.
2. In the navigation pane, click **Cluster Configuration**.
3. Select **Server Designation**.

4. Under **Local Server**, select **Primary** from the **Role** list.
5. Under **Replication Account**, select the **Enable Replication Account** check box.
6. In the **Username** box, type a username for the replication account. This value is arbitrary, but you must use the same value for all servers in the cluster.
7. In the **Password** box, type a password for the replication account. This value is arbitrary, but you must use the same value for all servers in the cluster.
8. Confirm the password and click **Save**.
9. Under **Local Server**, note the **UUID** value. You must enter this value on the other servers in the cluster.

Procedure job aid

Configure an Avaya Aura® Media Server as a primary server so that other servers in the cluster can replicate configuration from it.

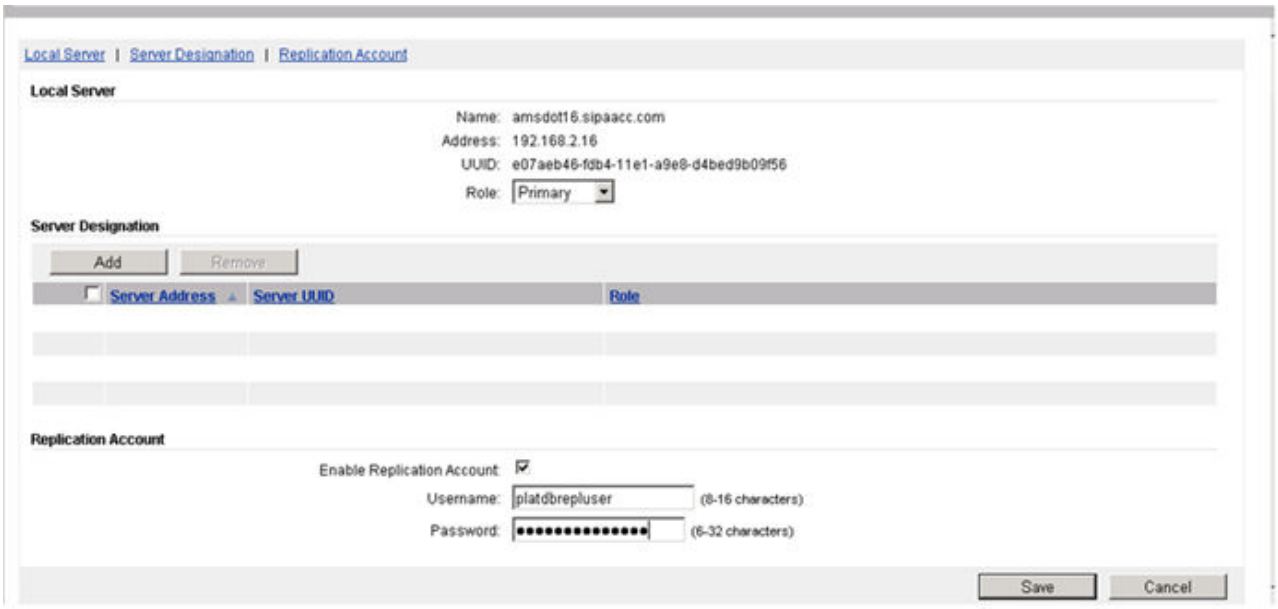


Figure 8: Example of configuring an Avaya Aura® Media Server as a primary server

Configuring a secondary Avaya Aura® Media Server for the cluster

Before you begin

- Designate an Avaya Aura® Media Server as the primary server for a cluster, and create a replication username and password.

About this task

Designate a secondary Avaya Aura® Media Server for the cluster. Configure the secondary server with the primary Avaya Aura® Media Server UUID and IP address, and enter the replication account details.

Avaya Aura® Media Server uses a custom password protected account to secure Avaya Aura® Media Server Content Store replication. Each Avaya Aura® Media Server in the cluster must be configured with the same replication account username and password details.

Procedure

1. Access the Element Manager for the secondary Avaya Aura® Media Server.
2. In the navigation pane, click **Cluster Configuration**.
3. Select **Server Designation**.
4. Under **Local Server**, select **Secondary** from the **Role** list.
5. Under **Server Designation**, type the UUID of the Primary server in the **Primary Server UUID** box.
6. Type the primary server IP address in the **Primary Server Address** box.
7. Under **Replication Account**, select the **Enable Replication Account** check box.
8. In the **Username** box, type the username for the replication account that you specified on the primary server.
9. In the **Password** box, type the password for the replication account that you specified on the primary server.
10. Confirm the password and click **Save**.

Procedure job aid

Configure the secondary Avaya Aura® Media Server to enter the primary server UUID and IP address, and the replication account for the cluster.

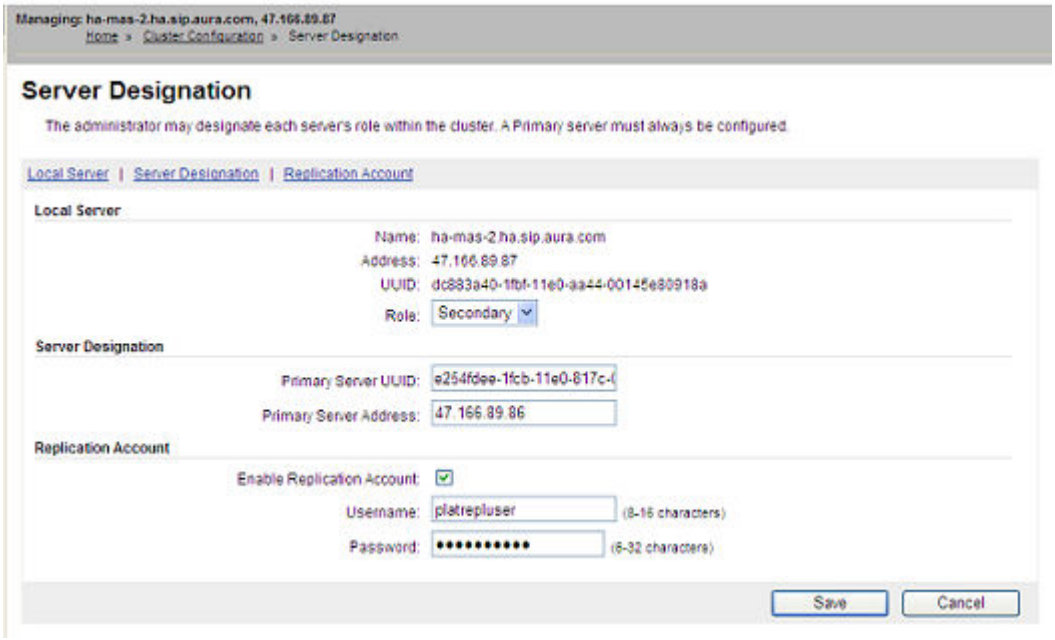


Figure 9: Example of designating an Avaya Aura® Media Server as a secondary server

Configuring a standard Avaya Aura® Media Server for the cluster

Before you begin

- Designate an Avaya Aura® Media Server as the primary server for a cluster, and create a replication username and password.
- Designate a secondary Avaya Aura® Media Server for the cluster.

About this task

Designate any remaining Avaya Aura® MS servers as standard servers for the cluster. Configure each standard Avaya Aura® Media Server with the primary Avaya Aura® Media Server UUID and IP address, and enter the replication account details.

Avaya Aura® Media Server uses a custom password protected account to secure Avaya Aura® Media Server Content Store replication. Each Avaya Aura® Media Server in the cluster must be configured with the same replication account username and password details.

Procedure

1. Access the Element Manager for the standard Avaya Aura® Media Server.
2. In the navigation pane, click **Cluster Configuration**.
3. Select **Server Designation**.

4. Under **Local Server**, select **Standard** from the **Role** list.
5. Under **Server Designation**, type the UUID of the Primary server in the **Primary Server UUID** box.
6. Type the primary server IP address in the **Primary Server Address** box.
7. Under **Replication Account**, select the **Enable Replication Account** check box.
8. In the **Username** box, type the username for the replication account that you specified on the primary server.
9. In the **Password** box, type the password for the replication account that you specified on the primary server.
10. Confirm the password and click **Save**.

Chapter 8: Avaya Aura® Media Server commissioning for HA deployments

Use the procedures in this chapter to commission Avaya Aura® Media Server if yourContact Center uses High Availability. If your deployment does not include HA, see Avaya Aura Media Server commissioning for non-HA deployments on page 59.

HA ensures uninterrupted availability of media processing and reduces loss of processing data when an Avaya Aura® Media Server fails. This provides call protection to the Contact Center.

High Availability uses two media servers operating in a standby deployment. Both the servers have identical configuration and provide full media processing capabilities. Give one of the servers the role of the active (primary) server in the HA pair and the other server is then the standby (backup) server.

Both the primary and backup servers communicate with each other using a heartbeat mechanism. Interruptions in the heartbeat from the primary server trigger a failover to the backup server. Since both the primary and backup servers are identical in functionality and configuration, the failover is seamless to Contact Center.

The following considerations apply to Avaya Aura® Media Server systems with High Availability:

- High Availability can be configured only in a 1+1 configuration (an HA pair).
- High Availability is available only if the Avaya Aura® Media Servers are installed standalone on RHEL operating system.

You can perform a manual failover on the active Avaya Aura® Media Server, and this Avaya Aura® Media Server becomes the standby server while the other becomes the active server.

One Avaya Aura® Media Server HA pair supports up to 1000 agents, without SIP call recording. To configure more than 1000 agents in an HA SIP Contact Center, deploy multiple Avaya Aura® Media Server HA pairs and configure replication from the primary server of one of the HA pairs.

You must still configure each Avaya Aura® Media Server HA pair separately in Contact Center Manager Administration. For each Avaya Aura® Media Server HA pair, configure one media server using the Service IP address of the Avaya Aura® Media Server replicating pair.

WebLM licensing

When you configure an Avaya Aura® Media Server as a Media Server in Contact Center Manager Administration, Contact Center License Manager pushes the license keys to that Avaya Aura® Media Server. You must restart the Avaya Aura® Media Server so it can acquire the licenses.

Avaya Aura® Media Server HA replication

High Availability content store replication ensures both Avaya Aura® Media Servers from each High Availability pair have the same configuration details. If your solution has more than one Avaya Aura® Media Server High Availability pair, Avaya Aura® Media Server Content Store replication ensures each HA pair is synchronized with the designated master High Availability pair. High Availability performs automatic Content Store replication of system and application configuration data from the primary Avaya Aura® Media Server to the backup Avaya Aura® Media Server.

A custom password-protected account secures Content Store replication. Each Avaya Aura® Media Server in a High Availability solution must be configured with the same replication account username and password details. The replication account is a custom account used to secure the Avaya Aura® Media Server Content Store during replication. It is not a Linux operating system account.

Avaya Aura® Media Server remote site HA

In Contact Center High Availability solutions with a remote site, Avaya Aura® Media Server supports the following deployments at the Contact Center remote site:

- Standalone Avaya Aura® Media Server
- Avaya Aura® Media Server cluster
- Avaya Aura® Media Server High Availability pair

This chapter describes, as a worked example, how to configure multiple Avaya Aura® Media Server HA pairs at the campus site and how to configure the Avaya Aura® Media Server cluster at the remote site. The other options (standalone and High Availability) are also supported at the remote site. The concepts and instructions to commission them are also described in this chapter.

Prerequisites

- Read *Avaya Aura® Contact Center Overview and Specification*.
- Install two Avaya Aura® Media Server systems on the Red Hat Enterprise Linux 64-bit operating system. You must install RHEL with the English language selected.
- Choose one server to use as the primary server and the other as the backup server.
- Select a managed IP address for the HA pair. You must configure the managed IP address on both the primary and the backup servers.
- Ensure both servers can ping their own FQDN and the other server's FQDN, either by modifying the server hosts files or by entering appropriate entries on the network DNS server.

Important:

This task flow requires restarting both Avaya Aura® Media Servers.

Avaya Aura® Media Server High Availability commissioning procedures

About this task

This task flow shows the sequence of procedures to commission High Availability on one or more pairs of Avaya Aura® Media Servers.

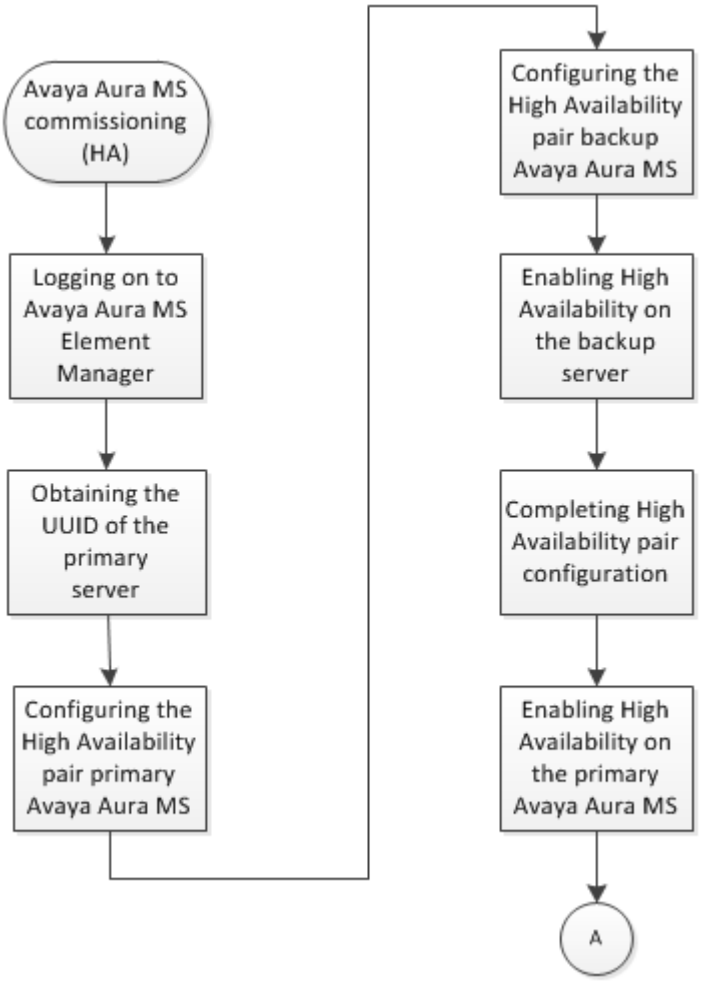


Figure 10: Avaya Aura® Media Server High Availability commissioning procedures

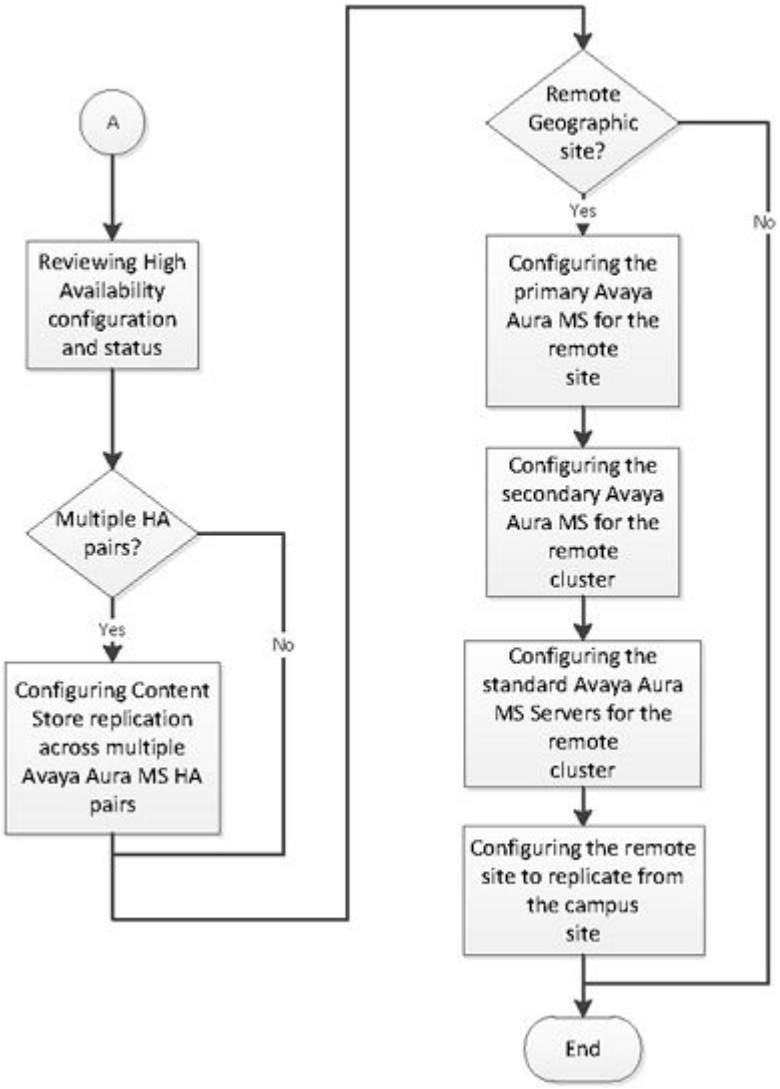


Figure 11: Avaya Aura® Media Server High Availability commissioning procedures continued

Avaya Aura® Media Server HA commissioning checklist

The following is a list of key configuration items required for Avaya Aura® Media Server High Availability (HA) commissioning.

Item	Your value	Description
Element Manager – User ID		The User ID used to log on to Avaya Aura® Media Server Element Manager.

Table continues…

Item	Your value	Description
Element Manager – Password		The password used to log on to Avaya Aura® Media Server Element Manager.
Primary 1 Avaya Aura® Media Server IP address		The IP address of the first primary Avaya Aura® Media Server in the pair.
Primary 1 Avaya Aura® Media Server Universally Unique Identifier (UUID)		The UUID of the first primary Avaya Aura® Media Server. The UUID is required for HA pair replication.
HA replication account Username		The username of the Avaya Aura® Media Server HA replication account.
HA replication account Password		The password of the Avaya Aura® Media Server HA replication account.
Backup 1 Avaya Aura® Media Server IP address		The IP address of the first backup Avaya Aura® Media Server in the pair.
Primary 2 Avaya Aura® Media Server IP address		The IP address of the second primary Avaya Aura® Media Server in the pair.
Primary 2 Avaya Aura® Media Server Universally Unique Identifier (UUID)		The UUID of the second primary Avaya Aura® Media Server. The UUID is required for HA pair replication.
HA replication account Username		The username of the Avaya Aura® Media Server HA replication account.
HA replication account Password		The password of the Avaya Aura® Media Server HA replication account.
Backup 2 Avaya Aura® Media Server IP address		The IP address of the second backup Avaya Aura® Media Server in the pair.
Primary 3 Avaya Aura® Media Server IP address		The IP address of the third primary Avaya Aura® Media Server in the pair.
Primary 3 Avaya Aura® Media Server Universally Unique Identifier (UUID)		The UUID of the third primary Avaya Aura® Media Server. The UUID is required for HA pair replication.
HA replication account Username		The username of the Avaya Aura® Media Server HA replication account.
HA replication account Password		The password of the Avaya Aura® Media Server HA replication account.
Backup 3 Avaya Aura® Media Server IP address		The IP address of the third backup Avaya Aura® Media Server in the pair.
Remote Primary Avaya Aura® Media Server IP address		The IP address of the remote primary Avaya Aura® Media Server in the pair.
Remote Primary Avaya Aura® Media Server Universally Unique Identifier (UUID)		The UUID of the remote primary Avaya Aura® Media Server. The UUID is required for HA pair replication.

Table continues…

Item	Your value	Description
Remote HA replication account Username		The username of the Avaya Aura® Media Server HA replication account.
Remote HA replication account Password		The password of the Avaya Aura® Media Server HA replication account.
Remote Backup Avaya Aura® Media Server IP address		The IP address of the remotea backup Avaya Aura® Media Server in the pair.

Logging on to Avaya Aura® Media Server Element Manager

Before you begin

- Obtain a valid user name and password to access Avaya Aura® Media Server Element Manager.

About this task

Log on to the Avaya Aura® Media Server Element Manager to configure Avaya Aura® Media Server.

Element Manager (EM) is a web-based administration tool that facilitates the Operation, Administration, and Maintenance (OAM) of Avaya Aura® Media Server. A SIP-enabled Contact Center solution must contain one or more Avaya Aura® Media Server servers.

Note:

You must have more than one Avaya Aura® Media Server account managed by separate users. If one account is disabled or lost, another account can perform critical tasks, backups or recovery. For more information, see *Implementing and Administering Avaya Aura® Media Server*.

Procedure

1. Start a Web browser.
2. In the address box, type the following URL:

   `https://SERVER_IP_ADDRESS:8443/em`

   Where SERVER_IP_ADDRESS is the IP address of the Avaya Aura® Media Server.
3. In the **User ID** box, type the Avaya Aura® Media Server User ID log on account name. The default user account name is `Admin`.
4. In the **Password** box, type the Element Manager password. Use the `Admin` account password. The default password is `Admin123$`.
5. Click **Sign In**.

Obtaining the Universally Unique Identifier of the primary server

Before you begin

- Access the Element Manager for the primary Avaya Aura® Media Server.

About this task

Perform this procedure to obtain the Universally Unique Identifier (UUID) of the primary Avaya Aura® Media Server. You need to enter the primary server UUID when you configure the backup server in the high availability pair.

If you have more than one Avaya Aura® Media Server High Availability pair, select one server from each Avaya Aura® Media Server pair to be the primary Avaya Aura® Media Server for that pair. Perform this procedure on the primary Avaya Aura® Media Server of each High Availability pair.

Procedure

1. In the primary Avaya Aura® Media Server Element Manager navigation pane, click **System Status**.
2. Click **Element Status**.
3. Record the UUID for the primary Avaya Aura® Media Server from the Element Status page.

Configuring the High Availability pair primary Avaya Aura® Media Server

Before you begin

- Access the Element Manager for the primary Avaya Aura® Media Server.

About this task

Designate the primary Avaya Aura® Media Server as the primary server in each High Availability pair, and create a replication username and password for the high availability pair.

If you have more than one Avaya Aura® Media Server High Availability pair, select one server from each Avaya Aura® Media Server pair to be the primary Avaya Aura® Media Server for that pair. Perform this procedure on the primary Avaya Aura® Media Server of each High Availability pair.

Avaya Aura® Media Server uses a custom password protected account to secure Content Store replication. Each Avaya Aura® Media Server in a High Availability solution must be configured with the same replication account username and password details. The Avaya Aura® Media Server replication account is a custom account used to secure the Avaya Aura® Media Server Content Store during replication, it is not a Linux operating system account.

Procedure

1. In the navigation pane, click **Cluster Configuration**.

2. Click **Server Designation**.
3. Under **Local Server**, from the **Role** list, select **Primary**.
4. Under **Replication Account**, select the **Enable Replication Account** check box.
5. In the **Username** box, type a username for the replication account. This value is arbitrary, but each Avaya Aura® Media Server in a High Availability solution must be configured with the same replication account username.
6. In the **Password** box, type a password for the replication account. This value is arbitrary, but each Avaya Aura® Media Server in a High Availability solution must be configured with the same replication account password.
7. Confirm the password and click **Save**.
8. Click **Confirm**.

Procedure job aid

Configure the primary Avaya Aura® Media Server to create a replication account for the High Availability pair.

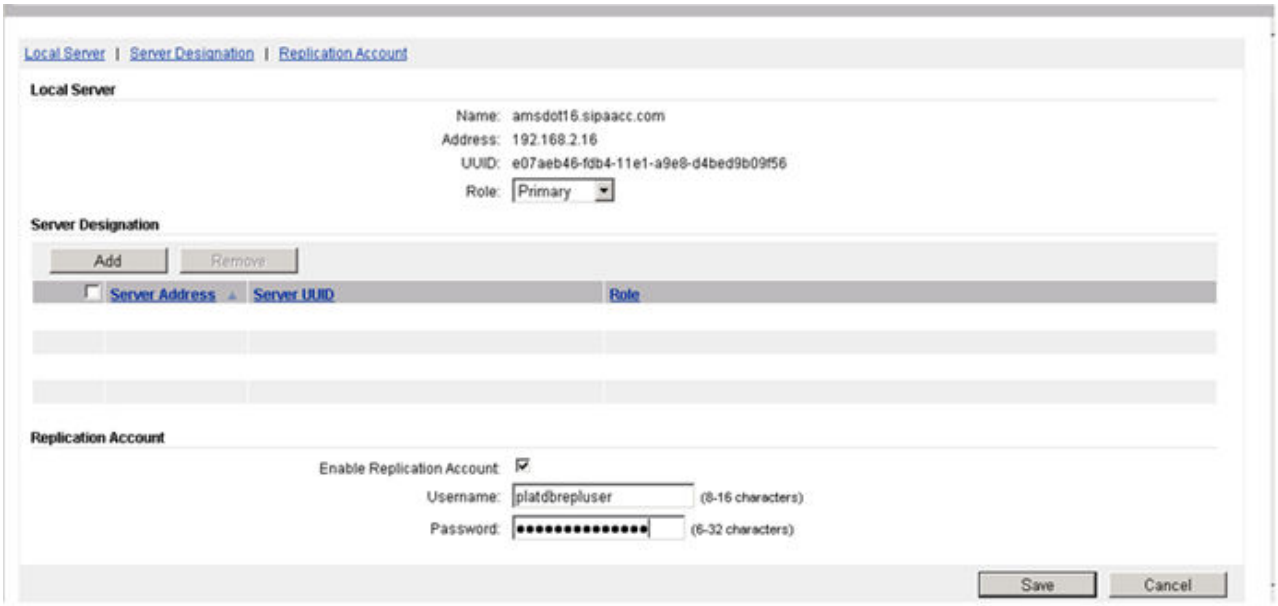


Figure 12: Example of designating an Avaya Aura® Media Server as a primary server

Configuring the High Availability pair backup Avaya Aura® Media Server

Before you begin

- Access the Element Manager for the backup Avaya Aura® Media Server.

About this task

Designate the backup server of the high availability pair, configure it with the primary server UUID and IP address, and enter the replication account details.

If you have more than one Avaya Aura® Media Server High Availability pair, select one server from each Avaya Aura® Media Server pair to be the backup Avaya Aura® Media Server for that pair. Perform this procedure on the backup Avaya Aura® Media Server of each High Availability pair.

Avaya Aura® Media Server uses a custom password protected account to secure Content Store replication. Each Avaya Aura® Media Server in a High Availability solution must be configured with the same replication account username and password details. The Avaya Aura® Media Server replication account is a custom account used to secure the Avaya Aura® Media Server Content Store during replication, it is not a Linux operating system account.

Procedure

1. In the backup Avaya Aura® Media Server Element Manager navigation pane, click **Cluster Configuration**.
2. Select **Server Designation**.
3. Under **Local Server**, select **Backup** from the **Role** list.
4. Under **Server Designation**, in the **Primary Server UUID** box, type the UUID of the Primary server.
5. Type the primary server IP address in the **Primary Server Address** box.
6. Under **Replication Account**, select the **Enable Replication Account** check box.
7. In the **Username** box, type the username for the replication account that you specified on the primary server.
8. In the **Password** box, type the password for the replication account that you specified on the primary server.
9. Confirm the password and click **Save**.
10. Click **Confirm**.

Procedure job aid

Configure the backup Avaya Aura® Media Server to enter the primary server UUID and IP address, and the replication account for the High Availability pair.

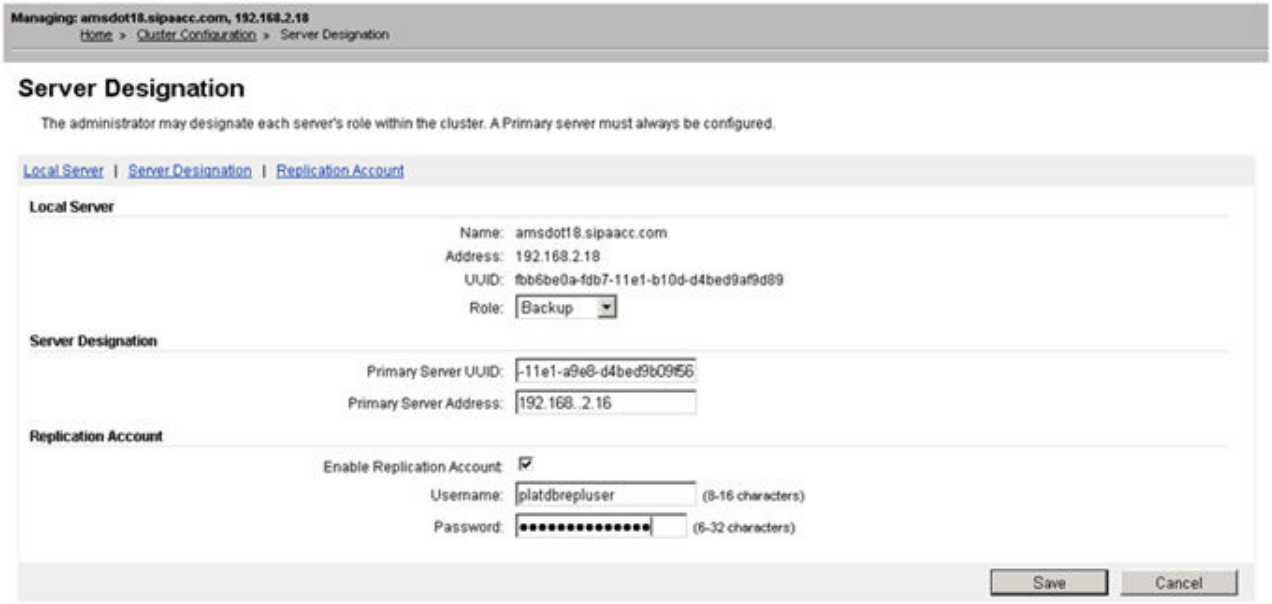


Figure 13: Example of designating an Avaya Aura® Media Server as a backup server

Enabling High Availability on the backup server

Before you begin

- Access the Element Manager for the backup Avaya Aura® Media Server.

About this task

Configure the backup server to start replicating from the primary server for High Availability.

If you have more than one Avaya Aura® Media Server High Availability pair, select one server from each Avaya Aura® Media Server pair to be the backup Avaya Aura® Media Server server. Perform this procedure on the backup Avaya Aura® Media Server of each High Availability pair.

Procedure

1. In the backup Avaya Aura® Media Server Element Manager navigation pane, click **Cluster Configuration**.
2. Click **High Availability**.
3. Under **General Settings**, select the **Enable High Availability** check box.
4. In the **Service IP Address** box, type the managed IP address for this High Availability pair.
5. Ensure **Local High Availability State Lock** is not selected.
6. Click **Save**.

Procedure job aid

Enable High Availability on an Avaya Aura® Media Server backup server.

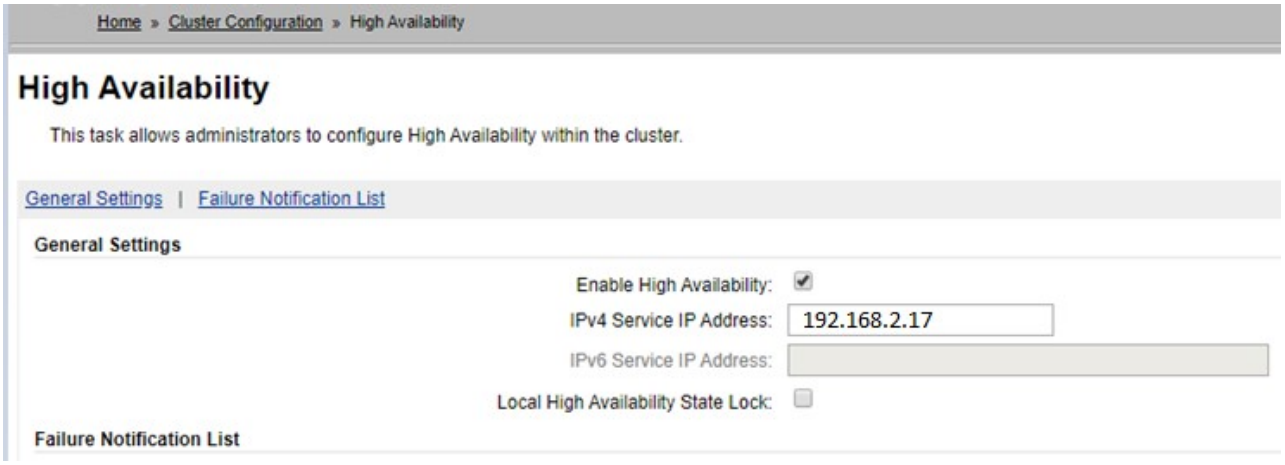


Figure 14: Example of Avaya Aura® Media Server High Availability backup server

Completing High Availability pair configuration

Before you begin

Configure the primary and backup Avaya Aura® Media Servers.

About this task

Perform the following procedure on the primary server of each High Availability pair to complete the High Availability server pairing.

Procedure

1. In the navigation pane, click **Cluster Configuration**.
2. Click **Server Designation**.
3. Ensure the **Local Server Role** is set to **Primary**.
4. Ensure one server is shown under **Server Designation** and the server has the **Role** of **Backup**.
5. Ensure **Enable Replication Account** is selected.
6. If the backup server is not listed in the **Server Designation** section, then click **Add**.
7. In the **Server Address** field, type the IP address of the backup server.
8. In the **Server UUID** field, type the UUID of the backup server.
9. Under **Role**, select **Backup**.
10. Click **Save**.

Example

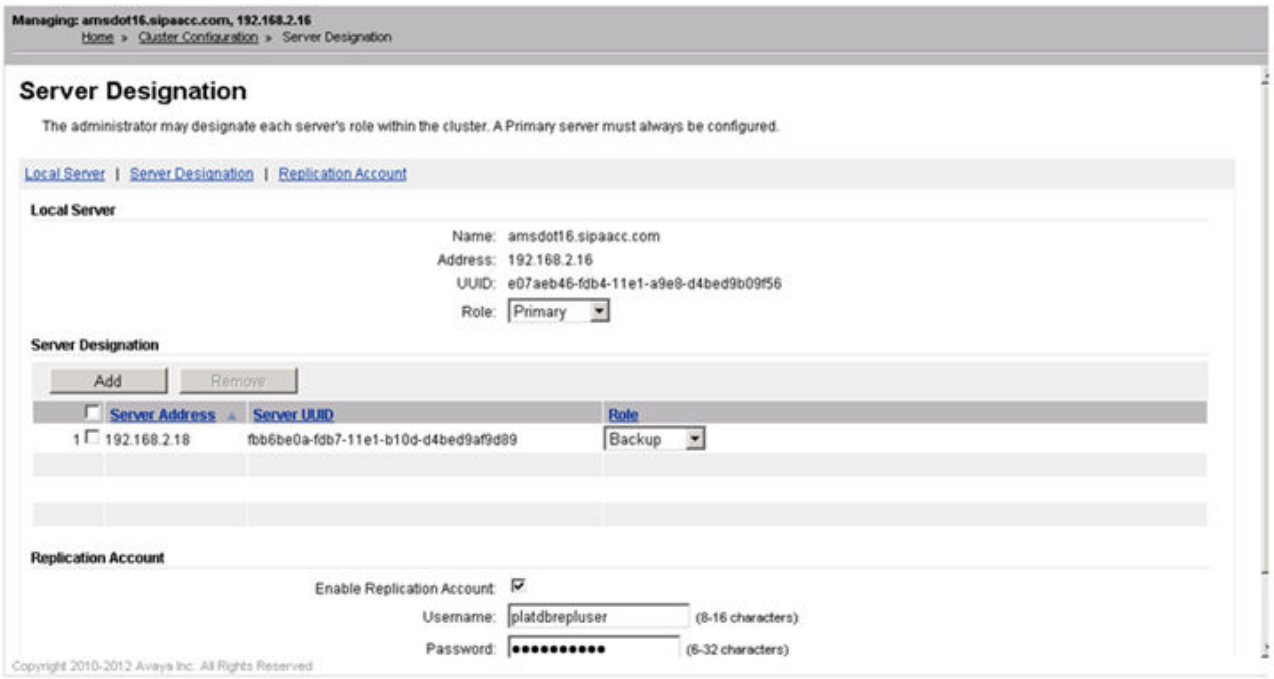


Figure 15: Completing High Availability pair configuration

Enabling High Availability on the primary Avaya Aura® Media Server

Before you begin

- Select one Avaya Aura® Media Server as the primary server.
- Access the Element Manager for the primary Avaya Aura® Media Server.

About this task

Enable High Availability on the primary Avaya Aura® Media Server. Configure Avaya Aura® Media Server to notify Contact Center Manager Server when an Avaya Aura® Media Server failure or switchover occurs.

If you have more than one Avaya Aura® Media Server High Availability pair, select one server from each Avaya Aura® Media Server pair to be the primary Avaya Aura® Media Server server. Perform this procedure on the primary Avaya Aura® Media Server of each High Availability pair.

Procedure

1. In the primary Avaya Aura® Media Server Element Manager navigation pane, click **Cluster Configuration**.
2. Click **High Availability**.

3. Under **General Settings**, select the **Enable High Availability** check box.
4. In the **Service IP Address** box, type the managed IP address for this Avaya Aura® Media Server High Availability pair.
5. Under the Failure Notification List, click **Add** to add the Contact Center Manager Server managed IP address.

   Avaya Aura® Media Server sends a notification to Contact Center Manager Server if a failover occurs.
6. In the **Server Address** box, type the managed IP address of the Contact Center Manager Server server.
7. In the **Server Port** box, type **57012**.

   This Avaya Aura® Media Server - **Failure Notification List** - **Server Port** number must match the Contact Center Manager Server High Availability utility - **Local SMMC Port** number.
8. Ensure **Local High Availability State Lock** is not selected.
9. Click **Save**.

Procedure job aid

Configure an Avaya Aura® Media Server primary server to complete creating a High Availability pair.

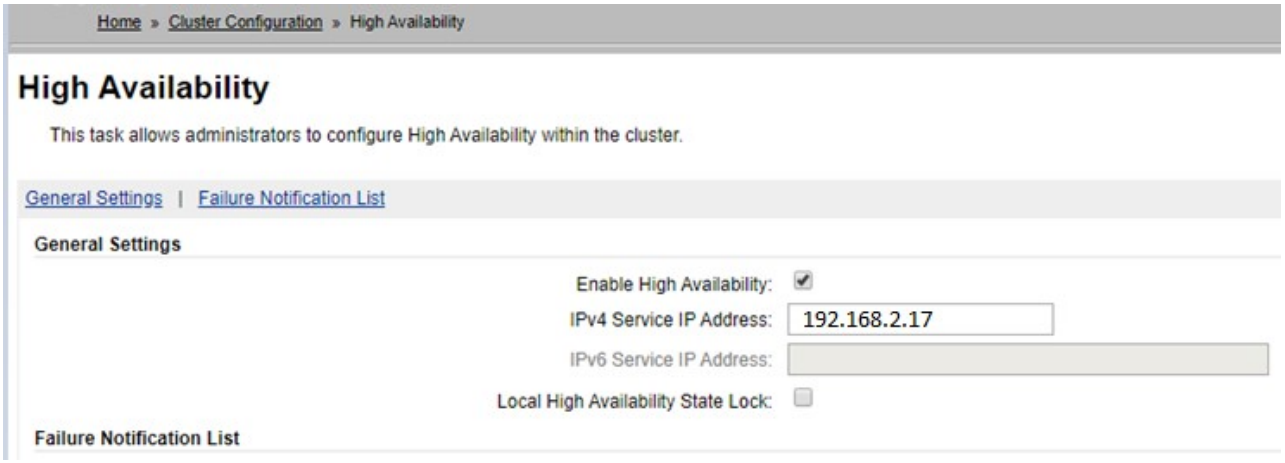


Figure 16: Example of configuring Avaya Aura® Media Server High Availability on the primary server

Reviewing High Availability configuration and status

About this task

After the High Availability pair is formed, several Element Manager 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. In the primary Avaya Aura® Media Server Element Manager navigation pane, click **System Status**.
2. Click **Cluster Status**.
3. Ensure only two nodes are listed.
4. Ensure one **Element Role** is listed for both the primary and backup server.
5. Ensure no alarms are listed in the **Alarm Description** column.
6. In the backup Avaya Aura® Media Server Element Manager navigation pane, click **System Status**.
7. Click **Cluster Status**.
8. Ensure only two nodes are listed.
9. Ensure one **Element Role** is listed for both the primary and backup server.
10. Ensure no alarms are listed in the **Alarm Description** column.

Configuring Content Store replication across multiple Avaya Aura® Media Server High Availability pairs

Before you begin

- Configure and enable each Avaya Aura® Media Server High Availability pair.

About this task

In a solution with more than one Avaya Aura® Media Server High Availability pair, select one of the Avaya Aura® Media Server High Availability pairs to be the Content Store master pair. Then configure the other Avaya Aura® Media Server High Availability pairs to replicate the media from this Content Store master pair.

You use the Element Manager of the Avaya Aura® Media Server Content Store master pair to configure Content Store media such as dialog prompts (announcements) and music. The Content Store media updates and changes you make on the Content Store master pair are then replicated to the other Avaya Aura® Media Server High Availability Content Store replicating pairs.

The following diagram shows two Avaya Aura® Media Server High Availability Content Store replicating pairs duplicating Content Store media from the Avaya Aura® Media Server High Availability Content Store master pair.

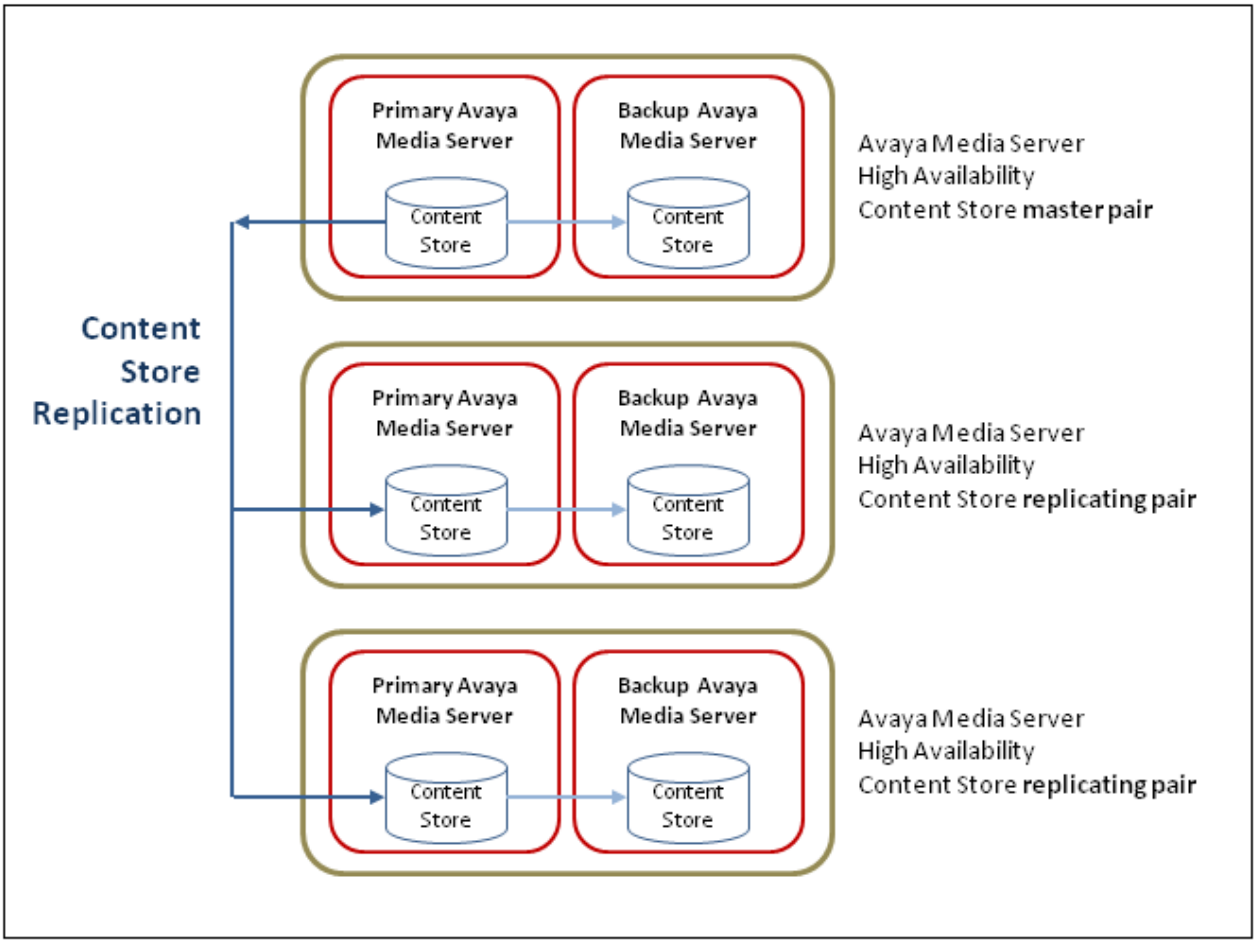


Figure 17: An image of two Avaya Aura® Media ServerHigh Availability Content Store replicating pairs duplicating Content Store media

Select one of the Avaya Aura® Media Server High Availability pairs to be the Content Store master pair and then configure all the other primary Avaya Aura® Media Server servers to replicate the Content Store media from the Content Store master pair.

Perform this procedure on all primary Avaya Aura® Media Server High Availability servers, except for the Avaya Aura® Media Server Content Store master pair primary, to configure each Avaya Aura® Media Server High Availability replicating pair to replicate Content Store master media data from the Content Store master.

⚠ Caution:

Do not perform this procedure on the Avaya Aura® Media Server High Availability Content Store master pair primary.

Procedure

1. Log on to an Avaya Aura® Media Server High Availability Content Store replicating pair primary Element Manager.
2. In the navigation pane, click **Cluster Configuration**.
3. Click **Replication Settings**.
4. In the **Master Cluster Primary Node Address** box, type the IP address for the primary Avaya Aura® Media Server of the High Availability Content Store master pair. Type the actual IP address of the HA master pair primary server and not the managed IP address of the HA master pair.
5. Click **Save**.
6. Repeat this procedure on the primary Avaya Aura® Media Server of each Avaya Aura® Media Server High Availability Content Store replicating pair.

Configuring the primary Avaya Aura® Media Server for the remote site

Before you begin

- Install Avaya Aura® Media Server software on a server at the remote site.

About this task

If you are using a remote geographic site with an Avaya Aura® Media Server cluster, designate one of the Avaya Aura® Media Servers as the primary server for the cluster, and configure the replication username and password.

If you are using a remote geographic site with an Avaya Aura® Media Server HA pair, designate one of the Avaya Aura® Media Servers as the primary server for the pair, and configure the replication username and password.

If you are using a remote geographic site with a single standalone Avaya Aura® Media Server, designate the Avaya Aura® Media Server as a primary server, and configure the replication username and password.

Avaya Aura® Media Server uses a custom password protected account to secure Avaya Aura® Media Server Content Store replication. Configure all of the Avaya Aura® Media Servers at the remote site with the same replication account username and password details as used by all of the Avaya Aura® Media Servers at the High Availability campus site.

Procedure

1. Log on to the Element Manager for the primary Avaya Aura® Media Server of the remote site cluster.
2. In the navigation pane, click **Cluster Configuration**.
3. Select **Server Designation**.

4. Under **Local Server**, select **Primary** from the **Role** list.
5. Under **Replication Account**, select the **Enable Replication Account** check box.
6. In the **Username** box, type a username for the replication account. Configure the primary Avaya Aura® Media Server at the remote site with the same replication account username as used by the Avaya Aura® Media Servers at the High Availability campus site.
7. In the **Password** box, type a password for the replication account. Configure the primary Avaya Aura® Media Server at the remote site with the same replication account password as used by the Avaya Aura® Media Servers at the High Availability campus site.
8. Confirm the password and click **Save**.
9. Under **Local Server**, note the **UUID** value. You must enter this value on the other servers in the cluster.

Configuring the secondary Avaya Aura® Media Server for the remote cluster

Before you begin

- Install Avaya Aura® Media Server software on a server at the remote site.
- Designate an Avaya Aura® Media Server as the primary server for a cluster, and create a replication username and password.

About this task

Designate a secondary Avaya Aura® Media Server for the cluster at the remote site. Configure the secondary server with the primary Avaya Aura® Media Server UUID and IP address, and enter the replication account details.

Avaya Aura® Media Server uses a custom password protected account to secure Avaya Aura® Media Server Content Store replication. Configure all of the Avaya Aura® Media Servers at the remote site with the same replication account username and password details as used by all of the Avaya Aura® Media Servers at the High Availability campus site.

Procedure

1. Access the Element Manager for the secondary Avaya Aura® Media Server.
2. In the navigation pane, click **Cluster Configuration**.
3. Select **Server Designation**.
4. Under **Local Server**, select **Secondary** from the **Role** list.
5. Under **Server Designation**, type the UUID of the Primary server at the remote site in the **Primary Server UUID** box.
6. In the **Primary Server Address** box, type the IP address of the remote cluster primary server.

7. Under **Replication Account**, select the **Enable Replication Account** check box.
8. In the **Username** box, type the username for the replication account. Configure the primary Avaya Aura® Media Server at the remote site with the same replication account username as used by the Avaya Aura® Media Servers at the High Availability campus site.
9. In the **Password** box, type the password for the replication account. Configure the primary Avaya Aura® Media Server at the remote site with the same replication account password as used by the Avaya Aura® Media Servers at the High Availability campus site.
10. Confirm the password and click **Save**.

Configuring the standard Avaya Aura® Media Server for the remote cluster

Before you begin

- Install Avaya Aura® Media Server software on a server at the remote site.
- Designate an Avaya Aura® Media Server as the primary server for the remote cluster, and create a replication username and password.
- Designate a secondary Avaya Aura® Media Server for the remote cluster.

About this task

Designate any remaining Avaya Aura® MS servers as standard servers for the cluster. Configure each standard Avaya Aura® Media Server with the primary Avaya Aura® Media Server UUID and IP address, and enter the replication account details.

Avaya Aura® Media Server uses a custom password protected account to secure Avaya Aura® Media Server Content Store replication. Configure all of the Avaya Aura® Media Servers at the remote site with the same replication account username and password details as used by all of the Avaya Aura® Media Servers at the High Availability campus site.

Procedure

1. Access the Element Manager for the standard Avaya Aura® Media Server of the remote site cluster.
2. In the navigation pane, click **Cluster Configuration**.
3. Select **Server Designation**.
4. Under **Local Server**, select **Standard** from the **Role** list.
5. Under **Server Designation**, type the UUID of the remote site Primary server in the **Primary Server UUID** box.
6. In the **Primary Server Address** box, type the IP address of the remote cluster primary server.
7. Under **Replication Account**, select the **Enable Replication Account** check box.

8. In the **Username** box, type the username for the replication account. Configure the primary Avaya Aura® Media Server at the remote site with the same replication account username as used by the Avaya Aura® Media Servers at the High Availability campus site.
9. In the **Password** box, type the password for the replication account. Configure the primary Avaya Aura® Media Server at the remote site with the same replication account password as used by the Avaya Aura® Media Servers at the High Availability campus site.
10. Confirm the password and click **Save**.
11. Repeat this procedure on each standard Avaya Aura® Media Server in the remote cluster.

Configuring the remote site to replicate from the campus site

Before you begin

- Obtain the IP address of the primary Avaya Aura® Media Server of the High Availability Avaya Aura® Media Server Content Store master pair.

About this task

Configure the primary Avaya Aura® Media Server of the remote site to replicate the Content Store contents from the campus site. This allows the administrator to perform Content Store configuration on the campus primary server, and the replication copies this to the primary Avaya Aura® Media Server at the remote site.

Avaya Aura® Media Server supports the following deployments at the Contact Center remote site:

- Standalone Avaya Aura® Media Server
- Avaya Aura® Media Server cluster
- Avaya Aura® Media Server High Availability pair

If your remote site uses a standalone Avaya Aura® Media Server, it must be configured as a primary server.

Caution:

Do not perform this procedure on the Avaya Aura® Media Server High Availability Content Store master pair.

Procedure

1. Log on to the Element Manager for the primary Avaya Aura® Media Server on the remote site that you want to have replicate from the Avaya Aura® Media Server High Availability Content Store master pair.
2. In the navigation pane, click **Cluster Configuration**.
3. Select **Replication Settings**.

4. In the **Master Cluster Primary Node Address** box, type the IP address of the primary Avaya Aura® Media Server of the campus High Availability Content Store master pair. Type the actual IP address of the campus HA master pair primary Avaya Aura® Media Server and not the managed IP address of the campus HA master pair.
5. Click **Save**.

Chapter 9: Avaya Aura® Media Server common commissioning

This chapter includes commissioning procedures for Avaya Aura® Media Server (Avaya Aura® MS) in a SIP-enabled contact center.

Configuring media on Avaya Aura® Media Server

Avaya Aura® Media Server (Avaya Aura® MS) provides default media for standard ringback and busy tones in a SIP-enabled contact center. Contact Center uses these default tones with SIP-enabled phone calls.

Continuous streaming media

Avaya Aura® MS supports the configuration of a continuously streamed source for music. To use continuous streamed source, you can configure either a Really Simple Syndication (RSS) provider or a HTTP/MP3 provider from which the Avaya Aura® MS can provide music to the Contact Center. Avaya Aura® MS supports up to 64 music streams across all of the supported providers.

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

To use streamed music in Contact Center Orchestration Designer (OD) flow applications, you create routes in Contact Center Manager Administration (CCMA) that link to the RSS or HTTP/MP3 Stream Key configured on Avaya Aura® MS. The OD flow applications reference these routes to access the streamed music.

Real Simple Syndication (RSS) provider:

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

The media server uses the RSS title element in the document as the title for the files in the cache. The files play in alphabetical order. The RSS provider on the media server supports audio files in WAV and MP3 formats. Avaya recommends that audio to be played by Avaya Aura® MS is encoded in G.711 or 16 bit, 8 kHz, single channel, PCM files. You can use codecs other than

PCM, or with higher sampling rates for higher quality recordings; however, this reduces system performance. The RSS provider on the media server does not support multiple channels or stereo.

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

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

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

Avaya Aura® MS uses cached files to provide continuous streaming service when the RSS URL becomes unreachable. If you update or delete the RSS URL, then the files in the cache are deleted.

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

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

HTTP/MP3 provider:

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

Most streaming radio stations on the internet stream over HTTP/MP3. Many of the stations use the SHOUTCast ICY protocol. Typically, a SHOUTCast stream provides a playlist in a .pls or .m3u

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

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

The HTTP/MP3 provider on Avaya Aura® MS supports stereo and mono MP3 streams. When the specified radio station supports metadata, the media server accepts the song title and artist information as it is received in real-time. Element Manager displays the current song title and artist on the monitoring page.

Avaya Aura® MS supports only MP3 SHOUTCast streams. Avaya Aura® MS does not support Advanced Audio Coding (AAC). To ensure that the HTTP/MP3 stream is compatible with Avaya Aura® MS:

- The audio must be encoded in MPEG-1 Audio Layer 3 (MP3) or MPEG-2 Audio Layer 3 (MP3).
- Avaya Aura MS supports the following MPEG-1 sample rates: 32000, 44100, and 48000 Hz.
- Avaya Aura MS supports the following MPEG-2 sample rates: 22050, 24000, and 16000 Hz.
- Avaya Aura MS supports the following bit rates: 32, 64, 96, 128, 160, 192, 256 and 320 kbps.
- The content type for playlists must be audio/x-scpls or audio/x-mpegurl.
- The content type for audio must specify audio/mpeg, audio/x-mpeg, or application/octet-stream.
- The server can respond with ICY 200 OK or standard HTTP 200 OK responses.
- Avaya Aura MS supports the ICY MetaData update mechanism. Use of this update mechanism is optional.
- Avaya Aura MS supports VLC and Icecast streaming sources, if the codec and content type used are also supported.

The Avaya Aura® MS HTTP/MP3 provider automatically records 15 minutes of content. The recorded content provides a backup when the streaming server is unreachable.

Avaya Aura® Media Server scripted music

Avaya Aura® MS supports the configuration of a continuously streamed source for scripted music. Configure Avaya Aura® MS to supply only scripted music treatments inserted in to a voice call by a Contact Center Orchestration Designer (OD) flow application.

Scripted music plays from an Avaya Aura® Media Server content store as a continuous stream.

Music on hold

Communication Manager can supply music when agents put a call on hold (music-on-hold). Communication Manager Release 7.0 or later supports configuring music-on-hold in addition to Avaya Aura® MS scripted music.

Note:

In most normal call flow situations, Contact Center suppresses Communication Manager music-on-hold if Avaya Aura® MS also plays music. However, it is possible that in some complex call flow scenarios, both sources can play music simultaneously.

If your solution uses Communication Manager Release 6.2 FP4 with music-on-hold enabled, do not configure Avaya Aura® MS to supply music-on-hold.

For more information on how to configure music-on-hold using your Communication Manager, see *Avaya Aura® Communication Manager Feature Description and Implementation.*

Prerequisites for Avaya Aura® Media Server common commissioning

- Install Avaya Aura® Media Server.
- Complete the procedures specific to your contact center deployment type. For more information, see Avaya Aura Media Server commissioning for non-HA deployments on page 59 or Avaya Aura Media Server commissioning for HA deployments on page 66.

Avaya Aura® Media Server common commissioning procedures

About this task

This task flow shows you the sequence of procedures you perform to configure the Avaya Aura® Media Server.

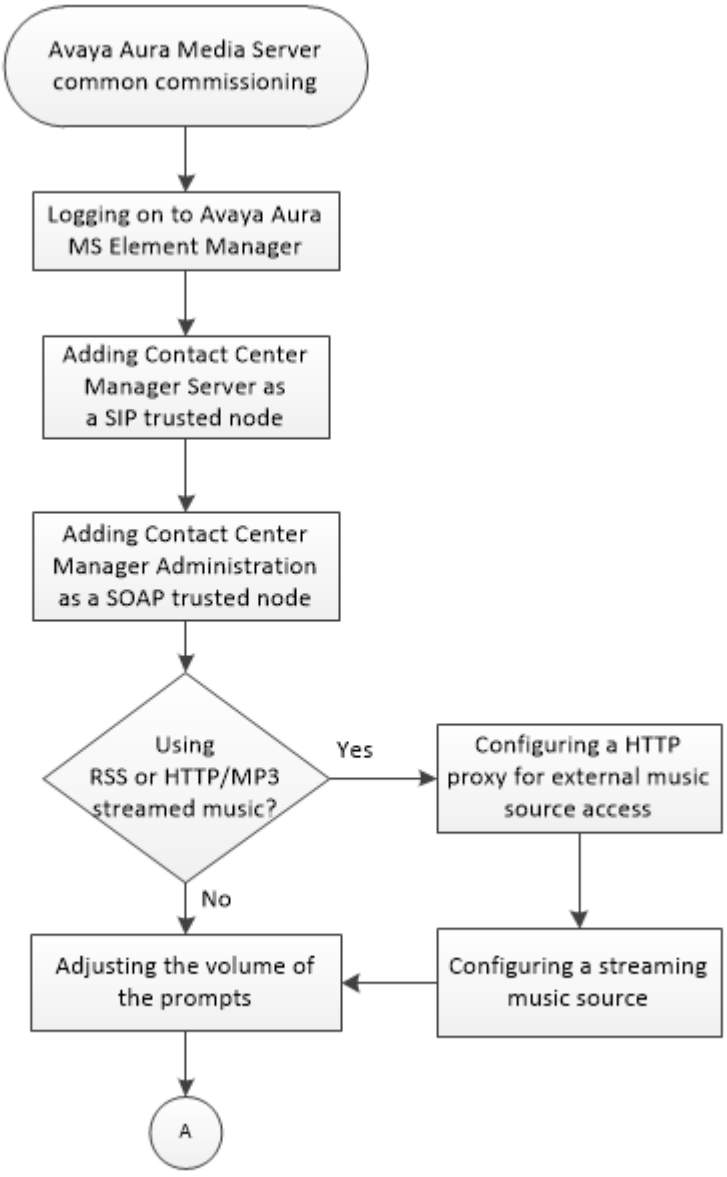


Figure 18: Avaya Aura® Media Server common commissioning procedures

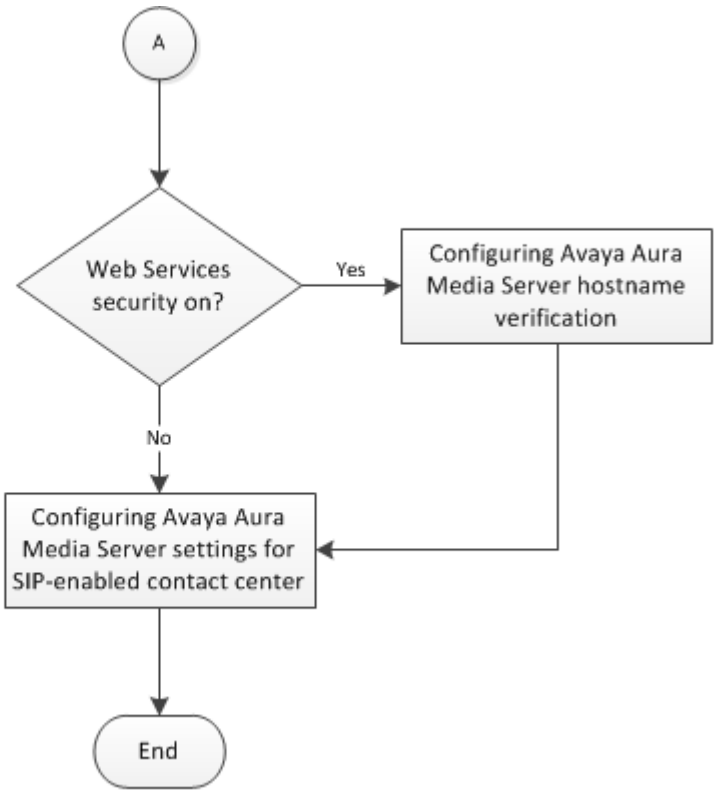


Figure 19: Avaya Aura® Media Server common commissioning procedures continued

Avaya Aura® Media Server common commissioning checklist

The following is a list of key configuration items required for Avaya Aura® Media Server common commissioning.

Item	Your value	Description
Element Manager – User ID		The User ID used to log on to Avaya Aura® Media Server Element Manager.
Element Manager – Password		The password used to log on to Avaya Aura® Media Server Element Manager.
AACC or CCMS IP address (Trusted Node)		The IP address of the AACC server. For Mission Critical High Availability solutions, enter the AACC Active, Standby, and Managed IP addresses.
AACC or CCMA IP address (SOAP Trusted Node)		The IP address of the AACC server.

Table continues…

Item	Your value	Description
Media content namespace		The AACC SIP domain.
Really Simple Syndication (RSS) server URL		You can optionally configure Avaya Aura® Media Server to use an RSS URL to provide continuous streamed source music to the contact center.

Logging on to Avaya Aura® Media Server Element Manager

Before you begin

- Obtain a valid user name and password to access Avaya Aura® Media Server Element Manager.

About this task

Log on to the Avaya Aura® Media Server Element Manager to configure Avaya Aura® Media Server.

Element Manager (EM) is a web-based administration tool that facilitates the Operation, Administration, and Maintenance (OAM) of Avaya Aura® Media Server. A SIP-enabled Contact Center solution must contain one or more Avaya Aura® Media Server servers.

Note:

You must have more than one Avaya Aura® Media Server account managed by separate users. If one account is disabled or lost, another account can perform critical tasks, backups or recovery. For more information, see *Implementing and Administering Avaya Aura® Media Server*.

Procedure

1. Start a Web browser.
2. In the address box, type the following URL:

   `https://SERVER_IP_ADDRESS:8443/em`

   Where SERVER_IP_ADDRESS is the IP address of the Avaya Aura® Media Server.
3. In the **User ID** box, type the Avaya Aura® Media Server User ID log on account name. The default user account name is `Admin`.
4. In the **Password** box, type the Element Manager password. Use the `Admin` account password. The default password is `Admin123$`.
5. Click **Sign In**.

Adding Contact Center Manager Server as a SIP trusted node

About this task

Add the Contact Center Manager Server as a SIP trusted node to Avaya Aura® Media Server. This permits Contact Center Manager Server to use the Avaya Aura® Media Server services.

If Avaya Aura® Media Server is co-resident on the CCMS server, you do not need to follow this procedure.

For High Availability systems, add the following trusted nodes to Avaya Aura® Media Server:

- the managed IP address of the CCMS High Availability pair
- the IP address of the Active CCMS server
- the IP address of the Standby CCMS server

Note:

Perform this procedure on every primary Avaya Aura® Media Server.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **System Configuration** > **Signaling Protocols** > **SIP**.
3. Click **Nodes and Routes**.
4. Click the **Trusted Nodes** link.
5. If the contact center is not a High Availability system:
   a. Click **Add**.
   b. On the **Add SIP Trusted Node** page, in the **Host or Server Address** field, type the IP address of the Contact Center Manager Server.
   c. Click **Save**.
6. If the contact center is a High Availability system:
   a. Click **Add**.
   b. On the **Add SIP Trusted Node** page, in the **Host or Server Address** field, type the managed IP address of the CCMS High Availability pair.
   c. Click **Save**.
   d. Click **Add**.
   e. On the **Add SIP Trusted Node** page, in the **Host or Server Address** field, type the IP address of the Active CCMS server.
   f. Click **Save**.
   g. Click **Add**.

h. On the **Add SIP Trusted Node** page, in the **Host or Server Address** field, type the IP address of the Standby CCMS server.

i. Click **Save**.

Adding Contact Center Manager Administration as a SOAP trusted node

About this task

To support Prompt Management in Contact Center Manager Administration (CCMA), you must add CCMA as a SOAP trusted node in Avaya Aura® Media Server Element Manager.

Procedure

1. Log on to Element Manager.
2. In the Element Manager navigation pane, click **System Configuration** > **Network Settings** > **General Settings**.
3. Click **SOAP**.
4. In the **Trusted Nodes** box, enter the IP address of the CCMA server.

   If you are using Avaya Aura® Contact Center High Availability, enter the Active, Standby, and Managed IP addresses of the CCMA servers.
5. Select **Enable Trusted SOAP Nodes**.
6. Click **Save**.

Configuring a HTTP proxy for external music source access

About this task

If external streaming servers use non-standard ports, enterprise firewalls can block outgoing HTTP connections. Perform the following procedure to configure the address and port of an internal HTTP proxy server, to allow access to external streaming servers. This proxy configuration applies to streaming that uses RSS, HLS, and ICY protocols over HTTP.

If your enterprise firewall does not block access to the external streaming servers, you can skip this procedure.

Before you begin

- Know the FQDN or IP address, and port, of the internal HTTP proxy server.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **System Configuration** > **Media Processing** > **Music** > **General Settings**.
3. In the **HTTP Proxy Host** field, type the FQDN or IP address of the internal proxy server that provides access to the external streaming servers.
4. In the **HTTP Proxy Port** field, type the port of the internal proxy server.
5. Click **Save**.

Configuring a streaming music source

Before you begin

- Ensure that the streaming music source server that you want to use is configured and operational.
- Ensure that the music source you configure meets the requirements for the provider type.

About this task

Configure Avaya Aura® Media Server to use a streaming music source URL to provide continuous streamed source music to the contact center.

To be able to use the streamed music in an OD flow application or script, you must configure and acquire a route for the channel using the CCMA Configuration page. This route name must match the stream key that you configure. For more information, see *Avaya Aura® Contact Center Client Administration*.

To provide music to callers, add or edit a flow application or script to provide scripted music using OD, using the Route Number entered in the CCMA Configuration page. For more information, see *Using Contact Center Orchestration Designer*.

Note:

Perform this procedure on every primary Avaya Aura® Media Server.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **System Configuration** > **Media Processing** > **Music** > **Stream Provisioning**.
3. Click **Add**.
4. From the **Stream Type** list, select the streaming music source type.
5. In the **Name** field, type a name for the new music source.

   This is the stream key that you use to create a route in CCMA.

6. Do not enter a value in the **Domain** field; if you do, you create a stream key that you cannot use as a Route name in CCMA.
7. In the **Primary URL** field, type the address of the music source.
8. To provide an alternate music source, in the **Backup URL** field, type the address of another music source.

   Avaya Aura® Media Server switches to the backup music source when the primary source is unavailable.
9. If you want to add the music source in the locked state so that Avaya Aura® Media Server cannot use the new music source, select the **Locked** check box.

   To use this music source later, you must edit the music source to unlock it.
10. Click **Save**.

Adjusting the volume of the prompts

Before you begin

- Check each prompt for consistent volume and quality through playback of the prompt.
- Check that all the prompts have similar volume levels and quality.

About this task

After you configure the prompts, check the prompt volume on an external call. If the phones in your contact center play prompts at a low volume, use the following procedure to increase the volume.

Procedure

1. Log on to Element Manager.
2. Navigate to **System Configuration** > **Media Processing** > **Advanced Settings**.
3. In the **Announcement Volume Adjustment (db)** field, enter the announcement prompt volume level adjustment in decibels (db).

   Note:

   The default value is -1 db. The range is from -24 to 24 db.
4. Restart the server for the changes to take effect.

   Adjust the volume in small increments. For example, increase the volume from the default value of -10 db to -5db, until you are satisfied with the volume level. You can keep checking the volume by calling in to the contact center.

Configuring Avaya Aura® Media Server hostname verification

About this task

If Web Services security is on, modify the Avaya Aura® Media Server hostname verification to ensure CCMA can upload prompts.

Procedure

1. Log on to Element Manager.
2. In the Element Manager navigation pane, click **System Configuration** > **Network Settings** > **General Settings** > **Connection Security**.
3. Clear **Verify Host Name on HTTPS Client Connections**.
4. Click **Save**.
5. Click **Confirm**.

Configuring Avaya Aura® Media Server settings for SIP-enabled contact center

About this task

Configure the Avaya Aura® Media Server settings to ensure Avaya Aura® Media Server can provide the optimal service for the Contact Center application.

When installed, Avaya Aura® Media Server automatically enables debug tracing. Avaya Aura® Media Server is a software-based media processing platform. All media processing is performed in software on the host CPUs. Avaya Aura® Media Server therefore does not support debug tracing in production systems. When you have commissioned and tested your SIP-enabled contact center solution, you must disable trace debugging before placing the system in production.

Avaya Aura® Media Server supports Secure Real-Time Transport Protocol (SRTP).

Note:

Perform this procedure on every primary Avaya Aura® Media Server.

Procedure

1. Log on to Element Manager.
2. If the solution uses SRTP, skip to Step 5. If this solution does not use SRTP, in the navigation pane, click **System Configuration** > **Media Processing** > **Media Security**.
3. On the **Media Security** page, from the **Security Policy** list, select **Security Disabled**.
4. Click **Save**.

5. In the navigation pane, click **System Configuration** > **Media Processing** > **Audio Codecs**.
6. On the **Audio Codecs** page, ensure that the codecs you want to support appear in the **Enabled** list.

   Important:

   If you are using Avaya Contact Recorder (ACR) for call recording, you must ensure that you enable the G.729 codec. ACR call recording has no impact on the quality of voice calls between agents and customers.
7. Click **Save**.

Chapter 10: Contact Center Manager Administration commissioning

Commission Contact Center Manager Administration (CCMA) after you install Contact Center Manager Administration server software to prepare your server for Avaya Aura® Contact Center operations.

CCMA single sign-on enables you to map Contact Center users to network user accounts. Users can then use their network logon ID and password to access CCMA. For more information about single sign-on configuration, see Single sign-on commissioning on page 160.

Prerequisites for Contact Center Manager Administration commissioning

- Install the Contact Center software.
- Read *Avaya Aura® Contact Center Overview and Specification*.
- Ensure that you have administrator privileges on the Contact Center server.

Contact Center Manager Administration commissioning procedures

About this task

This task flow shows you the sequence of procedures you perform to commission Contact Center Manager Administration.

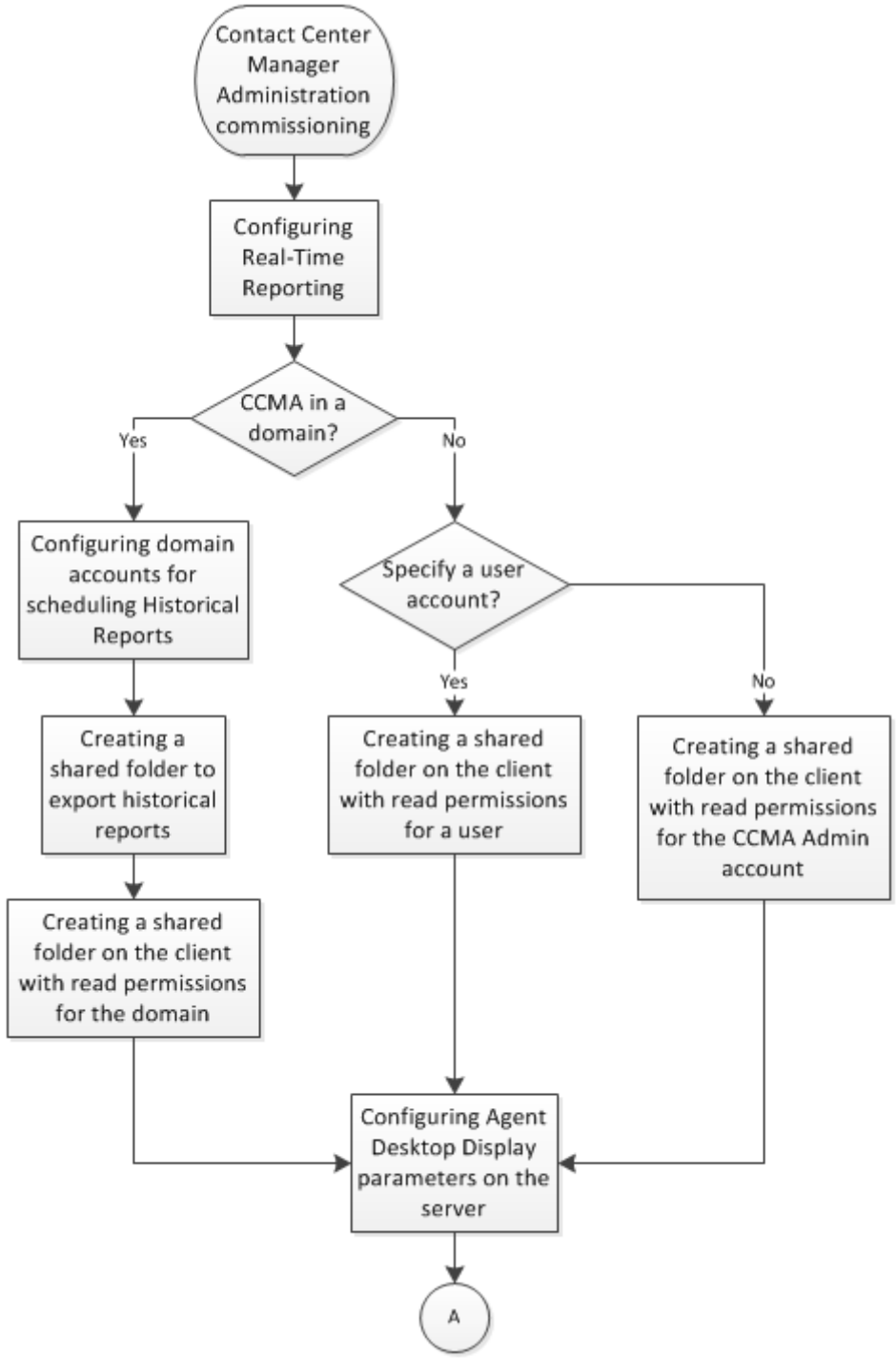


Figure 20: Contact Center Manager Administration commissioning procedures

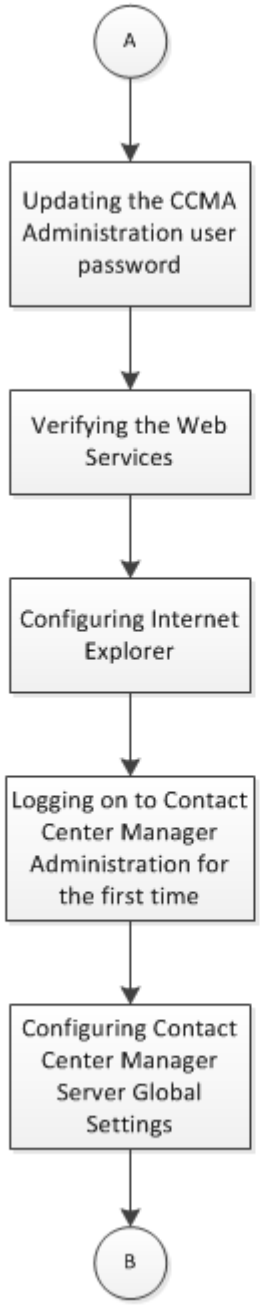


Figure 21: Contact Center Manager Administration commissioning procedures continued

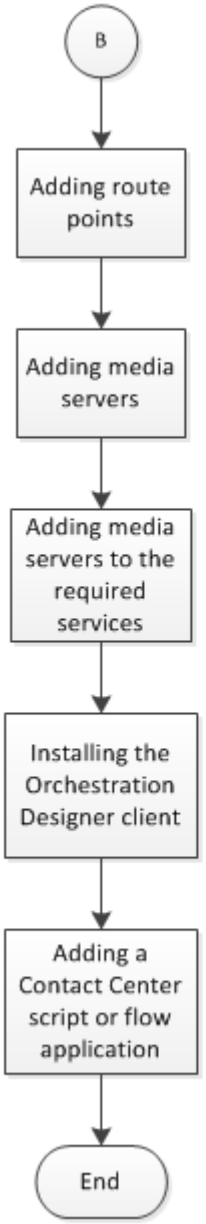


Figure 22: Contact Center Manager Administration commissioning procedures continued

Configuring Real-Time Reporting

Before you begin

- Ensure that the IP multicast addresses that you select for Real-time Statistics Multicast (RSM) sending and receiving are in the 224.0.1.0 to 239.255.255.255 range. Check with your network administrator for acceptable IP multicast addresses for your network.
- Ensure that the Contact Center Manager Administration server sending and receiving IP multicast addresses differ.
- If the Contact Center Manager Server is part of a networked Contact Center, ensure that all Contact Center Manager Servers within the network have the same multicast IP address.
- If your solution includes multiple instances of Contact Center Manager Administration, you must configure each Contact Center Manager Administration with different multicast IP send addresses.

Note:

In a High Availability solution, the active CCMA and the standby CCMA must have the same multicast IP send address.

About this task

Configure Real-Time Reporting if you plan to use multicast-based data transmission. You must configure the IP multicast addresses for the Contact Center Manager Server to receive Multicast data and the Contact Center Manager Administration server sending IP multicast data.

Note:

If you modify the Contact Center Manager Server multicast settings, you must modify the Contact Center Manager Administration multicast settings accordingly.

If you configure a standby server, you must select multicast for the transmission options under the Real-time Reporting Configuration.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.
3. In the **Avaya Applications Configuration** window, in the left pane, navigate to **Avaya** > **Applications** > **Real-Time Reporting**.
4. In the right pane, click the **RTR Registry Settings** icon.
5. In the **RTR Properties** dialog box, in the **IP Receive Address** box, type the Contact Center Manager Administration server receiving IP multicast address.
6. In the **IP Send Address** box, type the Contact Center Manager Administration server sending IP multicast address.
7. For the **Output Rate** box and the **Transform Rate** box, accept the default values (5000 and 1000).

Important:

You can adjust the default values; however, reducing the Output Rate value and the Transform Rate value increases the workload on the Contact Center Manager Administration server.

8. For the **OAM Timeout** box, accept the default value (120 000).
9. Select the **Compress Realtime Data Packets** check box.

   Important:

   If you clear this check box, you disable real-time data packet compression.
10. In the **Transmission Options** area, select one of the following options:
    - If your network supports multicast traffic, select **Multicast**. Avaya recommends this option.
    - To support both transmission types, select **Multicast and Unicast**.
11. If you selected the **Multicast** option, proceed to step 14 on page 105.
12. In the **Maximum Unicast Sessions** box, type the maximum number of simultaneous unicast sessions that you want the server to allow.
13. Select the **Restart Real Time Reporting Service** check box.
14. Click **OK**.

    The Restart ICERtdService status window appears while the service is restarting, and closes after the service successfully restarts.
15. Close all windows to complete the procedure.

Procedure job aid

You might need to increase the OAM Timeout value if the following situations occur:

- You can see no partition elements in the right pane when you create or view a partition in Access and Partition Management. This can occur when a large amount of data is stored on Contact Center Manager Server and the network is slow.
- Your Contact Center has a large numbers of agents or skillsets. In this case, it might not be possible to return a large list of agents or skillsets when you view a report using the Historical Reporting component.

If you increase the OAM Timeout value, this provides more time to collect the partition elements on each server. Avaya recommends that you increase this value in increments of 10 000 (milliseconds).

Configuring domain accounts to allow scheduling Historical Reports to a Network Server

Before you begin

- Understand how to update the CCMA Administration user password; see Updating the CCMA Administration user password on page 112.

About this task

If Contact Center CCMA is on a domain, configure a domain account to allow Historical Reports to run and be saved on a network server.

Procedure

1. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.
2. In the Avaya Applications Configuration window, in the left pane, expand **Avaya** > **Applications** > **IceAdmin Password Change**.
3. In the right pane, click the **IceAdmin Password Change** icon.
4. Click **Domain Account**.
5. Update the Domain Name, Domain User Account, and Password.
6. Click **OK**.

Creating a shared folder to export historical reports

Before you begin

- Grant change and read permissions to users who can access the scheduled report account; for example, the CCMA Admin account or the domain account.

About this task

Create a shared folder to export historical reports if you want multiple users to access scheduled historical reports stored in this folder from other computers.

Procedure

1. Log on to the server on which you installed the Contact Center Manager Administration server software.
2. Create a folder. Name the folder **Exported Reports**.
3. Right-click the new folder and select **Properties**.
4. In the **Properties** dialog box, on the **Sharing** page, click **Advanced Sharing**.
5. Select **Share this folder**.
6. Click **Permissions**.

7. Click **Add**.
8. In the **Select Users or Groups** dialog box, click **Advanced**.
9. Click **Find Now**.
10. In the expanded portion of the **Select Users or Groups** dialog box, locate and select the CCMA administrative account.

    OR

    Select the domain account used for IIS directory security.
11. Click **OK**.
12. In the **Select Users or Groups** dialog box, click **OK**.
13. In the **Permissions** dialog box, select the account that you selected in step 10 on page 107.
14. Select the **Allow** check box for the following:
    - **Change**
    - **Read**
15. Click **Apply**.
16. Click **OK** to close the **Permissions for Exported Reports** dialog box.
17. Click **OK** to close the **Advanced Sharing** dialog box.
18. Click **OK** to close the **Exported Reports Properties** dialog box.

Creating a shared folder on the client with read permissions for the domain

Before you begin

- Ensure that Contact Center Manager Administration is part of a network domain.
- Configure the domain account. See Configuring domain accounts to allow scheduling Historical Reports to a Network Server on page 106.

About this task

Create a shared folder with read permissions on the client for the domain account if Contact Center Manager Administration is part of a network domain. Use the shared folder to synchronize historical reports.

Procedure

1. On the client, create a folder.
2. Right-click the shared folder, and select **Properties**.

3. In the **New folder Properties** dialog box, click the **Sharing** tab.
4. Click **Advanced Sharing**.
5. Click **Share this folder**.
6. Click **Permissions**.
7. In the **Permissions for New folder** dialog box, Select **Everyone**.
8. Click **Remove** to remove the Everyone account.
9. Click **Add**.
10. In the **Select Users or Groups** dialog box, click **Advanced**.
11. Click **Find Now**.
12. In the expanded portion of the **Select Users or Groups** dialog box, locate and select the domain or directory security user account used to join the Contact Center Manager Administration server to the network domain.
13. Click **OK**.
14. In the **Select Users or Groups** dialog box, click **OK**.
15. In the **Permissions for New folder** dialog box, select the newly added group or user name account.
16. Select the **Allow** check box for **Read**.
17. Click **OK**.
18. Click **OK**.
19. Click **OK** to save your changes and close the **New folder Properties** dialog box.

Creating a shared folder on the client with read permissions for a user

Before you begin

- If Contact Center Manager Administration is part of a domain, configure the domain account. See Configuring domain accounts to allow scheduling Historical Reports to a Network Server on page 106.

About this task

Create a shared folder with read permissions on the client for a user account to ensure that the user can access the folder on the client.

Procedure

1. On the client, create a folder.
2. Right-click the folder, and select **Properties**.

3. In the **New folder Properties** dialog box, click the **Sharing** tab.
4. Click **Advanced Sharing**.
5. Click **Share this folder**.
6. Click **Permissions**.
7. In the **Permissions for New folder** dialog box, select the user login name.
8. Select the **Allow** check box for **Read**.
9. Clear all other check boxes.
10. Click **Apply**.
11. Click **OK**.
12. Click **OK**.
13. In the **New folder Properties** dialog box, click **Close**.

Creating a shared folder on the client PC with read permissions for the CCMA Administration account

Before you begin

- Ensure that Contact Center Manager Administration (CCMA) is part of a workgroup.

About this task

If CCMA is part of a workgroup, create a shared folder on the client PC with Read permissions for the CCMA Administration account, iceAdmin.

If you choose this option, you must maintain the CCMA Administration account on the client PC.

Procedure

1. On the client, create a folder.
2. Right-click the folder, and select **Properties**.
3. In the **New folder Properties** dialog box, click the **Sharing** tab.
4. Click **Advanced Sharing**.
5. Click **Share this folder**.
6. Click **Permissions**.
7. In the **Permissions for New folder** dialog box, Select **Everyone**.
8. Click **Remove** to remove the Everyone account.
9. Click **Add**.
10. In the **Select Users or Groups** dialog box, click **Advanced**.

11. Click **Find Now**.
12. In the expanded portion of the **Select Users or Groups** dialog box, locate and select the **iceAdmin** user account.
13. Click **OK**.
14. In the **Select Users or Groups** dialog box, click **OK**.
15. In the **Permissions** dialog box, select **iceAdmin**.
16. Select the **Allow** check box for **Read**.
17. Click **Apply**.
18. Click **OK**.
19. Click **OK** to close the **Advanced Sharing** dialog box.
20. Click **Close** to close the **New folder Properties** dialog box.

Configuring Agent Desktop Display parameters on the server

Before you begin

- Ensure that you have administrative privileges on the server on which you installed the Contact Center Manager Administration server software.

About this task

Configure parameters on the Contact Center Manager Administration server to use Agent Desktop Display on a client.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Agent Desktop Displays Configuration**.
3. In the **Configuration Parameters** dialog box, in the **IP multicast address** box, confirm that the address is the Contact Center Manager Administration server IP send address that you configured in the RTR Configuration Tool.
4. In the **Refresh rate (seconds)** box, type the rate in seconds at which you want the real-time data in the displays to be refreshed.
5. From the **View mode** list, select the mode in which you want to view the collected data:
   - **Moving window**
   - **Interval-to-date**
6. To require agents to log on to their phones before they can start Agent Desktop Display, select the **Agents phoneset login required for ADD** check box.

If this check box is clear, when an agent logs on to Agent Desktop Display, the agent sees data only if other agents log on to skillsets to which that agent is assigned.

7. To disable automatic notifications for Agent Desktop Display client upgrades, select the **Disable Automatic ADD Client Upgrade** check box.

   If you select this check box, agents receive no prompts to download available Agent Desktop Display client upgrades.

8. In the **Statistics Configuration** table, choose the statistics to appear in the Agent Desktop Display. You can add statistics columns to the displays or remove columns that you no longer want to show.
9. To add the statistics column to the displays, select the **Show** check box for each statistic.
10. Use the column order buttons to arrange the order in which the statistics columns appear. Select the statistic to move, and then click the up or down button to change its position.

    The statistic that you place at the top of the Statistics Configuration table appears in the first column of the display.

11. To assign the threshold display color, select a statistic.
12. From the following lists, select the threshold color for the highlighted statistic:

    - **Less than Level 1**
    - **Between Level 1 and Level 2**
    - **Greater than Level 2**

      If you configure no threshold levels in the Configuration component of Contact Center Manager Administration or in Contact Center Manager Server, the values appear in white in the Agent Desktop Display.

13. Repeat step 12 on page 111 to step 13 on page 111 for each statistic for which you want to configure threshold display colors.
14. If you want the selected statistic to blink in the Agent Desktop Display when its value reaches the threshold, select the **Blink** check box.
15. If you want the Agent Desktop Display to beep when the threshold value reaches the threshold, select the **Beep** check box.
16. If you did not select the **Beep** check box, proceed to step 20 on page 111.
17. To indicate that a beep occurs only once, select **Once**.
18. To indicate that a beep occurs continuously until the statistic reaches an acceptable value, select **Continuously**.
19. Click **Save**.

Variable definitions

Name	Description
IP multicast address	The IP multicast addresses that you select for RSM sending and receiving must be in the 224.0.1.0 to 239.255.255.255 range. Check with your network administrator for acceptable IP multicast addresses for your specific network.
Refresh rate	The minimum value that you can type in this box is 2 seconds. You must specify a value for the refresh rate.
View mode	Select one of the following view modes: • Moving window—In moving window mode, statistics represent the last 10 minutes of system activity. • Interval-to-date—In interval-to-date mode, statistics are collected only for the current interval. When the interval ends, data fields reset to 0 and collection begins for the next interval. The interval can correspond to a work shift or to another system-defined period.

Updating the CCMA Administration user password

Before you begin

- Use System Control and Monitor Utility (SCMU) to stop all Contact Center Manager Administration (CCMA) services.
- Reset Internet Information Services (IIS) (using the **`iisreset`** command) on the CCMA server.

About this task

Update the CCMA Administration account password on your CCMA server using the IceAdmin Password Change utility.

The CCMA Administration account is an administrator account for the CCMA server.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.
3. In the Avaya Applications Configuration window, in the left pane, expand **Avaya** > **Applications** > **IceAdmin Password Change**.
4. In the right pane, click the **IceAdmin Password Change** icon.

5. In the **Old Password** box, type the current password for the CCMA Administration user account.

   Important:

   If you use this utility for the first time, you cannot enter the old password because the box is dimmed.

6. In the **New Password** box, type the new password for the CCMA Administration user account.
7. In the **Confirm Password** box, type the new password again.
8. Click **OK**.
9. Use System Control and Monitor Utility (SCMU) to start CCMA.

Verifying web services

About this task

Verify CCMA web services. The web services displayed in green are running correctly.

Procedure

1. Open Microsoft Edge in Internet Explorer mode.
2. Type `https://<ccmaservername>/supportutil/testwebservices.asp` to check that web services are running correctly.

   If you turned off Web Services security, use `http://` instead.

Configuring internet options

About this task

To access Contact Center Manager Administration and other Contact Center applications, use Microsoft Edge in Internet Explorer mode. This procedure describes how to configure the internet options in your browser.

Procedure

1. In Microsoft Edge, navigate to **More tools** > **Internet Options**.
2. Click the **Security** tab.
3. Click **Trusted Sites**.
4. Click **Custom Level**.

   The Security Settings window for trusted sites is displayed.

5. Under the **.NET Framework-reliant components** heading, select **Enable** for the following:
   - **Run components not signed with Authenticode**
   - **Run components signed with Authenticode**
6. Under the **ActiveX controls and plug-ins** heading, select **Enable** for the following:
   - **Automatic prompting for ActiveX controls**
   - **Run ActiveX Controls and plug-ins**
   - **Script ActiveX Controls marked safe for scripting**
7. Under the **Downloads** heading, select **Enable** for the following:
   - **Automatic prompting for file downloads**
   - **File download**
8. Under the **Miscellaneous** heading, select **Enable** for the following:
   - **Allow script-initiated windows without size or position constraints**
   - **Allow websites to open windows without address or status bars**
9. Click **OK** and confirm if prompted.
10. On the Security tab, click the **Trusted Sites** icon again.
11. Click **Sites**.

    The Trusted sites window is displayed.
12. Clear the **Require server verification {https:} for all sites in this zone** check box.
13. In the **Add this website to the zone** field, type the server name or FQDN of your Contact Center server.

    Do not type the IP address instead of the server name.
14. Click **Add**.
15. In the **Add this website to the zone** field, type the server name (not the IP address) of your Contact Center Multimedia server.
16. Click **Add**.
17. If your contact center includes a Predictive Reporting server, in the **Add this website to the zone** field, type the server name (not the IP address) of your Predictive Reporting server.
18. Click **Add**.
19. Click **Close** to return to the Internet Properties window.
20. Click the **Privacy** tab.
21. Select the **Turn on Pop-up Blocker** check box.
22. Click **Settings**.

    The Pop-up Blocker Settings window is displayed.

23. In the **Address of website to allow** field, type the Contact Center Manager Administration URL.

    The default URL is `https://<server name>`, where <*server name*> is the name of the Contact Center Manager Administration server. If you turned off Web Services security, use `http://` instead of `https://`.

24. Click **Add**.
25. Click **Close** to return to the Internet Properties window.
26. Click the **Advanced** tab.
27. If HTTPS and TLS are enabled, under **Security**, clear the **Do not save encrypted pages to disk** check box.
28. Apply your changes.
29. Restart your browser to activate your changes.

Accessing Contact Center Manager Administration from Microsoft Edge in Internet Explorer mode

You can access Contact Center Manager Administration using the Microsoft Edge browser in Internet Explorer (IE) mode. To enable IE mode in Microsoft Edge, perform the following procedures:

1. Adding the Microsoft Edge administrative templates on page 116.
2. Configuring integration with Internet Explorer on page 116.
3. Configuring the Enterprise Mode Site List on page 117.

Before enabling IE mode in Microsoft Edge, install all recent Windows updates. Ensure that Microsoft Edge is installed at the system level. You can check it by typing `edge://version` in the Microsoft Edge address field. The executable path must start with `C:\Program Files`, which indicates a system install.

For more information about IE mode in Microsoft Edge, refer to the Microsoft documentation.

Important:

- Always start CCMA in a new browser tab.
- If you enabled SSO for your Contact Center, add the System Manager server FQDN to the Enterprise Mode Site List.
- For solutions with geographic redundancy, add the RGN server short name and FQDN to the Enterprise Mode Site List.
- For High Availability solutions, add the Managed Name and Managed FQDN of the HA pair to the Enterprise Mode Site List. Do not add short names and FQDNs of your active and standby servers.

Adding the Microsoft Edge administrative templates

About this task

Use this procedure to add the Microsoft Edge administrative templates to your computer.

Procedure

1. On the Microsoft website, go to the Edge for Business download page: https://www.microsoft.com/en-us/edge/business/download.
2. From the lists, select your current browser version, build, and platform.
3. Click the **Get Policy Files** button.
4. Click **Accept and download** to download the `MicrosoftEdgePolicyTemplates` file.

   The `MicrosoftEdgePolicyTemplates` archive is downloaded to the default folder on your computer.
5. Unzip the `MicrosoftEdgePolicyTemplates` archive.
6. Open the `MicrosoftEdgePolicyTemplates` folder and navigate to `windows\admx`.
7. From the `admx` folder, copy the `msedge.admx` file.
8. Navigate to `C:\Windows\PolicyDefinitions` and paste the `msedge.admx` file to the `PolicyDefinitions` folder.
9. In the `admx` folder, open the required language folder.

   For example, for the United States, open the `en-Us` folder.
10. From the language folder, copy the `msedge.adml` file.
11. Navigate to `C:\Windows\PolicyDefinitions` and paste the `msedge.adml` file to the matching language folder in the `PolicyDefinitions` folder.
12. **(Optional)** Verify that you have added the Microsoft Edge administrative template correctly by doing the following:

    a. Press `Win+R` and run `gpedit.msc` to open the Local Group Policy Editor.

    b. Click **Computer Configuration** > **Administrative Templates**.

    The `Administrative Templates` folder contains folders with the Microsoft Edge administrative templates.

Next steps

Configure web browser integration using Local Group Policy Editor.

Configuring integration with Internet Explorer

About this task

Use this procedure to enable your browser to work with Local Group Policy Editor.

Before you begin

Add the Microsoft Edge administrative templates to your computer.

Procedure

1. Press `Win+R` and run `gpedit.msc` to open the Local Group Policy Editor.
2. Click **Computer Configuration** > **Administrative Templates** > **Microsoft Edge**.
3. In the Microsoft Edge pane, double-click **Configure Internet Explorer integration**.
4. In the Configure Internet Explorer integration window, select **Enabled**.
5. From the **Configure Internet Explorer integration** list, select **Internet Explorer mode**.

   This is the default option for accessing CCMA in Microsoft Edge.
6. Click **OK**.

Result

IE mode in Microsoft Edge is now enabled.

Next steps

Configure the site list that you want to access using IE mode in Microsoft Edge.

Configuring the Enterprise Mode Site List

About this task

Use this procedure to configure the Enterprise Mode Site List.

On your computer, create an XML file with the list of sites that you want to access using Microsoft Edge in Internet Explorer mode.

The XML file must contain the following elements:

- **site-list version** number: The browser uses this number to verify whether the site list is new. Approximately 65 seconds after the browser starts, it compares your site list version to the stored version number. You must increase the site-list version number every time you update the Enterprise Mode Site List version.
- **<compat-mode>** tag: This tag specifies the compatibility settings for a specific site or domain. Use the `default` value.
- **<open-in>** tag: This tag specifies which browser version opens for a specific site or domain. Use the latest supported browser version.

Before you begin

- Add the Microsoft Edge Policy templates to your computer.
- Ensure that you have your Contact Center server short name and FQDN.
- If you enabled SSO for your Contact Center, ensure that you have your System Manager server FQDN.
- For a solution with geographic redundancy, ensure that you know your RGN server short name and FQDN.

- For a HA solution, ensure that your have your HA pair managed name and managed FQDN.

Procedure

1. On your computer, create the `sites.xml` file using the following template:

```
<site-list version="1">
    <!-- File creation header -->
    <created-by>
        <tool>EnterpriseSitelistManager</tool>
        <version>10240</version>
        <date-created>20200717.142200</date-created>
    </created-by>
    <!-- Begin Site List -->
    <site url="server short name">
        <compat-mode>default</compat-mode>
        <open-in>IE11</open-in>
    </site>
    <site url="server FQDN">
        <compat-mode>default</compat-mode>
        <open-in>IE11</open-in>
    </site>
</site-list>
```

2. In the first `<site>` element, for the `url` attribute, type the Contact Center server short name.

   For example, if your Contact Center server short name is `auracc12680`, use the following code: `<site url="auracc12680">`.

   For a HA solution, you must use your HA pair managed name instead of the server short name.

3. In the second `<site>` element, for the `url` attribute. type the Contact Center server FQDN.

   For example, if your Contact Center server FQDN is `auracc12680.aacc7dc2012.com`, use the following code: `<site url="auracc12680.aacc7dc2012.com">`.

   For a HA solution, you must use your HA pair managed FQDN instead of the server FQDN.

4. **(Optional)** Add your System Manager server to the site list using the following template:

```
<site url="SMGR server FQDN">
        <compat-mode>default</compat-mode>
        <open-in>IE11</open-in>
</site>
```

   For example, if your System Manager server FQDN is `smgr80176.aacc7dc2012.com`, use the following code: `<site url="smgr80176.aacc7dc2012.com">`.

5. **(Optional)** Add your RGN server to the site list using the following template:

```
<site url="RGN server short name">
        <compat-mode>default</compat-mode>
        <open-in>IE11</open-in>
</site>
<site url="RGN server FQDN">
        <compat-mode>default</compat-mode>
```

```
        <open-in>IE11</open-in>
</site>
```

6. Press `Win+R` and run `gpedit.msc` to open the Local Group Policy Editor.
7. Click **Computer Configuration** > **Administrative Templates** > **Microsoft Edge**.

   Local Group Policy Editor displays the Microsoft Edge pane.
8. In the Microsoft Edge pane, double-click **Configure the Enterprise Mode Site List**.
9. In the Configure the Enterprise Mode Site List window, select **Enabled**.
10. In the Options field, type the `sites.xml` location.

    For example: `file:///c:/Users/`*`user_name`*`/Documents/sites.xml`.
11. Click **OK**.
12. **(Optional)** In the Microsoft Edge address bar, type `edge://compat/enterprise` and press `Enter`.

    Microsoft Edge displays the Enterprise Mode Site List page, where you can view the current list of sites that Microsoft Edge opens in IE mode. Microsoft Edge automatically checks if there is a newer site list version and updates it approximately 65 seconds after launch. However, you can also manually configure Microsoft Edge to use the latest site list version by clicking **Force Update**.

Next steps

Launch Microsoft Edge and wait for approximately 65 seconds. You can now access CCMA using Microsoft Edge in IE mode.

Internet Explorer mode and Compatibility View configuration on the domain server

If you cannot configure IE mode or Compatibility View from a local computer, you can configure these settings on the domain server. For example, if you cannot use Internet Explorer according to your enterprise security policies, you can configure Compatibility View settings on the domain server.

To enable IE mode for Microsoft Edge on the domain server, perform the following procedures:

1. Adding the Microsoft Edge administrative templates to the domain server on page 120.
2. Creating a configuration file for Internet Explorer mode on page 121.
3. Enabling IE mode on the domain server on page 123.
4. Completing IE mode configuration on a local computer on page 125.

To enable Compatibility View on the domain server, see Configuring Compatibility View settings on the domain server on page 125.

For more information about IE mode in Microsoft Edge and Compatibility View, refer to the Microsoft documentation.

Important:

- If you use Windows 10, do not delete the Internet Explorer browser from your computer. Microsoft Edge for Windows 11 includes the Internet Explorer engine. Microsoft Edge uses the Internet Explorer engine to launch CCMA.
- Always launch CCMA in a new tab of Microsoft Edge.
- If you enabled SSO, add the System Manager server FQDN to the Enterprise Mode Site List.
- For solutions with geographic redundancy, add the RGN server short name and FQDN to the Enterprise Mode Site List.
- For High Availability solutions, add only the Managed Name and Managed FQDN of the HA pair to the Enterprise Mode Site List. Do not add short names and FQDNs of your active and standby servers.

Adding the Microsoft Edge administrative templates to the domain server

About this task

Use this procedure to add the Microsoft Edge administrative templates to the domain server.

Procedure

1. On the Microsoft website, go to the **Edge for Business** download page: https://www.microsoft.com/en-us/edge/business/download.
2. Click the **GET POLICY FILES** button.
3. Click **Accept and download** to download the `MicrosoftEdgePolicyTemplates` file.

   The `MicrosoftEdgePolicyTemplates` archive is downloaded to the default folder on your computer.
4. Unzip the `MicrosoftEdgePolicyTemplates` archive.
5. Open the `MicrosoftEdgePolicyTemplates` folder and navigate to `windows\admx`.
6. From the `admx` folder, copy the `msedge.admx` file.
7. Upload the `msedge.admx` file to the domain server to the `C:\Windows\PolicyDefinitions` folder.

   Use a file transfer program of your choice, such as SFTP, SCP, or WinSCP.
8. On your local computer, re-open the `MicrosoftEdgePolicyTemplates` folder and navigate to the `windows\admx\` folder.
9. In the `admx` folder, open a folder corresponding to the language and locale you use on Contact Center.

   For example, for the United States, open the `en-US` folder.
10. From the language folder, copy the `msedge.adml` file.

11. Upload the `msedge.adml` file to the domain server to the `C:\Windows\PolicyDefinitions\<LANGUAGE_FOLDER>` folder.

    In this file path, `<LANGUAGE_FOLDER>` is the language folder with the same name that you selected in step 9. For example, for the United States, copy `msedge.adml` to the `C:\Windows\PolicyDefinitions\en-US` folder.

Next steps

Create a configuration file for IE mode.

Creating a configuration file for Internet Explorer mode

About this task

Create an XML file that contains a list of sites you need to access from Microsoft Edge in IE mode. You will use this file to configure the Enterprise Mode Site List on the domain server.

The XML file must contain the following elements:

- **site-list version** number: The browser uses this number to verify whether the site list is new. Approximately 65 seconds after the browser starts, it compares your site list version to the stored version number. You must increase the site-list version number every time you update the Enterprise Mode Site List version.
- **<compat-mode>** tag: This tag specifies the compatibility settings for a specific site or domain. Use the `default` value.
- **<open-in>** tag: This tag specifies the browser version that opens for a specific site or domain.

  Use the latest supported browser version.

Before you begin

- Add the Microsoft Edge Policy templates to the domain server.
- Ensure that you have your Contact Center server short name and FQDN.
- If you enabled SSO for your Contact Center, ensure that you have your System Manager server FQDN.
- For a solution with geographic redundancy, ensure that you know your RGN server short name and FQDN.
- For a HA solution, ensure that your have your HA pair managed name and managed FQDN.

Procedure

1. Create an XML file using the following template:

```
<site-list version="1">
    <!-- File creation header -->
    <created-by>
        <tool>EnterpriseSitelistManager</tool>
        <version>10240</version>
        <date-created>20200717.142200</date-created>
    </created-by>
    <!-- Begin Site List -->
    <site url="<SERVER SHORT NAME>">
        <compat-mode>default</compat-mode>
```

```
        <open-in>IE11</open-in>
    </site>
    <site url="<SERVER FQDN>">
        <compat-mode>default</compat-mode>
        <open-in>IE11</open-in>
    </site>
</site-list>
```

2. In the first `<site>` element, for the `url` attribute, type the short name of your Contact Center server.

   For example, if the short name of your Contact Center server is `auracc12680`, use the following code:

   ```
   <site url="auracc12680">
   ```

   For a HA solution, you must use your HA pair managed name instead of the server short name.

3. In the second `<site>` element, for the `url` attribute, type the Contact Center server FQDN.

   For example, if your Contact Center server FQDN is `auracc12680.aacc7dc2012.com`, use the following code:

   ```
   <site url="auracc12680.aacc7dc2012.com">
   ```

   For a HA solution, you must use your HA pair managed FQDN instead of the server FQDN.

4. **(Optional)** If you use SSO on your Contact Center, add a new `<site>` element for System Manager to the file using the following template:

   ```
   <site url="SMGR server FQDN">
           <compat-mode>default</compat-mode>
           <open-in>IE11</open-in>
   </site>
   ```

   For example, if your System Manager FQDN is `smgr80176.aacc7dc2012.com`, use the following code:

   ```
   <site url="smgr80176.aacc7dc2012.com">
           <compat-mode>default</compat-mode>
           <open-in>IE11</open-in>
   </site>
   ```

5. **(Optional)** For a solution with geographic redundancy, add a new `<site>` element for your RGN server to the site list using the following template:

   ```
   <site url="RGN server short name">
           <compat-mode>default</compat-mode>
           <open-in>IE11</open-in>
   </site>
   <site url="RGN server FQDN">
           <compat-mode>default</compat-mode>
           <open-in>IE11</open-in>
   </site>
   ```

6. Save the file using the `sites.xml` name.

Next steps

- Upload the configuration file to one of the following locations:
  - To the CCMA server. For more information about uploading the file to the CCMA server, see Uploading the configuration file for IE mode to the CCMA server on page 123.
  - To a shared folder on the domain server.
- Enable IE mode on the domain server.

Uploading the configuration file for IE mode to the CCMA server

About this task

You can store the configuration file `sites.xml` for IE mode on the CCMA server.

Before you begin

Create the configuration file `sites.xml` for IE mode.

Procedure

1. Copy the `sites.xml` file to the CCMA server to the `D:\Avaya\Contact Center\Manager Administration\Apps` folder.

   Use a file transfer program of your choice, such as SFTP, SCP, or WinSCP.

2. If you use SSO, do the following:

   a. Add the following entry to the `AgentPromValues.xml` file, which is located in the `D:\Avaya\Contact Center\Manager Administration\Server\Data` folder:

   ```
   <NOT_ENFORCED value="sites.xml*" />
   ```

   b. On the Contact Center, disable SSO.

   c. Re-enable SSO.

3. Open Microsoft Edge, enable the Internet Explorer mode, and then type the following URL in the address bar:

   `https://<CCMA_FQDN>/sites.xml`

   In this URL, `<CCMA_FQDN>` is the FQDN of the CCMA server.

4. Ensure that you can view the `sites.xml` file contents in the browser.

Next steps

Enable IE mode on the domain server.

Enabling IE mode on the domain server

About this task

Enable IE mode on the domain server to access CCMA from Microsoft Edge.

Before you begin

- Add the Microsoft Edge Policy templates to your computer.
- Create the configuration file `sites.xml` for IE mode.
- Upload the configuration file to one of the following locations:
  - To the CCMA server. For more information about uploading the file to the CCMA server, see Uploading the configuration file for IE mode to the CCMA server on page 123.
  - To a shared folder on the domain server.

Procedure

1. On the domain server, navigate to **Control Panel** > **Administrative tools** > **Group Policy Management**.
2. Go to your domain.
3. Right-click the domain group policy and click **Edit**.
4. In the Group Policy Management Editor, go to **Computer Configuration** > **Policies** > **Administrative Templates** > **Microsoft Edge**.

   The Group Policy Management Editor displays the Microsoft Edge pane.
5. In the Microsoft Edge pane, double-click **Configure Internet Explorer integration**.
6. In the Configure Internet Explorer Integration window, select **Enabled**.
7. In the Options area, from **Configure Internet Explorer integration**, select one of the following:
   - **Internet Explorer mode**: To open sites in Microsoft Edge in IE mode.
   - **None**: To prevent users from configuring IE mode using `edge://flags` or CLI.
8. Click **OK**.
9. In the Group Policy Management Editor, go to **Computer Configuration** > **Policies** > **Administrative Templates** > **Microsoft Edge**.
10. In the Microsoft Edge pane, double-click **Configure the Enterprise Mode Site List**.
11. In the Configure the Enterprise Mode Site List window, select **Enabled**.
12. In the Options area, from **Configure the Enterprise Mode Site List**, specify the location of the `sites.xml` configuration file as follows:
    - If the `sites.xml` file is on the CCMA server, use the following format:

      `https://<CCMA FQDN>/sites.xml`

      In this entry, `<CCMA_FQDN>` is the FQDN of the CCMA server. For example:

      `https://192.0.2.1/sites.xml`
    - If the `sites.xml` file is in a shared folder on the domain server, use the following format:

      `\\<NETWORK_PATH>\sites.xml`

In this entry, `<NETWORK_PATH>` is the full path to the `sites.xml` on the domain server. For example:

```
\\198.51.100.1\Shared\sites.xml
```

13. Click **OK** to save the policy settings.

Next steps

Complete IE mode configuration on a client computer.

Completing IE mode configuration on a local computer

About this task

After configuring IE mode on the domain server, update group policies on the local computer you use to access CCMA and ensure you can access CCMA using Microsoft Edge.

Before you begin

- Configure IE mode on the domain server.
- Ensure that the operating system and Microsoft Edge browser installed on your local computer comply with the system requirements for IE mode listed at https://docs.microsoft.com/en-us/deployedge/edge-ie-mode.

Procedure

1. On your local computer, run the following command:

   ```
   gpupdate /force
   ```

2. To check if Group Policy Objects are applied, run the following command:

   ```
   gpresult /r
   ```

   In the command output, the Applied Group Policy Objects section must contain the domain group policy name that you configured on the domain server.

3. In the Microsoft Edge address bar, type `edge://compat/enterprise` and ensure that the Enterprise Mode Site List tab contains the `sites.xml` file you added to the domain server.

4. In Microsoft Edge, open the CCMA site.

Next steps

Configure the Compatibility View List on the domain server.

Configuring Compatibility View settings on the domain server

About this task

Compatibility View is a feature that enables you to open websites that are incompatible with the latest browser version. If Microsoft Edge cannot display the CCMA site even in IE mode, you can configure Compatibility View settings for the CCMA site. If you cannot configure the Compatibility View settings on your local computer, you can configure them on the domain server.

If you are using Windows 11, you do not need to enable Compatibility View.

Important:

In this procedure, you will add a registry key to Group Policy Objects. If you change your Compatibility View settings, you must delete this registry key and then add it again.

Procedure

1. On the domain server, start Microsoft Edge with Internet Explorer mode.
2. Click the **Tools** icon and then click **Compatibility View Settings**.

   The browser displays the Compatibility View Settings window.
3. In **Add this website**, type your domain name and then click **Add**.
4. On the domain server, go to **Control Panel** > **Administrative tools** > **Group Policy Management**.
5. Select your domain.
6. Right-click the domain group policy and click **Edit**.

   You can also create a new domain group policy and link it to the domain.
7. In the Group Policy Management Editor, go to **User Configuration** > **Preferences** > **Windows Settings** > **Registry**.
8. Right-click **Registry** and click **New** > **Registry Wizard**.
9. In the Registry Wizard, select the local machine and then navigate to **HKEY_CURRENT_USER** > **Software** > **Microsoft** > **Internet Explorer** > **BrowserEmulation** > **ClearableListData**.
10. Select the check box for the UserFilter parameter.
11. Click **Finish**.
12. On your local computer, to update the group policy settings, run the following command:

    ```
    gpupdate /force
    ```
13. To check if Group Policy Objects are applied, run the following command:

    ```
    gpresult /r
    ```

    In the command output, the Applied Group Policy Objects section must contain the domain group policy name that you configured on the domain server.
14. **(Optional)** Verify that the registry key `HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\BrowserEmulation\ClearableListData\UserFilter` contains the same value that is configured on the domain server.
15. Restart Microsoft Edge in Internet Explorer mode to apply the changes in the Compatibility View settings.

Disabling Internet Explorer 11 as a standalone browser

About this task

Disable Internet Explorer 11 as a standalone browser to force users in your domain to use Microsoft Edge. When users try to open shortcuts or files associated with Internet Explorer 11, URLs open in Microsoft Edge instead.

Before you begin

Ensure that the operating system and Microsoft Edge browser installed on your local computer comply with the system requirements for IE mode listed at https://docs.microsoft.com/en-us/deployedge/edge-ie-disable-ie11.

Procedure

1. On the domain server, navigate to **Control Panel** > **Administrative Tools** > **Group Policy Management**.
2. Go to your domain.
3. Right-click the domain policy and click **Edit**.

   You can also create a new domain policy and link it to the domain.
4. In the Group Policy Management Editor, go to **Computer Configuration** > **Policies** > **Administrative Templates** > **Windows components** > **Internet Explorer**.
5. In the Microsoft Edge pane, double-click **Disable Internet Explorer 11 as a standalone browser** and select **Enabled**.
6. In the Options area, select one of the following:
   - **Never**: To notify users that Internet Explorer is disabled.
   - **Always**: To notify users every time they are redirected from Internet Explorer.
   - **Once per user**: To notify users only the first time they are redirected.
7. Click **OK**.
8. Log in to a computer in the domain and run the `gpupdate /force` command.
9. To check if Group Policy Objects are applied, run the `gpresult /r` command.

Logging in to Contact Center Manager Administration for the first time

About this task

When you log in to Contact Center Manager Administration for the first time, you must log in as the default administrator, webadmin. For security reasons, you must change the default password when you first log in to the application. For information about default login values, see *Avaya Aura® Contact Center Server Administration*.

If you did not turn off Web Services security, you must install the Certificate Authority root certificate on each CCMA web client computer. If you are using TLS, the server name must be the FQDN name that was used when generating the certificate in Security Manager.

Before you begin

- Ensure that the Contact Center Manager Server (CCMS) name is registered either with the Domain Name Service (DNS) or in the HOSTS table.
- To access CCMA and other Contact Center applications, ensure that you are using Microsoft Edge in Internet Explorer mode.

Procedure

1. In the **Address** field in your browser, type the server name (not the IP address) and then press `Enter`.

   For example, type `https://<server name>`. If you turned off Web Services security, type `http://<server name>`.
2. In the main login page, in the **User ID** field, type your username.
3. In the **Password** field, type the password.
4. Click **Login**.

   When logging in for the first time, you are prompted to change your password.
5. In the **Old password** field, type the old password.
6. In the **New password** field, type a new password.

   CCMA user passwords can contain only English characters and special characters. Passwords must be at least eight characters long, and include at least one number, one uppercase letter, one lowercase letter, and no spaces.
7. In the **Confirm password** field, type the new password again.

   You can only modify the default password. You cannot change the default username, webadmin.

   Important:

   If you lose or forget the new webadmin password, you cannot log in to CCMA as the webadmin administrator. To avoid this scenario, in Access and Partition Management, you can create a new user account with administrator rights, such as tempadmin. If you forget or lose the new webadmin password, you can log in to the CCMA server as tempadmin to change the password. If you forget all passwords for accounts with administrator rights, contact support personnel to have the webadmin password reset.
8. Click **Change Password**.
9. On the login page, type the username and your new password.
10. Click **Login**.
11. Click **OK**.

12. In the **Display Name** field for the current CCMS, type the name of the server as you want it to appear in the system tree in CCMA.

    Contact Center automatically creates a display name that is the same as the server name.
13. In the **Login ID** field, type the sysadmin username.
14. In the **Password** field, type the password for the CCMS.
15. If you see a login sequence error message, log in to Server Utility to check your username and password.
16. Click **Submit**.

    The CCMA launchpad is displayed.

Variable definitions

Name	Description
Contact Center Manager Administration Server name	The name of the Contact Center Manager Administration server.

Configuring Contact Center Manager Server global settings

About this task

Configure Contact Center Manager Server global settings to set up the Agent Order Preference, Default DN, Expected Wait Time algorithm, and the server designated for historical statistical data.

Configure a Default DN to catch treated calls that are defaulted by the contact center script or not answered by agents. Avaya recommends that you configure an attendant as the Default DN.

Procedure

1. Log in to Contact Center Manager Administration.

   If configured in the security settings, CCMA displays the date and time of your last login and the number of failed login attempts since your last successful login.
2. From the Launchpad, click **Configuration**.
3. In the left pane, expand the Contact Center Manager Server on which to configure global settings.
4. Select the **Global Settings** folder.
5. Configure the global settings for your Contact Center based on the fields listed in the Global Settings window.
6. In the **Default DN** field, type the default DN to use when a script defaults or a treated call is not answered.

Consider configuring an attendant as the default DN.

7. Click **Submit**.

Adding route points

About this task

Add route points to your contact center to route contacts.

Procedure

1. Log on to Contact Center Manager Administration with administrative privileges.
2. On the **Launchpad**, click **Configuration**.
3. In the left pane, click the plus sign (+) next to the Contact Center Manager Server to which you want to add the route point.
4. Select the **CDNs (Route Points)** folder.
5. On the **CDNs (Route Points)** window, in the **Name** box, type the name of the route point.
6. In the **Number** box, type the number for the route point.
7. In the **URI** box, type the value for the Uniform Resource Indicator (URI) of the route point on the server.
8. From the **Call Type** list, select **Local**.
9. Click any other row of the table to save the Route Point.
10. Select the **Acquired** check box.
11. Click any other row of the table to acquire the Route Point.
12. Click **Refresh Status** and confirm that the route point has an Acquired status.

Variable definitions

Name	Description
Name	A name that describes the route point, type, or function (for example, IM_sales for an IM route point that handles sales).
Number	The number used internally by the SIP-enabled contact center that is inherited from AML-based contact centers and appears in the TFE scripts as a CDN.

Table continues…

Name	Description
URI	The URI the SIP-enabled contact center accepts for processing by the SIP-enabled contact center. INVITEs received that do not match these URI are rejected. Avaya recommends that you use lowercase letters for URIs.
Type	Local or network. You must enable the networking option to use the Route Point for network calls.
Acquired	Select this check box to indicate to the system to acquire and process calls using this URI.

Adding media servers

About this task

Add media servers to Contact Center Manager Server using Contact Center Manager Administration.

Avaya Aura® Contact Center uses Avaya Aura® Media Server media processing capabilities. Configure each Avaya Aura® Media Server in a Contact Center as a Media Server.

Procedure

1. Log on to Contact Center Manager Administration with administrator privileges.
2. On the **Launchpad**, click **Configuration**.
3. In the left pane, click the plus (+) sign next to the SIP-enabled Contact Center Manager Server.
4. From the list of configuration items for the Contact Center Manager Server, select **Media Services and Routes** and delete Avaya Aura® Media Server from the **Selected** list.

   If Avaya Aura® Media Server is not on the **Selected** list, move to the next step directly.
5. From the list of configuration items for the Contact Center Manager Server, select **Media Servers**.
6. On the **Media Servers** window, under **Master Content Store** , uncheck the default Avaya Aura® Media Server check box and then delete the Avaya Aura® Media Server.

   To delete the server, highlight the row and press the **Delete** button on the keyboard.
7. Add Avaya Aura® Media Server to Contact Center Manager Server Configuration as the trusted host name (AMS server name or AMS FQDN name).

   The trusted host name is the Avaya Aura® Media Server name or Avaya Aura® Media Server FQDN name that is used to sign the certificate.

Note:

If you are using the Avaya Aura® Media Server High Availability (HA) feature enter the AMS managed name (short name or FQDN name) already signed in the certificate.

8. In the **IP Address** box, type the IP address of each Avaya Aura® Media Server media server. If you are using the Avaya Aura® Media Server – High Availability (HA) feature, type the Managed IP address of the Avaya Aura® Media Server HA pair only. Do not type the IP address of the primary or backup Avaya Aura® Media Server. On the Avaya Aura® Media Server the Managed IP address is configured under **High Availability** as the **Service IP Address**. For more information, see Enabling High Availability on the backup server on page 75.
9. In the **Port Number** box, type the port number.

   Important:

   The port number must match the Avaya Aura® Media Server port number. The default port number is 5060.

   Avaya Aura® Media Server does not have TLS configured at this stage of the commissioning process, but if you enable it later you must change this port to 5061. For more information, see Avaya Aura Media Server security and SRTP commissioning on page 151.
10. Select the **Master Content Store** check box for the Avaya Aura® MS server that manages media and prompts.

    Master Content Store is the Avaya Aura® MS server that manages the prompts. If the Avaya Aura® MS server does not contain existing contact center media, Contact Center Manager Administration uploads base media to it. If the Avaya Aura® MS server does contain media, it is left as is and the existing media content is not overwritten.

    Note:

    You must select the **Master Content Store** check box for only one media server. If you try to select the **Master Content Store** check box for another media server, the system displays a warning message. In an RGN High Availability solution, you must select the **Master Content Store** check box for the Avaya Aura® MS server that manages the prompts on both the campus and RGN site.
11. Click any other row in the grid to save your changes.
12. On the **Prompt Management**, connect to Avaya Aura® Media Server. The connection means that the Avaya Aura® Media Server is configured correctly, Contact Center Manager Administration is added as a trusted node and that a namespace matching the SIP domain name exists.
13. Repeat step 1 on page 131 to step 12 on page 131 for each media server to add. Take care to configure only one of the Avaya Aura® Media Servers as the Master Content Store.
14. From the **Transport** drop-down list, select the transport type for Avaya Aura® MS.

    Select either **TCP**, **UDP**, or **TLS**, if licensed.

15. Click **Update Transport**.

    This updates the transport type for all media servers.

Adding media servers to the required services

Before you begin

- Add the media servers to Contact Center Manager Server. See Adding media servers on page 131.

About this task

Each SIP-enabled contact center requires at least one Avaya Aura® Media Server to supply the ACC_APP_ID service.

Avaya Aura® Contact Center uses the media processing capabilities of Avaya Aura® Media Server. Configure each Avaya Aura® Media Server in a Contact Center as a Media Server. To configure an Avaya Aura® Media Server to provide conference, announcement or dialog sessions, assign the associated Media Server to provide ACC_APP_ID services.

To configure an Avaya Experience Portal system to provide external dialog services, assign the associated Media Server to provide XDIALOG services.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the **Launchpad**, click **Configuration**.
3. In the left pane, click the plus sign (+) next to the SIP-enabled Contact Center Manager Server.
4. From the list of configuration items for the Contact Center Manager Server, select **Media Services and Routes**.
5. Select **ACC_APP_ID**.
6. Select the media server.
7. Select the arrow key.
8. Click **Submit**.
9. Repeat step 6 on page 133 to step 9 on page 133 for each additional service required.
10. Once you add a ACC_APP_ID Media Services and Routes specification for a particular Media Server, and if you are using WebLM, you must restart Contact Center License Manager to ensure that Contact Center License Manager pushes the required license to the current Avaya Aura® Media Server.

Installing the Orchestration Designer client

About this task

Install the Orchestration Designer to manage Contact Center applications. Applications are used to route contacts based on certain criteria from the contact such as skillset or customer name.

Perform the following procedure to ensure that the version of the Orchestration Designer that you start from within the Contact Center Manager Administration application is current. You can also install the Orchestration Designer on any client to work with script or flow applications without affecting the Contact Center environment.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the **Launchpad**, click **Scripting**.
3. In the Scripting window, on the menu, click **Orchestration Designer**, and then click **Launch Orchestration Designer**.
4. On the message box requesting you to download a .msi file, click **OK**.
5. On the dialog box, click **Run**.
6. On the **Orchestration Designer- InstallShield Wizard**, click **Next**.
7. In the **User Name** box type a name.
8. In the **Organization** box type your company name.
9. Select one of the following options:
   - **Anyone who uses this computer (all users)**
   - **Only for me (User Name)**
10. Click **Next**.
11. Accept the default **Destination Folder**.

    OR

    Click **Change...** to select a different location.
12. Click **Next**.
13. Click **Install**.
14. Click **Finish**.

Procedure job aid

You can find more information about the Orchestration Designer in *Using Contact Center Orchestration Designer*.

Adding a Contact Center script or flow application

About this task

Add a Contact Center script or flow application to provide treatments for customer calls. Script applications use commands to define call treatments. Flow applications use graphical flow chart symbols to define call treatments.

Calls to the Contact Center are routed to a Master application for processing, treatments and queuing to an appropriate skillset. Avaya Aura® Contact Center answers the customer call and runs the Master application, and optional primary and secondary applications.

Applications contain instructions that determine the sequence of steps that a contact follows after the contact arrives at Contact Center. These steps can include call treatments (such as music or ringback), call routing (such as skill-based routing), or interaction with the caller (entering account numbers). Applications perform two major functions: they define the path a contact follows, and they provide treatments to a contact as the contact moves through Contact Center. You can also use the applications to track and record information about each step in the progress of a contact, and use this information to analyze how your contact center functions to improve service.

A primary application is an application run or referenced by the Master application. Contact Center Manager Server records Master application and primary application actions in statistical records. Statistics are not recorded for secondary applications.

Avaya recommends that you modify your application to check each call for useful data. If the call has useful data or intrinsics such as CLID (Calling Line Identification), use this data to queue the call to the most appropriate skillset. If the call does not have useful data, queue the call to the appropriate default skillset.

You can use Contact Center Orchestration Designer to edit the script or flow applications. Orchestration Designer is a graphical tool that you use to create applications.

Procedure

Use the Orchestration Designer application to add a script or flow application. For more information, see *Using Contact Center Orchestration Designer*.

Procedure job aid

You can use the Contact Center Orchestration Designer graphical tool to edit the Contact Center script or flow applications.

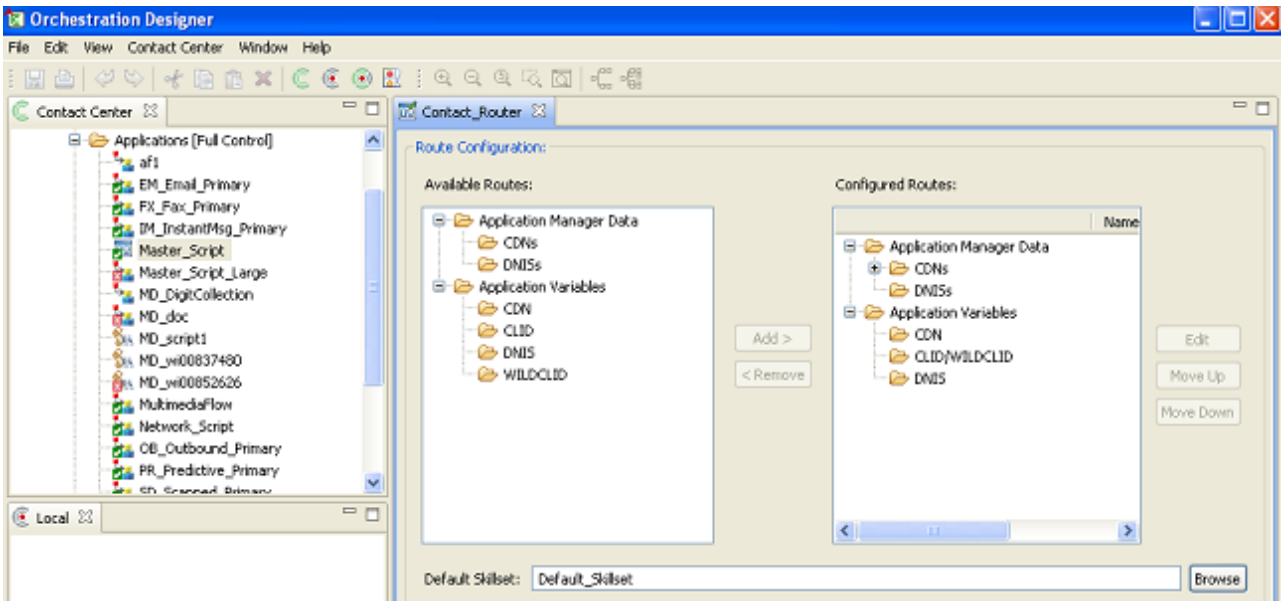


Figure 23: Example of using Orchestration Designer

Chapter 11: Contact Center Manager Server certificate commissioning

When you install Contact Center you can create a security store containing the certificates required to secure Web Services, AES communications, and the Agent Browser application. If you turn off Web Services security, you must still configure security certificates for AES communications, and, optionally, the Agent Browser application. If you configured Contact Center security already, skip the procedures in this chapter.

Avaya Aura® Contact Center uses industry-standard SIP and CSTA (TR/87 over SIP) interfaces to communicate with other telecoms and data systems, such as Application Enablement Services.

The SIP CTI link between Contact Center and Application Enablement Services (AES) uses the Transport Layer Security (TLS) protocol to provide secure communication. TLS uses signed security certificates to secure the link between the CCMS and the AES.

Security Manager maintains a security store to manage signed and root security certificates.

You must use signed security certificates to secure the link between Contact Center and AES. Until you configure Contact Center TLS certificates to communicate securely with Application Enablement Services, the SIP CTI link between Contact Center and AES is down.

Avaya recommends that you use a third party Certificate Authority or follow your organization's security policies and procedures to better secure the TLS link between Contact Center and the Application Enablement Services server. For improved security, Avaya recommends that you obtain a signed certificate and root certificate from a third-party Certificate Authority, or from your organization's Certificate Authority.

This section describes how to configure Contact Center TLS certificates to communicate securely with Application Enablement Services, and, optionally, the Agent Browser application, using a secure TLS connection.

Important:

In a SIP-enabled contact center using High Availability resiliency, the active and standby Contact Center servers must both have security certificates in place to communicate securely with the AES server and to support High Availability switchover.

For more information about configuring the Application Enablement Services end of the secure SIP CTI link, see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.

Creating a new security store

About this task

The Security Manager uses a store to hold Certificate Authority root certificates and signed certificates. Create the security store if you plan to use a Certificate Authority and generate signed certificates.

The default encryption setting is SHA2 with a key size of 2048. For backward compatibility, you can choose SHA1 or a key size 1024. However, neither SHA1 nor 1024 provide the industry-recommended level of encryption. If you select one of these values, Contact Center displays a warning message.

If you created a security store at install time using the Ignition Wizard, skip this procedure.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. In the **Security Manager** window, select the **Security Store** tab.
4. In the **Security Store** tab, in the **Full Computer Name (FQDN)** box, type the full FQDN of the server on which you are creating the security store.

   Important:

   The FQDN must be the full machine name of the server that the Security Store resides on. The FQDN name is case-sensitive.
5. In the **Name of Organizational unit** box, type the name of the department or division within the company.
6. In the **Name of Organization** box, type the company name.
7. In the **City or Locality** box, type the name of the city or district in which the contact center is located.
8. In the **State or Province** box, type the state or province in which the contact center is located.
9. In the **Two Letter Country Code** box, type the country code in which the contact center is located.
10. In the **Security Store password** box, type a password for accessing the new security store.
11. In the **Confirm Store password** box, confirm the password for accessing the new security store.

    Important:

    Ensure you remember this password, because you need it the next time you log on to Security Manager. If you forget the password, you are not able to access Security Manager.

12. If you want to change the encryption setting, select the required encryption settings from the **Encryption Algorithm** and **Key Size** drop-down lists.

    The default value for **Encryption Algorithm** is SHA2 and the default value for **Key Size** is 2048.

    Contact Center displays a warning message if you select SHA1 or 1024. Contact Center includes these values for backward-compatibility only, because these settings do not meet the industry-recommended level of encryption.

13. Click **Create Store**.

    Contact Center creates the private key required for private-public key encryption.

    Security Manager automatically displays the Certificate Request tab, showing the newly created Certificate Signing Request file contents.

    Contact Center automatically backs up the new security store to the folder `D:\Avaya\Contact Center\autoBackUpCertStore`. Do not overwrite or delete this backup location.

14. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Variable definitions

Name	Description
Full Computer Name (FQDN)	The host name and parent domain which fully qualifies the computer where the security store is to be created. The FQDN name is case sensitive. The Security Manager auto-populates the FQDN field by reading the name from the operating system. You can modify this field if required. Example FQDN format: computerX.DomainY.com
Name of Organizational unit	The department or division within a company.
Name of Organization	The company name.
City or Locality	The city or district in which the system is located.
State or Province	The state or province in which the system is located.
Two Letter Country Code	The country code in which the system is located.

Creating a security store with Subject Alternative Names

About this task

If you are implementing High Availability in the contact center, generate the security store using Subject Alternative Names (SANs). Include the Managed name and the current server name as SANs.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. In the **Security Manager** window, select the **Security Store** tab.
4. In the **Security Store** tab, in the **Full Computer Name (FQDN)** box, type the full FQDN of the server on which you are creating the security store.

   Important:

   The FQDN must be the full machine name of the server that the Security Store resides on. The FQDN name is case-sensitive.
5. In the **Name of Organizational unit** box, type the name of the department or division within the company.
6. In the **Name of Organization** box, type the company name.
7. In the **City or Locality** box, type the name of the city or district in which the contact center is located.
8. In the **State or Province** box, type the state or province in which the contact center is located.
9. In the **Two Letter Country Code** box, type the country code in which the contact center is located.
10. Under **Subject Alternative Name (SAN)**, for each SAN you want to add:
    a. From the **Type** drop-down list, select DNS.
    b. In the **Value** field, type the FQDN for the server.
    c. Click **Add SAN**.

    For a High Availability system, add the current server name and the Managed name for the HA pair.
11. On the Security Store tab, in the **Security Store password** box, type a password for accessing the new security store.
12. In the **Confirm Store password** box, confirm the password for accessing the new security store.

Important:

Ensure you remember this password, because you need it the next time you log on to Security Manager. If you forget the password, you are not able to access Security Manager.

13. If you want to change the encryption setting, select the required encryption settings from the **Encryption Algorithm** and **Key Size** drop-down lists.

    The default value for **Encryption Algorithm** is SHA2 and the default value for **Key Size** is 2048.

    Contact Center displays a warning message if you select SHA1 or 1024. Contact Center includes these values for backward-compatibility only, because these settings do not meet the industry-recommended level of encryption.

14. Click **Create Store**.

    Contact Center creates the private key required for private-public key encryption.

    Security Manager automatically displays the Certificate Request tab, showing the newly created Certificate Signing Request file contents.

    Contact Center automatically backs up the new security store to the folder `D:\Avaya\Contact Center\autoBackUpCertStore`. Do not overwrite or delete this backup location.

15. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Next steps

Send the Certificate Signing Request file to the Certificate Authority, and receive a signed certificate, so that you can import the signed certificate to the security store.

Copying the Certificate Signing Request file

Before you begin

- Speak with your System Administrator to identify a Certificate Authority.

About this task

Security Manager automatically generates a Certificate Signing Request (CSR) when it creates a new security store. The Security Manager—Certificate Request tab displays the name, location, and contents of the Certificate Signing Request (CSR) file on the server. A Certificate Authority uses this Certificate Signing Request (CSR) file to generate a signed security certificate. Contact Center uses the signed security certificate to establish secure communication links with Application Enablement Services (AES) servers, the Agent Browser application, and Web Services clients.

Until you add a signed certificate, the Signing Request Status field shows the CSR status as Pending. When the CSR is signed, and you add it to the security store using the “Add Certificate Tab”, the status changes to “Signed” to indicate that this CSR has been signed.

Procedure

1. Log on to the Contact Center server containing the security store.
2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. Select the **Certificate Request** tab.
4. Check the **Signing Request Status** value. If this value is **Pending**, you must have the CSR signed by a Certificate Authority.
5. Note the location of the Certificate Signing Request file from **File location**.
6. Select **Logout**.
7. Copy the Certificate Signing Request file from the directory referenced in **File location**, to send to a Certificate Authority.
8. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Next steps

After you perform this procedure, the certificate must be signed by a Certificate Authority. Contact your System Administrator for the preferred method of processing the signed certificate request file to obtain a signed certificate. Send the Certificate Signing Request file to a Certificate Authority and receive a signed certificate and root certificate to import to the security store.

Variable definitions

Name	Description
Security Store Status	Indicates if the Security Store is created.
Signing Request Status	Indicates if the generated Certificate Signing Request that appears is signed and added back into the store. Pending: Security Manager is waiting for a signed certificate to be added back into the store. Signed: Security Manager added the certificate signed by a specific Certificate Authority into the store.
File Location	Location of the Certificate Signing Request file.
Contents	Displays the contents of the Certificate Signing Request file. You can copy this directly from the field and have it signed.

Adding certificate files to the security store

Before you begin

- Use the CSR file from the Contact Center Security Manager to obtain a Certificate Authority signed certificate and root certificate.
- Save the certificate files on the Contact Center server.

About this task

Contact Center Security Manager can add both Certificate Authority root certificates and signed certificates to the security store. Contact Center requires a signed certificate and a corresponding Certificate Authority root certificate to communicate using secure services.

There are two options when adding CA root and signed certificates.

Automatically adding certificates :

You can select a folder that contains signed and root certificates. Security Manager accesses this folder and automatically determines which are signed certificates and which are root certificate and then adds them to the security store accordingly.

Important:

Security Manager attempts to import all files and certificates it finds in the certificate folder. Ensure that the certificate folder contains only Certificate Authority root certificates and signed certificates.

Manually adding certificates :

For manually added certificates, you can browse for individual signed and root CA certificates and add them to the security store, one at a time. Security Manager checks the certificates and does not add signed certificates as root CA certificates.

Procedure

1. Log on to the Contact Center server containing the security store.
2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. On the **Store Access** dialog, type the security store password.
4. Click **OK**.
5. In the Security Manager window, select the **Add Certificate** tab.
6. To add certificates automatically:
   a. Click **Browse**.
   b. On the Select Directory dialog, browse to the directory where you saved the certificate files, and click **Select Directory**.

      Security Manager displays the certificates in the **Certificates** field.
   c. Click **Add all Certificates**.

7. To add certificates manually:
   a. Select **Add Certificates Manually**.
   b. To manually add a Certificate Authority root certificate, click **Browse**.
   c. Browse to the Certificate Authority root certificate, and click **Select File**.
   d. Click **Add CA Certificate**.
   e. To manually add a signed certificate, click **Browse**.
   f. Browse to the Certificate Authority signed certificate, and click **Select File**.
   g. Click **Add Signed Certificate**.
8. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Variable definitions

Name	Description
Security Store password	Password to access the security store.
Add Certificates Automatically	Security Manager automatically determines which certificates are signed and which are root certificate and then adds them to the security store accordingly.
Select folder	The folder from which Security Manager automatically loads certificates.
Add Certificates Manually	Manually add certificates, one at a time.
Add Root Certificate	The name and location of the root certificate. Root Certificate Authority certificates must be in Base64 format.
Add Signed Certificate	The name and location of the signed certificate. Signed certificates must be in DER format.

Procedure job aid

The same root certificate must be applied to the Application Enablement Services so that Contact Center Manager Server (CCMS) can communicate securely with it using TLS. For more information about configuring Application Enablement Services certificates, see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.

Configuring the minimum TLS version

About this task

Configure minimum TLS versions that Contact Center can negotiate for secure connections. This enables third-party and legacy systems that do not support TLS 1.2 to communicate securely with

Contact Center. If you do not change these settings, Contact Center uses only TLS 1.2, and does not connect to systems that support only lower versions of TLS.

You can set minimum TLS versions separately for the following communications:

- SIP and CTI signaling
- CCMA and CCMM administration
- Event Broker Web service (this setting also sets the minimum TLS version used for Web Statistics)

Procedure

1. Log on to the server as a local administrator.

   Important:

   If you log on to the server as a domain administrator, this procedure does not complete successfully.

2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. On the Store Access dialog, type the password for the security store, and click **OK**.
4. On the Security Manager screen, select the **Security Configuration** tab.
5. In the **SIP and CTI Signaling Level** box, select the lowest version of TLS for SIP signaling communication.
6. In the **CCMA — Multimedia Web Service Level** box, select the lowest version of TLS for CCMA and Multimedia Web service communication.

   This changes the setting for IIS, and for Windows Server generally.
7. In the **Event Broker Web Service Level** box, select the lowest version of TLS for Event Broker Web Service communication.
8. In the **Current TLS Level for Cache Database** box, select the lowest version of TLS for Cache Database Level communication.
9. Click **Apply**.
10. Click **Log Out**.
11. Reboot the Contact Center server to complete the procedure.
12. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Exporting a root certificate from the security store

About this task

Export the certificate authority root certificate from the Contact Center security store so that clients using secured services can trust the public key for encryption. Avaya recommends that you

always export the root certificate from the security store, so that it is consistent with the current signed certificate.

Before you begin

- Add a signed certificate and root certificate to the security store.

Procedure

1. Log on to the Contact Center server containing the store.
2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. On the **Store Access** dialog, type the security store password, and click **OK**.
4. In the Security Manager window, select the **Store Maintenance** tab.
5. In the **Root Certificates** field, select the root certificate that you want to export.
6. Click **Export**.
7. On the Select Directory To Export To dialog, select or create a directory to which you want to export the root certificate.
8. Click **Export To**.

   Security Manager exports two files to the directory. The PEM file is for AES and Avaya Aura® MS; the Security Certificate file is for all other clients.
9. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Next steps

Apply the root certificate to all Contact Center clients.

Manually applying the root certificate to AES

About this task

For the Application Enablement Services server to communicate securely with Contact Center, the root certificate must be installed on both systems.

Follow this procedure to apply the root certificate to the AES server.

Before you begin

- Add a signed certificate and root certificate to the security store.
- Export the root certificate from the security store.

Procedure

1. In the left pane of the AES management console, click **Security**.
2. Click **Certificate Management** > **CA Trusted Certificates**> .
3. Click **Import**.

A Trusted Certificate Import page appears.

4. In the **Certificate Alias** box, type the certificate alias.
5. Click **Browse**, and select your root certificate.
6. Click **Apply**.

   A Certificate imported successfully message appears when the certificate is imported.
7. Click **Close**.

   The root certificate is added to the list of CA trusted certificates.
8. On the list of **CA Trusted Certificates**, locate your root certificate and confirm that the **Status** for it is **valid**.

Importing the Contact Center root certificate into Avaya Aura® MS

Before you begin

- Export the root certificate from the Contact Center Security Store, and save the PEM file to a location on the Avaya Aura® MS server.

About this task

Import the Contact Center root certificate into the Avaya Aura® MS trust store to support Transport Layer Security (TLS) communications. You perform this procedure on the Avaya Aura® MS server. If you have multiple Avaya Aura® MS servers, repeat this procedure on each server. Avaya Aura® MS supports importing only the PEM format root certificate file.

Procedure

1. Log on to Avaya Aura® MS Element Manager.
2. Navigate to **EM** > **Security** > **Certificate Management** > **Trust Store**.
3. Click **Import**.
4. In the **Trust friendly name** field, type a friendly name for the CA root certificate.
5. Click **Browse**.
6. Select the root certificate file that you exported from the Contact Center Security Store.
7. Click **Save**.
8. If you have multiple Avaya Aura® MS servers, repeat this procedure on each server.

Configuring SMTP server details

Before you begin

- Provision, configure, and maintain a Simple Mail Transport Protocol (SMTP) server. Contact Center Security Manager supports Microsoft Exchange Server.
- Know the authentication logon account and password details for the SMTP server.
- Ensure that the Contact Center server can access the SMTP server at all times.
- On the SMTP server, configure an email address for the contact center administrator. Security Manager sends the notification emails to this address. Ensure the contact center administrator monitors this email address.
- On the SMTP server, configure an email address for Avaya Aura® Contact Center Security Manager. Security Manager can then use this email address to send notification emails.

About this task

Configure the details of the SMTP server and accounts used to send the Security Manager status report email.

Procedure

1. On the **Security Manager** screen, select the **Expiration Alerts** tab.
2. Select **SMTP Configuration**.
3. From the **Outgoing e-mail server (SMTP)** list, select **IP** or **Address**. The Contact Center server must be able to communicate with the SMTP server by IP address or SMTP address.
4. In the **Outgoing e-mail server (SMTP)** box, enter the IP address or SMTP address of the SMTP server.
5. In the **Port number** box, enter the TCP port number for the SMTP server. The default port number is 25.
6. In the **Sender e-mail address** box, enter the email address to be used by Security Manager to send notification emails. Ensure this email address is registered with the SMTP server.
7. In the **Recipient e-mail address** box, enter the email address to which Security Manager is to send the notification emails. Ensure this email address is registered with the SMTP server. This is typically the contact center administrator’s email address. You must monitor this email address for notifications about the status of Contact Center security certificates.
8. If your SMTP server requires authentication, select **SMTP server requires authentication**. If your SMTP server does not require authentication, clear this check box.
9. In the **User name** box, enter the user account name used to authenticate with the SMTP server.
10. In the **Password** box, enter the password of the user account used to authenticate with the SMTP server.

11. Click **Save Configuration**.
12. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Scheduling a security store inspection task

Before you begin

- Configure the SMTP server and email account details.

About this task

Schedule a security store inspection task. Security Manager adds the scheduled task to the underlying Windows Task Scheduler. The scheduled task runs the security store inspection utility once a week. You can select the time and day of the week that the security store inspection task runs during the week.

Procedure

1. Log on to the Avaya Aura® Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. Select **Expiration Alerts** > **Schedule Alerts**.
4. From the **Day of week** list, select the day on which to schedule the weekly inspection task.
5. In the **Time (24 hr)** section, enter the time of day on which to schedule the weekly inspection task. Use twenty four hour format time.
6. In the **User** box, enter the name of a Windows user account that has the privileges necessary to access the Windows Task scheduler and schedule the task.
7. In the **Password** box, enter the password of the Windows user account that has the privileges necessary to access the Windows Task scheduler and schedule the task.
8. Click **Apply Schedule**.

   Security Manager then schedules this task on the underlying Microsoft Windows Task Scheduler. After successfully scheduling the task, the name on the **Apply Schedule** button changes to **Modify Schedule** and the button is disabled. To enable the **Modify Schedule** button, select a new time. You can then update the scheduled task time by clicking **Modify Schedule**.
9. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Verifying the scheduled security store inspection task

Before you begin

- Configure the scheduled task.

About this task

Verify that the Windows Task Scheduler lists the Security Manager scheduled inspection task. Do not modify the scheduled task in Task Scheduler. Use only Security Manager to modify the scheduled inspection task.

Procedure

1. Log on to the Contact Center server.
2. On the **Start** screen, under **Administrative Tools**, click **Task Scheduler**.
3. In the left pane, click **Task Scheduler Library**.
4. In the middle pane, confirm that there is a task named **aaccSentinel**.
5. Confirm that the task **Status** is **Ready**.
6. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Chapter 12: Avaya Aura® Media Server security and SRTP commissioning

Avaya Aura® Contact Center (AACC) supports implementing secure communications with Avaya Aura® Media Server using TLS . When installed, Avaya Aura® Media Server includes a default certificate that you can use for testing purposes. Do not use the default certificate in a production environment.

You can specify which Avaya Aura® Media Server services you want to secure, and use different server certificates to secure each service, if required. You can secure the following services:

- Application: in a Contact Center deployment, this affects the REST-based User Agent interface used by the Agent Greeting recorder application.
- Clustering: in a Contact Center deployment, this affects all communications between HA pairs or across Avaya Aura® Media Server clusters.
- Element Manager: this service provides the Element Manager web-based administration interface. Element Manager always enforces a TLS connection.
- OAM: in a Contact Center deployment, this SOAP-based Web service provides management of media content, such as prompts and music, from CCMA.
- Signaling: this service provides the Session Initiation Protocol (SIP) interface for call processing.

On a new deployment, all these services use the default server certificate. When you create a new certificate, assign it to all these services. Apart from Element Manager, all services accept both TLS and insecure TCP requests by default. Disabling the use of insecure TCP connections requires changing other configuration settings in Avaya Aura® Media Server Element Manager.

Important:

If you have a cluster, or one or more HA pairs in your Contact Center deployment, you must use the same Certificate Authority to sign the certificates of all the Avaya Aura® Media Servers.

Implementing Secure Real-Time Transport Protocol for Contact Center voice

Avaya Aura® Contact Center (AACC) supports implementing Secure Real-Time Transport Protocol (SRTP) for voice contacts within the contact center.

Secure Real-Time Transport Protocol (SRTP) is an extension to the Real-time Transport Protocol (RTP) to support secure real-time communications. The primary use of SRTP is to encrypt and authenticate voice over IP (VOIP) on the network.

Before implementing SRTP in Contact Center, you must have TLS connectivity enabled on the following links:

- Communication Manager to Session Manager
- Agent telephones to Communication Manager
- Session Manager to Contact Center
- Contact Center to Application Enablement Services
- Contact Center to Avaya Aura® Media Server SIP signaling services

To provide SRTP for routed Contact Center voice calls, you must configure SRTP on the following links:

- Agent telephones to Communication Manager
- Agent telephones to Avaya Aura® Media Server
- DMCC interface from Communication Manager to Avaya Contact Recorder (if used)

This chapter describes how to how to generate and apply your own security certificates and, optionally, to configure SRTP on Avaya Aura® Media Server. If you are enabling SRTP on Avaya Aura® Media Server, you must also configure SRTP on the Unified Communications platform. For more information on how to configure SRTP on your Unified Communications platform, see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.

Creating a new certificate signing request for Avaya Aura® Media Server

About this task

Create a Certificate Signing Request (CSR) file to send to a Certificate Authority (CA) to get a signed server certificate. You use the signed server certificate to secure services provided by Avaya Aura® MS. If you have multiple Avaya Aura® MS servers, repeat this procedure on each server.

Procedure

1. Log on to Avaya Aura® MS Element Manager.
2. Navigate to **EM** > **Security** > **Certificate Management** > **Key Store**.
3. In the **Key Certificates** section, click **Create New**.
4. On the Create New Certificate screen, in the **Signing authority** field, select **Other Certificate Authorities**.
5. In the **Certificate friendly name** field, type a name for this certificate.
6. In the **Key bit length** field, select **2048**.
7. In the **Signature algorithm** field, select **SHA-2/SHA-512**.
8. In the **Organization** field, type the company name.

9. In the **Organization unit** field, type the name of the department or division within the company.
10. In the **Common name** field, type the FQDN of the Avaya Aura® MS server.
11. In the **Country (ISO 3166)** box, type the country code in which the contact center is located.
12. In the **State / Province (full name)** box, type the state or province in which the contact center is located.
13. In the **City / Locality** box, type the name of the city or district in which the contact center is located.
14. If this Avaya Aura® MS server is part of a HA pair, select **Include Subject Alternative Name with FQDN**, and type the full FQDN for the managed name of the HA pair.
15. Click **Save**.
16. Select the location where you want to save the CSR file.
17. Click **Save**.

    Avaya Aura® MS displays the Key Store screen, with the new certificate listed in a Pending state.
18. If you have multiple Avaya Aura® MS servers, repeat this procedure on each server.

Next steps

After you perform this procedure, the certificate must be signed by a Certificate Authority. Contact your System Administrator for the preferred method of processing the CSR file to obtain a signed certificate. Send the CSR file to a Certificate Authority and receive a signed server certificate and root certificate to import to the Avaya Aura® MS key store.

If you use different CAs to sign the Avaya Aura® MS certificates and Contact Center certificates, copy the new Avaya Aura® MS root certificate to a folder on the Contact Center server.

Adding signed certificate files to the Avaya Aura® MS key store

About this task

Add the Certificate Authority (CA) root certificate and signed server certificate to the Avaya Aura® MS key store. Avaya Aura® MS requires a signed server certificate and a corresponding Certificate Authority root certificate to communicate using secure services.

Before you begin

- Use the CSR file that you created to obtain a CA signed server certificate and root certificate.
- Save the certificate files on the Contact Center server.

Procedure

1. Log on to Avaya Aura® MS Element Manager.
2. Navigate to **EM** > **Security** > **Certificate Management** > **Key Store**.
3. In the **Key Certificates** section, select the Pending certificate.
4. Click **Process Certificate Signing Request**.
5. On the Process Certificate Signing Request screen, click **Browse**.
6. On the Choose File to Upload dialog, browse to the location where you downloaded the certificate file from the CA, and select the file.
7. Click **Open**.
8. On the Process Certificate Signing Request screen, click **Process Signed Certificate**.
9. If you have multiple Avaya Aura® MS servers, repeat this procedure on each server.

Next steps

Specify the Avaya Aura® MS services that use the new server certificate, and export the CA root certificate to the clients that use those services.

Assigning the server certificate to an Avaya Aura® MS service profile

About this task

Assign the server certificate to one or more Avaya Aura® MS services, to use that server certificate to secure those services.

Before you begin

- Add the signed server certificate and corresponding root certificate to the Avaya Aura® MS key store.

Procedure

1. Log on to Avaya Aura® MS Element Manager.
2. Navigate to **EM** > **Security** > **Certificate Management** > **Key Store**.
3. On the Process Certificate Signing Request screen, in the **Service Profiles** section, click **Assign**.
4. On the Assign Certificate screen, select the new certificate for each service profile that you want to secure.
5. Click **Save**.
6. If you have multiple Avaya Aura® MS servers, repeat this procedure on each server.

Next steps

Export the CA root certificate from Avaya Aura® MS, and import it to the clients that use the secured services.

Creating a Certificate Signing Request with multiple Subject Alternative Names for Avaya Aura® Media Server

Before you begin

Use this procedure only if your contact center uses the High Availability (HA) feature.

About this task

Avaya Aura® MS with High Availability feature requires Certificate Signing Request (CSR) with multiple Subject Alternative Names (SAN).

You can not generate a CSR with multiple SANs on Avaya Aura® MS. For this purpose, you must use System Manager (SMGR). Use this procedure to generate a CSR with multiple SANs for Avaya Aura® MS with High Availability feature.

Procedure

1. Open **SMGR**.
2. In the **Services** tab, select **Security**.
3. Click **Certificates** and select **Authority**.
4. Under **RA Functions** section, select **Add End Entity**.

   The Add End Entity page displays.
5. On the **Add End Entity** page, in the **End Entity Profile** field, from the drop-down list, select `INBOUND_OUTBOUND_TLS`.
6. In the **Username** field, enter your user name.
7. In the **Password (or Enrollment Code)** field, enter your password.
8. In the **Confirm Password** field, confirm the password entered above.
9. Fill in the **CN, Common name** field as follows:
   - For non-HA solutions: enter the Avaya Aura® MS FQDN.
   - For HA solutions: enter the Avaya Aura® MS Managed FQDN.
10. In the **Other subject attributes** sections, under **Subject Alternative Name**, fill in the **DNS Name** field as follows:
    - For non-HA solutions: enter the Avaya Aura® MS Hostname.
    - For HA solutions: enter the Avaya Aura® MS Managed Hostname.
11. In the **IP Address** field, enter the IP addresses of the DNS names entered above.

12. Under **Main certificate data**, fill in the following fields:
    - **Certificate Profile**: From the drop down list, select `ID_CLIENT_SERVER`.
    - **CA**: From the drop down list, select `tmdefaultca`.
    - **Token**: From the drop down list, select `P12 file`.
13. (Optional) Fill in the other non-required fields if you need to.
14. Click **Add**.
15. Select **Public Web** and click **Create Browser Certificate** .
16. In the **Username** field, enter the user name you created above.
17. In the **Password** field, enter the password you created above.
18. In the **Key Length** field, select **2048 bits**.
19. Click **Enroll**.
20. Click **Download** to download the generated certificate.
21. If you have multiple Avaya Aura® MS servers, repeat this procedure on each server.

Adding signed certificates generated in SMGR to the Avaya Aura® MS key store

About this task

Use this procedure to import signed certificate files generated in SMGR to the Avaya Aura® MS key store.

Procedure

1. Log on to Avaya Aura® MS.
2. Navigate to **Home > Security > Certificate Management > Key Store**.
3. Select **Import**.
4. Enter the name of the certificate you want to import.
5. Enter the path to the certificate you want to import.
6. Click **Save**.

   The imported certificate appears in the **Key Certificates** list.

Assigning the server certificate generated in SMGR to an Avaya Aura® MS service profile

About this task

Assign the server certificate generated in SMGR to one or more Avaya Aura® MS services, to use that server certificate to secure those services.

Before you begin

Add the signed server certificate to the Avaya Aura® MS key store.

Procedure

1. Log on to Avaya Aura® MS.
2. Navigate to **Home > Security > Certificate Management > Key Store**.
3. On the Process Certificate Signing Request screen, in the **Service Profiles** section, click **Assign**.
4. On the Assign Certificate screen, select the new certificate for each service profile that you want to secure.
5. Click **Save**.
6. If you have multiple Avaya Aura® MS servers, repeat this procedure on each server.

Importing the Avaya Aura® MS root certificate into the Contact Center security store

About this task

Import the Avaya Aura® MS root certificate into Contact Center so that Contact Center can establish secure communications with Avaya Aura® MS. If you used the same Certificate Authority (CA) to sign both the Contact Center and the Avaya Aura® MS certificates, you can skip this procedure.

Before you begin

Copy the AAMS root certificate to a folder on the Contact Center server.

Procedure

1. Log on to the Contact Center server containing the security store.
2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. On the **Store Access** dialog, type the security store password.
4. Click **OK**.
5. In the Security Manager window, select the **Add Certificate** tab.

6. Select **Add Certificates Manually**.
7. Click **Browse**.
8. Browse to the AAMS root certificate, and click **Select File**.
9. Click **Add CA Certificate**.
10. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Verifying the TLS configuration on Avaya Aura® Media Server

About this task

Avaya Aura® Media Server has TLS configured by default. Follow this procedure to ensure that the TLS configuration is in place, in case previous configuration activities disabled it.

Procedure

1. Log on to the Avaya Aura® Media Server Element Manager. See Logging on to Element Manager on page 60.
2. In the navigation pane, expand **System Configuration** > **Signaling Protocols** > **SIP** > **General Settings**.
3. Ensure **Enable SIP TLS Mutual Authentication** is enabled.
4. Ensure **Enable SIP TLS in Secured Media Mode** is enabled.
5. If you needed to make changes, click **Save**.

Configuring SRTP on Avaya Aura® Media Server

About this task

Follow this procedure to enable SRTP on Avaya Aura® Media Server.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, expand **System Configuration** > **Media Processing** > **Media Security**.
3. Under **Security Policy**, select the security policy you want to use.
4. Under **Best Effort Mode**, select **CAPABILITY**.

5. Ensure you un-check **Enable SRTCP Encryption**, as Communication Manager does not support SRTCP Encryption.
6. Select **Enable SRTP Encryption**.
7. Select **Enable SRTP Authentication**.

Verifying the Media Server configuration in CCMA

About this task

The Media Server transport type global setting in CCMA must be set to TLS. When you set this, all configured Media Servers implement this transport type. The port number for each Media Server must be 5061.

Important:

This configuration affects Avaya Experience Portal (AAEP) servers configured on this screen, for example, AAEP servers used for back-end IVR in the contact center. Therefore you must enable TLS and SRTP on your AAEP server.

Procedure

1. Log on to CCMA with administrative privileges.
2. From the Launchpad, click **Configuration**.
3. In left pane, select the CCMS server for which you are configuring SRTP.
4. Click **Media Servers**.
5. From the **Transport** list, select **TLS**.
6. Click **Update Transport**.
7. Click **Yes** to confirm.
8. For each Media Server, ensure the **Port Number** value is set to 5061.
9. Restart the Contact Center server.

Chapter 13: Single sign-on commissioning

Perform the procedures in this chapter to commission single sign-on (SSO) for Contact Center Manager Administration.

Prerequisites for single sign-on commissioning

- Install or upgrade the Contact Center software.
- Install System Manager.
- Read *Avaya Aura® Contact Center Overview and Specification*.
- Ensure that you have administrator privileges on the Contact Center server.
- Ensure that you have administrator privileges on System Manager.

Single sign-on commissioning procedures

About this task

This task flow shows you the sequence of procedures you perform to commission single sign-on (SSO).

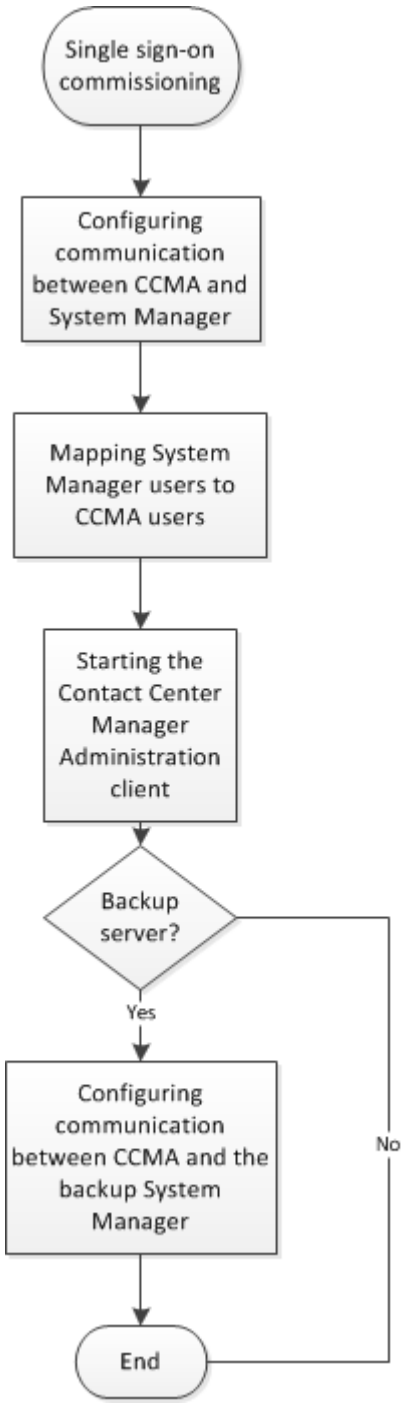


Figure 24: Single sign-on (SSO) commissioning procedures

Configuring communication between CCMA and System Manager

About this task

Configure communication between Contact Center Manager Administration and System Manager to ensure that the two applications work with each other.

Before you begin

- Commission CCMA. See Contact Center Manager Administration commissioning on page 100.
- Ensure that the System Manager server is a trusted site on the Contact Center server.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.
3. In the Configuration window, in the left pane, expand **Avaya** and **Applications**.
4. Select **Security Settings**.
5. In the **CCMA FQDN** field, type the Contact Center Manager Administration FQDN.
6. In the **Web Site Identifier** list, select **Default Web Site, 1**.
7. For **CCMA Server Protocol** select **https**.
8. For **IIS Port Number**, accept the default value.
9. In the **Security Server Details** section, in the **Security Server FQDN** field, type the System Manager FQDN.
10. In the **Security Server Port Number** field, type the security server port number.
11. In the **Cache Interval** field, type the number of local sessions for which information is cached on the server.
12. Click **Enable**.
13. When prompted, click **Yes**.
14. Click **OK** to accept the updates.
15. Click **Close**.

Variable definitions

Name	Description
Security Details	Select **Other server** to configure CCMA to use System Manager as the primary security server for SSO.

Table continues…

Name	Description
Security Server Details	The fully qualified domain name for the System Manager.
Cache Interval	The number of local sessions of information cached on the server.
Security Server Port Number	The port number used on the System Manager for communication with Contact Center Manager Administration. The default number is 8443.
CCMA Server Protocol	The protocol used to communicate between Contact Center Manager Administration and the internet. Select **https**: Contact Center deployments using SSO support only https.

Mapping System Manager users to CCMA users

About this task

Map all System Manager users to Contact Center Manager Administration users to ensure the single sign on feature is enabled for all applications.

When you create users in Contact Center Manager Administration, you can use this utility to map CCMA users to System Manager users.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.
3. In the Configuration window, in the left pane, expand **Avaya** > **Applications**.
4. Select **CCMA User Migration**.
5. In the right pane, click **CCMA User Migration**.
6. Under **Search Type**, select **Local Security Server** or **Domain**.
7. If you selected **Local Security Server**, enter the username and password of a local security server administrative user account.
8. Under **Search Options**, specify the details for the users you want to find.

   OR

   On the right side of the window, click **List All**.
9. Under the **Map User Accounts** list, select a configured System Manager account you want to map.

10. Under the **Unassigned CCMA Users** list, select a CCMA user that you want to map to the System Manager account.
11. Click **Map User**.
12. Click **Save**.
13. Click **Close**.

Variable definitions

Name	Description
Search Type	Search for users configured on the system. Local Security Server—find all accounts configured on the server. Domain—find all external users on a domain, such as an LDAP or database.
User ID	Available only if you select Local Security Server. Type the user name of a local security server user account that has administrative privileges.
Password	Available only if you select Local Security Server. Type the password of the local security server user.
Domain Details: Server IP (or DNS)	Available only if you select Domain. Type the IP address or domain name of a server from which to get the user names (For example, an LDAP or user database server.)
Domain Account: User ID	Available only if you select Domain. Type a the user name of a domain user with administrative privileges.
Domain Account: Password	Available only if you select Domain. Type the password for the domain user.

Starting the Contact Center Manager Administration client using a secure account

About this task

Start the CCMA client with the specific URL for single sign-on. To access CCMA and other Contact Center applications, use Microsoft Edge in Internet Explorer mode.

Before you begin

- Map the Contact Center Manager Administration user accounts to the System Manager accounts. See Mapping System Manager users to CCMA users on page 163.
- Ensure that the System Manager server is a trusted site.

Procedure

1. On the CCMA server, open your browser and type `https://FQDN:<security port>`.
2. Log in using a CCMA account that is mapped to a System Manager account.
3. If prompted, change the password for your user account.

Configuring communication between CCMA and the backup System Manager

About this task

Some deployments include a backup System Manager. If your deployment uses a backup System Manager, configure communication between Contact Center Manager Administration and the backup System Manager to ensure that the two applications work together.

Before you begin

- Commission the CCMA server. See Contact Center Manager Administration commissioning on page 100.
- Ensure that the backup System Manager server is a trusted site on the Contact Center server.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.
3. In the Configuration window, in the left pane, expand **Avaya** and **Applications**.
4. Select **Security Settings**.
5. In the **Resiliency Security Details** field, select **Failover Security Server**.
6. Click **Add**.
7. In the **Security Server Details** section, in the **Security Server FQDN** field, type the backup System Manager FQDN .
8. In the **Port Number** field, type the port number. The default is 8443.
9. Click **Add**.
10. Click **Enable**.
11. When prompted, click **Yes**.

12. Click **OK** to accept the updates.
13. Click **Close**.

Variable definitions

Name	Description
Security Details	Select **Other server** to configure CCMA to use the backup System Manager as the backup security server for SSO.
Security Server Details	The fully qualified domain name for the System Manager.
Cache Interval	The number of local sessions of information cached on the server.
Security Server Port Number	The port number used on the backup System Manager for communication with Contact Center Manager Administration. The default number is 8443.
CCMA Server Protocol	The protocol used to communicate between Contact Center Manager Administration and the internet. Select **https**: Contact Center deployments using SSO support only https.

Configuring Agent Greeting properties for SSO

About this task

Configure Agent Greeting properties for SSO to avoid errors in System Manager in the case of an HTTPS authentication request.

Note:

For SSO CCMA connectivity settings, you cannot configured a mapped CCMA to System Manager user from the configuration file in the Agent Greeting properties.

```
ccma.protocol=auto
ccma.address=127.0.0.1
ccma.username=AgentGreetingUser
ccma.password=uoWEh8X3PKifdqKw9LZHsg==
```

For more information about mapping users, see Mapping System Manager users to CCMA users on page 163.

Procedure

1. Create an SSO Agent Greeting user with a different name than *agentgreetinguser* in System Manager.

2. From the CCMA User Migration tool, map the newly created user with *agentgreetinguser*.
3. Add the new SSO Agent Greeting user ID and password to the Agent Greeting properties.

   To do this, use the following link: `https://<FQDN>:8445/ccag/settings/set/ccmacredentials/<SSO User ID>/<Mapped SSO User Password>`
4. In the Agent Greeting properties, manually replace the CCMA IP address with the CCMA FQDN.
5. To restart the Tomcat service, do the following:
   a. From the **Start** menu, navigate to **Administrative Tools** > **Services**.
   b. Right-click **Contact Center Tomcat Service** and then click **Restart**. It is recommended

Chapter 14: High Availability single sign-on commissioning

Perform the procedures in this chapter to commission the active Contact Center servers to communicate with the active, standby, and geographic System Managers.

High Availability single sign-on configuration

In order to deploy single sign-on (SSO) in a High Availability (HA) solution, you must install and configure a primary and standby System Manager. When configuring the Contact Center server on which single sign-on is deployed, you must use a Fully Qualified Domain Name (FQDN).

If you have a geographic HA contact center solution, you can also use an optional geographic System Manager on a remote site.

Prerequisites for High Availability single sign-on commissioning

- Install the active and standby Contact Center servers.
- Install the primary and standby System Managers.
- Optionally, install the geographic System Manager at a remote site.
- Read *Avaya Aura® Contact Center Overview and Specification*.
- Ensure that you have administrator privileges primary and standby Contact Center servers.
- Ensure that you have administrator privileges on the servers on the System Manager servers.
- Ensure the primary and backup System Manager servers can ping each other using their respective Fully Qualified Domain Names (FQDN).

High Availability single sign-on commissioning procedures

About this task

This task flow shows you the sequence of procedures you perform to commission single sign-on for High Availability.

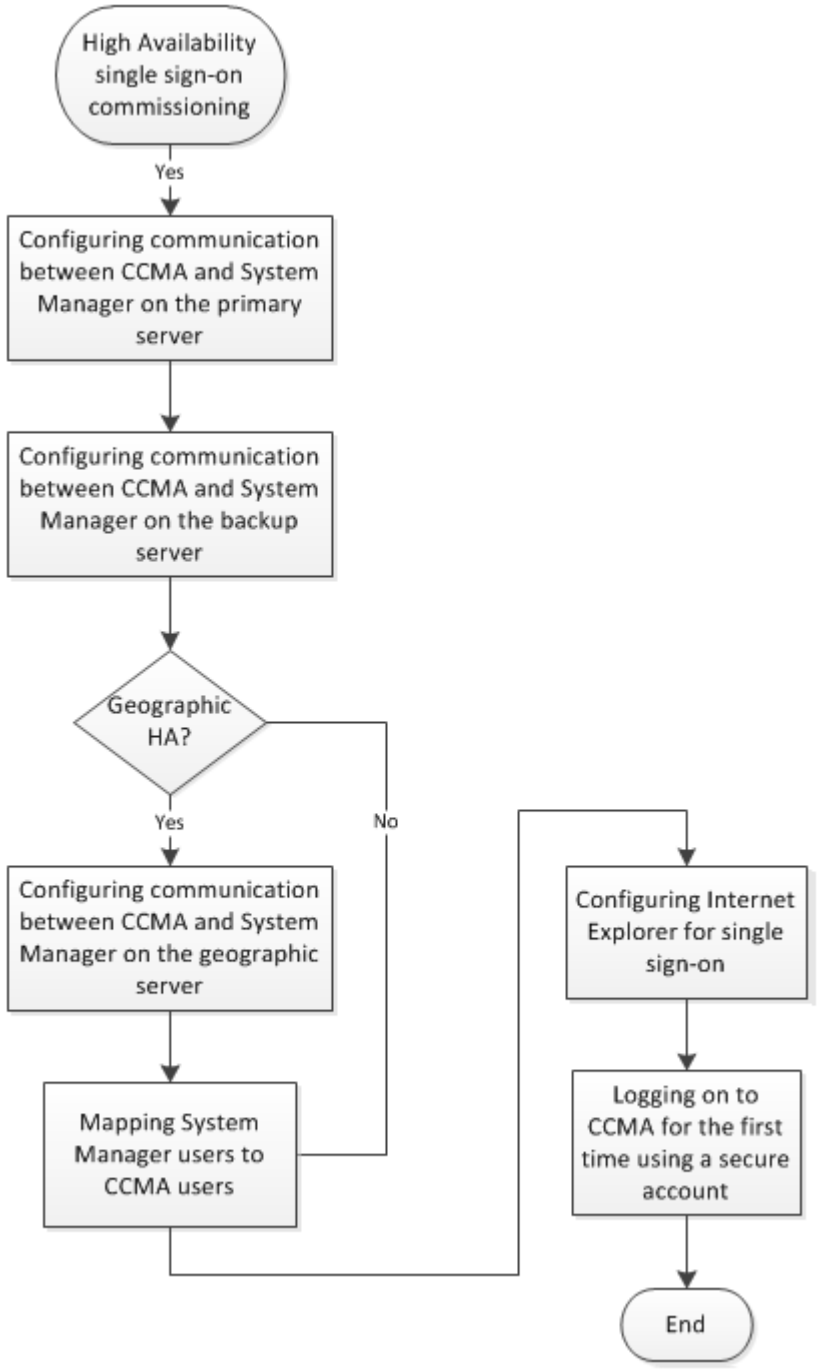


Figure 25: High Availability single sign-on commissioning procedures

Configuring communication between CCMA and System Manager on the primary Contact Center server

About this task

Configure communication between Contact Center Manager Administration and System Manager to ensure that the two applications work with each other.

Before you begin

- Commission Contact Center Manager Administration on the primary Contact Center server. See Contact Center Manager Administration commissioning on page 100.
- Configure your internet options to ensure that the System Manager servers are trusted sites on the Contact Center server.

Procedure

1. Log on to the primary Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.
3. In the left pane, expand **Avaya** > **Applications**.
4. Select **Security Settings**.
5. Select the **Is this a High Availability setup?** check box.
6. In the **Contact Center Manager Administration (CCMA) Details** section, in the **CCMA FQDN** field, type the managed FQDN of your CCMA server.
7. In the **Web Site Identifier** list, select **Default Web Site, 1**.
8. For **CCMA Server Protocol**, select **https**.

   Otherwise, the default setting is **http**.
9. For **IIS Port Number**, accept the default value.
10. In the **Primary – Security Server Details** section, in the **Security Server FQDN** field, type the FQDN of your primary System Manager.
11. In the **Security Server Port Number** field, type the System Manager server port number.
12. In the **Cache Interval** field, type a number, which represents the number of local sessions for which information is cached on the server.
13. In the **Resiliency – Security Server Details** section, select the **Failover Security Server** check box.
14. Click **Add**.

    The Add Failover Server Details window is displayed.
15. In the **Fully Qualified Domain Name (FQDN)** field, type the FQDN of the secondary System Manager.
16. In the **Port Number** field, type the System Manager server port number.

17. Click **Add**.
18. If you have a geographic High Availability solution:
    a. On the Security Details page, click **Add**.

       The Add Failover Server Details window is displayed.

    b. In the **Fully Qualified Domain Name (FQDN)** field, type the FQDN of the geographic System Manager server.
    c. In the **Port Number** box, type the port number of the geographic System Manager.
    d. Click **Add** and ensure that the backup System Manager is displayed first in the list.
19. Click **Enable**.
20. When prompted, click **Yes**.
21. Click **OK** to accept the updates.
22. Click **Close**.

Configuring communication between CCMA and System Manager on the standby Contact Center server

About this task

Configure the communication information between Contact Center Manager Administration and System Manager to ensure that the two applications work with each other.

Before you begin

- Commission Contact Center Manager Administration on the primary Contact Center server. See Contact Center Manager Administration commissioning on page 100.
- Configure your internet options to ensure that the System Manager servers are trusted sites on the Contact Center server.

Procedure

1. Log on to the standby Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.
3. In the left pane, expand **Avaya** > **Applications**.
4. Select **Security Settings**.
5. Select the **Is this a High Availability setup?** check box.
6. In the **Contact Center Manager Administration (CCMA) Details** section, in the **CCMA FQDN** field, type the managed FQDN of your CCMA server.
7. In the **Web Site Identifier** list, select **Default Web Site, 1**.

8. For **CCMA Server Protocol**, select **https**.

   Otherwise, the default setting is **http**.
9. For **IIS Port Number**, accept the default value.
10. In the **Primary – Security Server Details** section, in the **Security Server FQDN** field, type the FQDN of your primary System Manager.
11. In the **Security Server Port Number** field, type the System Manager server port number.
12. In the **Cache Interval** field, type a number, which represents the number of local sessions for which information is cached on the server.
13. In the **Resiliency – Security Server Details** section, select the **Failover Security Server** check box.
14. Click **Add**.

    The Add Failover Server Details window is displayed.
15. In the **Fully Qualified Domain Name (FQDN)** field, type the FQDN of the secondary System Manager.
16. In the **Port Number** field, type the System Manager server port number.
17. Click **Add**.
18. If you have a geographic High Availability solution:
    a. On the Security Details page, click **Add**.

       The Add Failover Server Details window is displayed.
    b. In the **Fully Qualified Domain Name (FQDN)** field, type the FQDN of the geographic System Manager server.
    c. In the **Port Number** box, type the port number of the geographic System Manager.
    d. Click **Add** and ensure that the backup System Manager is displayed first in the list.
19. Click **Enable**.
20. When prompted, click **Yes**.
21. Click **OK** to accept the updates.
22. Click **Close**.
23. When the Contact Center system switches from the standby server to the active server, do the following to reconfigure the Server Details settings:
    a. Select **Security Settings**.
    b. In the **Primary – Security Server Details** section, in the **Security Server FQDN** field, enter the FQDN of the failover System Manager that is displayed in the **Resiliency — Security Server Details** section.
    c. In the **Resiliency – Security Server Details** section, remove the server configuration.
    d. Clear the **Failover Security Server** check box.

e. Click **Save**.

Configuring communication between CCMA and System Manager on the geographic Contact Center server

About this task

Configure communication between Contact Center Manager Administration and System Manager to ensure that the two applications work with each other.

Before you begin

- Commission Contact Center Manager Administration on the geographic Contact Center server. See Contact Center Manager Administration commissioning on page 100.
- Configure your internet options to ensure that the System Manager servers are trusted sites on the geographic Contact Center server.

Procedure

1. Log on to the geographic Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.
3. In the left pane, expand **Avaya** > **Applications**.
4. Select **Security Settings**.
5. Select the **Is this a High Availability setup?** check box.
6. In the **Contact Center Manager Administration (CCMA) Details** section, in the **CCMA FQDN** field, type the managed FQDN of your CCMA server.
7. In the **Web Site Identifier** list, select **Default Web Site, 1**.
8. For **CCMA Server Protocol**, select **https**.

   Otherwise, the default setting is **http**.
9. For **IIS Port Number**, accept the default value.
10. In the **Primary – Security Server Details** section, in the **Security Server FQDN** field, type the FQDN of your primary System Manager.
11. In the **Security Server Port Number** field, type the System Manager server port number.
12. In the **Cache Interval** field, type a number, which represents the number of local sessions for which information is cached on the server.
13. In the **Resiliency – Security Server Details** section, select the **Failover Security Server** check box.
14. Click **Add**.

    The Add Failover Server Details window is displayed.

15. In the **Fully Qualified Domain Name (FQDN)** field, type the FQDN of the geographic System Manager.
16. In the **Port Number** field, type the port number of the geographic System Manager server.
17. Click **Add**.
18. If you have a geographic High Availability solution:
    a. On the Security Details page, click **Add**.

       The Add Failover Server Details window is displayed.

    b. In the **Fully Qualified Domain Name (FQDN)** field, type the FQDN of the secondary System Manager server.
    c. In the **Port Number** field, type the System Manager server port number.
    d. Click **Add** and ensure that the geographic System Manager is displayed first in the list.
19. Click **Enable**.
20. When prompted, click **Yes**.
21. Click **OK** to accept the updates.
22. Click **Close**.
23. When the Contact Center system switches from the Remote Geographic Node to the High Availability campus site, do the following to reconfigure the Server Details settings:
    a. In the Avaya Applications Configuration window, select **Security Settings**.
    b. In the **Primary – Security Server Details** section, in the **Security Server FQDN** field, enter the FQDN of the failover System Manager that is displayed in the **Resiliency — Security Server Details** section.
    c. In the **Resiliency – Security Server Details** section, remove the server configuration.
    d. Clear the **Failover Security Server** check box.
    e. Click **Save**.

Mapping System Manager users to CCMA users

About this task

Map all System Manager users to Contact Center Manager Administration users to ensure the single sign on feature is enabled for all applications. When you create users in Contact Center Manager Administration, you can use this utility to map CCMA users to System Manager users.

Procedure

1. Log on to the Contact Center server.

2. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.
3. Select **CCMA User Migration**.
4. In the right pane, click **CCMA User Migration**.
5. Under **Search Type**, select **Local Security Server** or **Domain**.
6. If you selected **Local Security Server**, enter the username and password of a local security server administrative user account.
7. Under **Search Options**, specify the details for the users you want to find.

   OR

   On the right side of the window, click **List All**.
8. Under the **Map User Accounts** list, select a configured System Manager account you want to map.
9. Under the **Unassigned CCMA Users** list, select a CCMA user that you want to map to the System Manager account.
10. Click **Map User**.
11. Click **Save**.
12. Click **Close**.

Configuring internet options for SSO

About this task

To access CCMA and other Contact Center applications, you must use the Microsoft Edge browser in Internet Explorer mode. Configure the internet options in your browser for SSO. Perform this configuration on each client in an HA deployment to access the SSO security server in System Manager.

Procedure

1. In Microsoft Edge, navigate to **More tools** > **Internet Options**.
2. Click the **Security** tab.
3. Click **Trusted Sites**.
4. Click **Custom Level**.

   The Security Settings window for trusted sites is displayed.
5. Under the **Miscellaneous** heading, select **Enable** for **Don’t prompt for client certificate selection when no certificates or only one certificate exists**.
6. Click **OK** and confirm if prompted.
7. On the Security tab, click the **Trusted Sites** icon again.

8. Click **Sites**.

   The Trusted sites window is displayed.
9. Clear the **Require server verification {https:} for all sites in this zone** check box.
10. In the **Add this website to the zone** field, type the server name (not the IP address) for your System Manager server.
11. Click **Add** and then click **Close** to return to the Internet Properties window.
12. Click the **Advanced** tab.
13. Under **Security**, clear the **Do not save encrypted pages to disk** check box.
14. Apply your changes.
15. Click **Close**.

Logging in to CCMA for the first time using a secure account

About this task

Start the CCMA client with the URL for single sign-on. Ensure that you are using Microsoft Edge in Internet Explorer mode.

Before you begin

- Map the Contact Center Manager Administration user accounts to the System Manager accounts. See Mapping System Manager users to CCMA users on page 175.
- Configure your internet options to ensure that the System Manager servers are trusted sites.

Procedure

1. Open your browser on the CCMA server and type `https://<FQDN>:<security port>`.

   The default security port is 8443.
2. Log in using an account mapped to System Manager.
3. If prompted, change the password for your user account.

Chapter 15: Contact Center Manager Administration client commissioning

After you install Contact Center Manager Administration server software, commission the client computers to access Contact Center applications. You must complete the procedures in this section in sequential order.

Prerequisites for client commissioning

- Install or update the Contact Center server software.
- Install or update the required client applications.
- To access Contact Center Manager Administration and other Contact Center applications, ensure that you are using Microsoft Edge in Internet Explorer mode.

Configuring the display settings

About this task

Configure the display settings on each client computer to ensure that Contact Center Manager Administration components, such as reports, are displayed correctly in the browser window.

Procedure

1. On the client computer, open **Control Panel**.
2. Click **System** > **Display**.
3. Navigate to the Scale and layout area.
4. Use the **Change the size of text, apps, and other items** drop-down list to set the font size.

   Ensure that **100%** is selected.
5. Set the display resolution to **1024 X 768**.

Important:

Avaya recommends this resolution to accommodate Real-Time Display billboard collections.

Configuring internet options on each client

About this task

Configure internet options on each client to access Contact Center Manager Administration. You must use Microsoft Edge in Internet Explorer mode.

Before you begin

If you are using SSO on your client, ensure that you add the System Manager server as a trusted site in your internet options.

Procedure

1. In Microsoft Edge, navigate to **More tools** > **Internet Options**.
2. Click the **Security** tab.
3. Click **Trusted Sites**.
4. Click **Custom Level**.

   The Security Settings window for trusted sites is displayed.
5. Under the **.NET Framework-reliant components** heading, select **Enable** for the following:
   - **Run components not signed with Authenticode**
   - **Run components signed with Authenticode**
6. Under the **ActiveX controls and plug-ins** heading, select **Enable** for the following:
   - **Automatic prompting for ActiveX controls**
   - **Run ActiveX Controls and plug-ins**
   - **Script ActiveX Controls marked safe for scripting**
7. Under the **Downloads** heading, select **Enable** for the following:
   - **Automatic prompting for file downloads**
   - **File download**
8. Under the **Miscellaneous** heading, select **Enable** for the following:
   - **Allow script-initiated windows without size or position constraints**
   - **Allow websites to open windows without address or status bars**
9. Click **OK** and confirm if prompted.

10. On the Security tab, click the **Trusted Sites** icon again.
11. Click **Sites**.

    The Trusted sites window is displayed.
12. Clear the **Require server verification {https:} for all sites in this zone** check box.
13. In the **Add this website to the zone** field, type the server name (not the IP address) or the FQDN for your Contact Center Manager Administration server.
14. Click **Add**.
15. In the **Add this website to the zone** field, type the server name (not the IP address) of your Contact Center Multimedia server.
16. Click **Add**.
17. If your contact center includes a Predictive Reporting server, in the **Add this website to the zone** field, type the server name (not the IP address) of your Predictive Reporting server.
18. Click **Add**.
19. Click **Close** to return to the Internet Properties window.
20. Click the **Privacy** tab.
21. Select the **Turn on Pop-up Blocker** check box.
22. Click **Settings**.

    The Pop-up Blocker Settings window is displayed.
23. In the **Address of website to allow** field, type the Contact Center Manager Administration URL.

    The default URL is `https://<server name>`, where *<server name>* is the name of the Contact Center Manager Administration server. If you turned off Web Services security, use `http://` instead of `https://`.
24. Click **Add**.
25. Click **Close** to return to the Internet Properties window.
26. Click the **Advanced** tab.
27. If HTTPS and TLS are enabled, under **Security**, clear the **Do not save encrypted pages to disk** check box.
28. Apply your changes.
29. Restart your browser to activate your changes.

Adding your browser to the firewall exceptions list

About this task

Add your web browser to the firewall exceptions list to ensure data can move between the clients and the server for reporting. To access Contact Center Manager Administration and other Contact Center applications, use Microsoft Edge in Internet Explorer mode.

Before you begin

Ensure that the Windows Firewall/Internet Connection Sharing (ICS) is running.

Procedure

1. On the client computer, open **Control Panel**.
2. Under Windows Defender Firewall, click **Allow an app through Windows Firewall**.
3. Click **Change settings** and then click **Allow another app**.
4. On the Add an app window, click **Browse** and navigate to the browser you want to add.
5. Click **Add** and then click **OK**.

Installing ActiveX controls

About this task

The ActiveX controls are rules that specify how applications share information using a web browser. In Contact Center, ActiveX controls enable communication between the clients and servers to report data and display information from the database.

Install the `ActiveX Controls.msi` file on each client as an administrator if your company security policy prevents agents from logging in to clients as an administrator. Controls downloaded using the `ActiveX Controls.msi` file are not displayed in your standard Downloads folder.

Before you begin

Configure internet options to enable, initialize, and script ActiveX Controls not marked as safe. See Configuring internet options on each client on page 179.

Procedure

1. Read the Contact Center Release Notes to obtain the location of the latest `ActiveX Controls.msi` file for your Contact Center release.
2. Log in to the client computer with administrator privileges.
3. Copy the `ActiveX Controls.msi` file to a location on the client computer.
4. Double-click the MSI file to begin the installation.
5. Click **Next**.
6. Select a destination folder or accept the default installation folder.

7. Click **Next**.
8. When prompted, click **Install**.
9. Click **Finish**.
10. Repeat steps 2 to 9 for each client.

Applying the ActiveX controls

About this task

Apply the `ActiveX Controls.msi` file you installed to the clients in your Contact Center to enable communication between the clients and servers in your network.

Procedures performed through an SMS system can vary from one company to the next, so this procedure offers general guidelines only. In addition to using an SMS server, a system administrator can install this package on clients within the same domain using the Windows Group Policy.

For details, see the documentation on the Microsoft website at www.microsoft.com.

Before you begin

- Install ActiveX controls.
- Ensure that you have administrator privileges to apply the `ActiveX Controls.msi` file to clients using an SMS server or the Windows Group Policy.
- Configure internet options to enable, initialize, and script ActiveX Controls not marked as safe.

Procedure

1. Read the Contact Center Release Notes to obtain the location of the latest `ActiveX Controls.msi` file for your Contact Center release.
2. Log in to the SMS server with administrator privileges.
3. Copy the `ActiveX Controls.msi` file to a location on the SMS server.
4. Double-click the MSI file to run the installation and install the files on all SMS client computers in your network.

Chapter 16: Communication Control Toolkit commissioning for SIP-enabled Contact Center

Use the procedures in this section to commission the Communication Control Toolkit (CCT) software in your SIP-enabled Contact Center. You must complete all the procedures in this section in sequential order.

Prerequisites to CCT commissioning for SIP-enabled Contact Center

- Read *Avaya Aura® Contact Center Overview and Specification*.
- Install the Contact Center software.
- Commission Contact Center Manager Server (CCMS) and Contact Center Manager Administration (CCMA).

Confirming that the CCT services start

About this task

Confirm that the Communication Control Toolkit services start so you can configure the Communication Control Toolkit database.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **System Control and Monitor Utility**.
3. Select the **CCT** tab.
4. Confirm that the Communication Control Toolkit services are running.
5. If a Communication Control Toolkit service is not running, re-start CCT.

6. Close the System Control and Monitor Utility.

Adding Communication Control Toolkit to CCMA

Before you begin

- Obtain a user ID and password with administrative privileges for the Contact Center Manager Administration (CCMA) client application. Only an administrator can add a server.
- Know the computer name of the server to add.
- To add Communication Control Toolkit (CCT), you must first have added Contact Center Manager Server (CCMS) with Open Queue enabled.
- Ensure you know the CCT Tomcat website port number. The default CCT Tomcat website port number is 8081.

About this task

Add CCT to CCMA then associate it to CCMS, to administer CCT from the CCMA client application.

Procedure

1. Log on to CCMA.
2. On the Launchpad, click **Configuration**.
3. From the **Server** menu, click **Add Server**.
4. In the right pane, in the **Server Name** box, type the computer name of the server.
5. Press **Tab**. The server IP address automatically appears in the IP Address box and the system automatically assigns a display name that is the same as the server name.
6. To use a different display name, in the **Display Name** box type the name of the CCT server as you want it to appear in the system tree in Contact Center Manager Administration.
7. From the **Type** list, select **CCT**.
8. In the **CCT Website: Port Number** box, type the port number of the Communication Control Toolkit server website.
9. From the **Associated CCMS Servers** list, select the Contact Center Manager Server with which to associate Communication Control Toolkit.
10. Click **Submit**.
11. In the left pane, expand the CCT name to access it.

Variable definitions

Name	Description
Associated CCMS Servers	For server types that you can associate with a Contact Center Manager Server, lists the available Contact Center Manager Servers. Select a Contact Center Manager Server with which to associate the CCT server.
CCT Website: Port Number	For the CCT server type, the default port number is 8081. Change this value if you change the port number on the Communication Control Toolkit server Tomcat configuration files.
CCT Website: URL	For the CCT server type, this box displays the URL for the Communication Control Toolkit server administration Web page. This is for information only.

Adding agents in CCMA for SIP-enabled Contact Centers

Before you begin

- Ensure that you have a domain user account for your Contact Center domain with privileges to list the domain users.
- You must have the appropriate access class to access and work in this window. If you cannot open part of the window that you need to work with, ask your administrator to update the access class assigned to you. To work with all sections of this window and add and edit all types of users, you need the Add/Edit/Delete Agents and Supervisors access level.
- Add CCT server to CCMA configuration, see Adding Communication Control Toolkit to CCMA on page 184.
- Log on to CCMA.
- Open the Contact Center Management component.

About this task

Create SIP agents using CCMA and associate them with contact center windows users.

Procedure

1. In the left pane, click the Contact Center Manager Server under which to add the agent.
2. From the **Add** menu, select **Agent**.
3. In the New Agent Details window, enter the following mandatory information about the agent:
   - First name
   - Last name

- Login ID
- Voice URI
- Create CCT Agent
- Primary supervisor

Note:

Login ID = 1 is reserved for the system use.

4. Enter any optional information about the agent (for example, Call Presentation Class, Threshold, Title, Department, or Comments).
5. If available, click **Create CCT Agent**, and complete the **Associate User Account** fields to create a CCT user for this agent.
6. If this agent uses the multiplicity feature on Avaya Agent Desktop, select a multiplicity presentation class from the **Multiplicity Presentation Class** list.

   If multiplicity is not enabled, the Multiplicity Presentation Class list does not appear.
7. If Agent Greeting is enabled, click the **Agent Greeting** heading and complete the fields for Agent Greeting.
8. If Offsite Agent is enabled on your system, click the **Offsite Agent** heading and complete the fields.
9. If Open Queue is enabled on the Contact Center Manager Server, click the **Contact Types** heading.

   If Open Queue is not enabled, the Contact Types section does not appear.
10. Select the check box beside each **Contact Type** to assign to the agent.
11. Click the **Skillsets** heading.
12. In the **Skillsets** area, click **List All** to list all skillsets configured on the server.

    If you do not see a skillset to which you need access, it might be because it is not included in your partition. Contact your administrator and request that the administrator add the skillset to the partition assigned to you.
13. From the **Priority** list for each skillset to assign to the agent, select the priority level or select **Standby** to put the agent in standby mode for this skillset.

    Priority levels range from 1 to 48, with 1 being the highest priority for the skillset.

    Important:

    With an Open Queue-enabled Contact Center Manager Server, you can only assign skillsets to an agent that belongs to the same contact type.
14. If you have administrator privileges, you can add this new agent to the partitions assigned to the agent's supervisor (instead of having to do so in Access and Partition Management). Click the **Partitions** heading.

    The list of partitions configured on the server appears.

15. Select the check boxes beside the partitions to which to add the new agent.
16. Click **Submit** to save your changes.

Variable definitions

Name	Description
First Name	The first name of the user. The first name is mandatory for all users and can be a maximum of 30 characters long.
Last Name	The last name of the user. The last name is mandatory for all users and can be a maximum of 30 characters long.
Title	The title for the user. The title is optional and can be up to 40 characters long.
Department	The user's department. The department is optional and can be up to 40 characters long.
Language	Select the language preference for the user. Language selection is mandatory for all users.
Comment	Comments you have about the user. Comments are optional and can be up to 127 ASCII characters in length. The 127 character limit can be lower if you use non-ASCII characters.
User Type	Select the user type. This value is mandatory. Select the agent user type. Agents are users who are assigned skillsets and who answer contacts in the Contact Center. All agents must be assigned to a supervisor.
Login ID	The number that the user enters to log on to the phone. This value is mandatory for all users.
Voice URI	The SIP address of the TR87-controlled terminal dedicated to this agent, in the format sip:agent. Use Extension@SM IP address. For example, sip:4400@47.166.115.99.
Enable CTI for this agent	Select if the agent has a CTI-enabled telephone. This field is mandatory on a SIP-enabled Contact Center.
Create CCT Agent	Select this box to display the Associate User Account fields. This field is mandatory on a SIP-enabled Contact Center.
Primary Supervisor	The agent's supervisor. You can choose from all supervisors configured on the server to which you are currently logged on.

Table continues…

Name	Description
Call Presentation	The call presentation class to assign to this agent. The call presentation class determines whether the agent can take a break between calls, whether the agent can put DN calls on hold for incoming Route Point calls, and whether the agent phone shows that the agent is reserved for a network call. Call Presentation is mandatory for all users with agent and supervisor/agent capability.
Multiplicity Presentation Class	The multiplicity presentation class to assign to this agent. The multiplicity presentation class determines the type and number of Multimedia contacts an agent can have open simultaneously on Avaya Agent Desktop. If multiplicity is not enabled, the Multiplicity Presentation Class list does not appear.
Agent Greeting Enabled	Select to enable Agent Greeting for the agent.
Agent Greeting Password	The password the agent uses to dial into the Agent Greeting recording application.
Agent Greeting Recorded	The system indicates that an agent greeting is recorded.
Communication Manager Agent ID	The Avaya Aura® Communication Manager ID for this Agent.
Communication Manager Server	The display name of the Avaya Aura® Communication Manager server for this Agent.
Threshold	The threshold class to assign to this user. The threshold class is mandatory for all users with agent and supervisor/agent capability.
Offsite Agent Enabled	Select to allow this agent to use Offsite Agent. Available only if the Contact Center is licensed for Offsite Agent.
Offsite Agent Mode	Select the mode in which this agent works when they log on to the Contact Center as an offsite agent.
Phone 1	The primary telephone number at which this agent receives calls from the Contact Center when working as an offsite agent. The phone number has a maximum of 15 digits.
Phone 2	The secondary telephone number at which this agent receives calls from the Contact Center when working as an offsite agent. The phone number has a maximum of 15 digits.

Table continues…

Name	Description
Allow agent to enter an alternate phone	Select to allow the agent to enter an alternate number to the numbers configured in Phone 1 or Phone 2. The agent can enter a different number when they log on to Agent Desktop as an offsite agent.
Search local operating system	Select if you want the user to be able to log on using accounts from the operating system on the local server (i.e., the CCMA server). Select this for a single-server install. Applies to supervisor/agents and agents.
Search domain users	Select to search for users from the Contact Center domain. Applies to all user types.
Domain Details - Server IP (or DNS)	If you selected Search domain users, enter the IP address of the domain controller from which you want to select the user account (mandatory).
Domain Details - Specify Domain Account	Select to allow you to specify a user account with which to search the domain as an authenticated domain user.
Domain Account	If you select Specify Domain Account, complete the following: • (Domain\User ID)–enter the domain user name to use to authenticate on the domain. This user must have the correct privileges to list domain users. **Note:** The domain name is case sensitive. • Password–enter the password for the user name you want to use to authenticate on the domain. • Base DN or Domain–enter the FQDN of the domain from which you want to select the user account (mandatory). • Use Secure Connection–select to search over a secure connection. Mandatory if the domain requires secure access. • Port Number–if the domain controller is not using the default port, enter the port number. If you selected Use Secure Connection, you must specify the secure port here (the default for domain controllers is 626).

Table continues…

Name	Description
Search all user accounts where:	Select the domain user field to search on. You can search on the user Last Name, First Name, Group Name, or User ID.
starts with	Enter a string with which you want to search user accounts. The search matches this string only against the start of the selected user account field.
and includes	Select from this list to refine your search to return: • all users–lists all users in the domain. • available users only–lists only the users in the domain that are not already associated with a supervisor or an agent.
Search	Click to search for users in the domain that match your search criteria. The Results grid appears and displays the domain users matching the search.
List All	List everything in the domain without applying search criteria.
Results	Display the users returned by your search. Click on a user to associate the account with this agent. You can associate only those users where the Status is Available.

Verifying CCT using Reference Client

About this task

Verify Communication Control Toolkit configuration by using the Reference Client to ensure that all resources are available and accessible to route contacts for CCMS. The Reference Client is an installation testing tool and is not to be deployed for production contact center use.

Procedure

1. Log on to the Contact Center server with the Local Administrator user ID and password.
2. From the **Start** menu, in the Avaya area, click **Contact Center Ref Client**.
3. In the **Server Settings** dialog box, click **OK**.
4. From the **Session** menu, choose **Connect As**.
5. In the **User Credentials** dialog box, enter the details of a user, enter a **User ID**, **Domain** and **Password**.
6. Click **OK**.
7. In the **Available Devices** box, select the address you want to use for the test call.
8. Enter the Destination Address in the text box to the right of the **Originate** button.

9. Click **Originate**. The destination address shows a Local State of Ringing in the Reference Client.
10. Select the Ringing Address on the Reference Client, and click **Answer**.
11. Release the call.

Chapter 17: Contact Center Multimedia commissioning

Commission the Contact Center Multimedia to manage multimedia contacts in your Avaya Aura® Contact Center. You must complete all the procedures in this section in sequential order.

Contact Center Multimedia server commissioning prerequisites

About this task

- Configure Open Queue as a feature in the Contact Center Manager Server installation.
- Configure Communication Control Toolkit on the Contact Center Manager Server configuration window.
- Commission Communication Control Toolkit.
- Apply the most recent service packs for Contact Center Multimedia. See *Upgrading and Patching Avaya Aura® Contact Center*.

Providing local users with the Log on as a service right

About this task

Provide local users with the log on as a service right to ensure that administrators and the agents in your Contact Center have access to the Agent Desktop application.

Procedure

1. Log on to the Contact Center server.
2. On the **Start** screen, click **Administrative Tools**.
3. Click **Local Security Policy**.
4. In the left pane, click **Local Policies**.
5. In the right pane, double-click **User Rights Assignment**.

6. In the right pane, double-click **Log on as a service**.
7. Click **Add User or Group**.
8. Click **Locations**.
9. In the **Locations** dialog box, select the Contact Center Multimedia server name from the list.
10. Click **OK**.
11. In the **Enter the object name to select** box, type **IUSR**.
12. Click **Check Names** to verify that the user name exists on the local computer.
13. Click **OK**.
14. Click **Apply** to save the changes.
15. Click **OK**.
16. Close the **Local Security Settings** window.

Variable definitions

Name	Description
IUSR	An Internet Information Services (IIS) account used for all communication between the Multimedia server and the Contact Center Agent Desktop over HTTP.

Verifying that Contact Center Multimedia services start

Before you begin

- Log on to the Contact Center Multimedia (CCMM) server.

About this task

Verify that Contact Center Multimedia services start to ensure that contacts are routed immediately after the server restarts for any reason.

Procedure

1. On the CCMM server, on the **Start** screen, click **Administrative Tools**.
2. Double-click **Services**.
3. Next to **CCMM License Service**, verify that the status is **Started** and the startup type is **Automatic**.
4. Next to **CCMM Starter Service**, verify that the status is **Started** and the startup type is **Automatic**.

5. Verify that the following services started:
   - CCMM Multimedia Contact Manager
   - CCMM OAM service
   - CCMM Campaign Scheduler service
   - CCMM Phonebook Service
6. If the contact center has licenses for email or outbound contacts, verify that the following services started:
   - CCMM Email Manager
   - CCMM Email Scheduler Service
   - CCMM POM Blending Service
   - CCMM POM Proxy Service
   - CCMM POM Reporting Service
7. If any service does not start, in the Services window, right-click the service name, and then click **Start**.

Adding the multimedia servers to Contact Center Manager Administration

Before you begin

- Obtain a user ID and password for the Contact Center Manager Administration client application.
- Know the computer name of the server to add.

About this task

Add the servers necessary to manage multimedia contacts to the Contact Center Manager Administration to provide reporting and connectivity support.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Log on to Contact Center Manager Administration.
3. On the Launchpad, click **Configuration**.
4. On the configuration menu, select **Server** > **Add Server**.
5. From the **Type** list, select CCMM.
6. In the **Server Name** box, type the computer name of the Multimedia server.
7. Press the Tab key.

   The server IP address automatically appears in the IP Address box.

8. In the **Display Name** box, type the name of the Multimedia server as you want it to appear in the system tree in Contact Center Manager Administration.

   Contact Center automatically assigns a display name that is the same as the server name. To enter a different display name, you must enter a unique name.

9. To add a Contact Center Multimedia server, in the **Login ID** box, type `mmReport`.

10. In the **Password** box, type `mmRep`.

    Important:

    You must change this password if the system sends a message that contains a logon request for validation.

11. Click **Submit**.

12. Click the plus symbol (+) beside the server name to access the server.

13. In the left pane, select the Contact Center Manager Server with which you want to associate the Contact Center Multimedia server.

14. Right-click the Contact Center Manager Server and then click **Edit Properties**.

15. Under **Associated Reporting Server**, select the check box next to the current active Contact Center Multimedia server name.

16. Click **Submit**.

Variable definitions

Name	Description
Login ID	For Contact Center Multimedia, the Login ID corresponds to the user in running historical reports in Contact Center Manager Administration. This user is configured in the Multimedia database and has access to data within that database. The Login ID is always mmReport.
Password	For Contact Center Multimedia, the default password is mmRep. To change this password, use the Contact Center Multimedia Administrator.

Logging in to the Multimedia Administration tool for the first time

About this task

Log in to the Contact Center Manager Administration tool to configure the Contact Center. You need a user ID and password for the Contact Center Manager Administration client application. Ensure that you are using Microsoft Edge in Internet Explorer mode.

Procedure

1. Log in to the Contact Center server.
2. In Microsoft Edge, navigate to **More tools** > **Internet Options**.
3. Click the **Security** tab.
4. Click **Trusted sites** and then click **Sites**.
5. Under **Add this website to the zone**, type the name of the Contact Center Multimedia (CCMM) server.
6. Click **Add**.
7. Click **Close**.
8. Click **OK**.
9. Log in to the Contact Center Manager Administration client with administrative privileges.
10. From the Launchpad, click **Multimedia**.
11. In the left pane, select the Contact Center Multimedia server to which you want to log in.
12. Select **Install Prerequisite Software** and click **Launch Multimedia Client** to run CCMA.

Configuring server settings

Before you begin

- Ensure that you understand for which contact types your Contact Center is licensed.
- Install the required software on your Web server and email servers (if applicable).

About this task

Configure the Contact Center application servers, Web communications, and email servers to ensure that you can connect the Contact Center Multimedia server to the external servers for handling email, voice mail, fax, scanned documents, and Web communications contacts.

Certain server types appear by default because the install required the details for these servers. Additionally you can add the following server types:

- CallPilot Server

- Communication Manager Server
- Communication Manager Standby Server
- Geographic Standby CCT Server
- Inbound POP3 or IMAP Server
- Outbound SMTP Server
- Secondary Predictive Application Server
- TSP Dialer

Important:

- Contact Center Multimedia supports only adding a maximum of five POP3 or IMAP servers as inbound email servers and five SMTP servers as outbound email servers. You can have a mix of email servers that have POP3 or IMAP protocols for receiving email messages and SMTP protocol for sending email messages with a mix of TLS, STARTTLS, and no security channels.
- If you are using SSO to access Contact Center Manager Administration, you must ensure that the entry for the CCMA server **Hostname** uses the FQDN.

Procedure

1. Log on to Contact Center Manager Administration with administrator privileges.
2. On the Launchpad, click **Multimedia**.
3. In the left pane, select the server to which you want to log on.
4. Click **Launch Multimedia Client**.
5. In the left column, select **General Administration**.
6. Click **Server Settings**.
7. Select the server to update, and click **Edit**.
8. In **Edit Server**, type the details for the server.
9. Click **Save**.

Variable definitions

Name	Description
Server Name	The host name of the server.
Server Port	The communications port number for the server.
Server Type	Choose the server type, for example; CCT, CCMS, License Manager, or Standby CCT.
Backup Server	The standby license server name.
MCMC Event Port	The Multimedia Contact Management Client port number.

Table continues…

Name	Description
Primary Hostname	The host name of the primary email server. Required for Outbound SMTP and Inbound POP3 or IMAP server types.
Port Number	The server port that CCMM uses to communicate with the server. Required for Outbound SMTP, Inbound POP3 or IMAP, Secondary Predictive Application, and Geographic Standby CCT server types.
Secondary Hostname	The host name of the optional secondary email server. Available for Outbound SMTP and Inbound POP3 or IMAP server types.
SMTP Authentication	Enable or disable SMTP Authentication. Required for Outbound SMTP Server.
Username	The LDAP Server access account name. Required for Directory LDAP and Phonebook LDAP server types.
Password	The LDAP Server access account password.Required for Directory LDAP and Phonebook LDAP server types.
Search base	The LDAP base search string. Required for Directory LDAP and Phonebook LDAP server types.
Polling Interval (hrs)	The LDAP polling interval. Required for Directory LDAP and Phonebook LDAP server types.

Configuring an LDAP server for Agent Desktop voice contacts

Before you begin

Ensure that the LDAP server that you use for voice contacts is commissioned and operational.

Important:

- To retrieve contacts from the LDAP server, ensure that the **Enable Address Book Retrieval** check box is selected.
- If you are using TLS, import a valid certificate for the LDAP server to keystore using the keytool command.

About this task

Configuring a Lightweight Directory Access Protocol (LDAP) server provides agents using Agent Desktop with a list of contacts during a voice call.

Important:

Avaya Agent Desktop Phonebook (`PhonebookLDAPData.zip`) displays voice contacts only if contacts have a telephone number associated with their profiles in Active Directory.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Open the Contact Center Manager Administration application.
3. Type your user ID and password.
4. On the **Launchpad**, click **Multimedia**.
5. In the left pane, select the server to which you want to log on.
6. Click **Launch Multimedia Client**.
7. In the left column, select **General Administration**.
8. Click **Server Settings**.
9. Click **New**.
10. In the **Server Type** list, select the **Phonebook LDAP Server** option.
11. In the **User** field, type the user name for the administrator on the Phonebook LDAP server in the format domain name\user name.
12. In the **Password** field, type the password for the administrator on the Phonebook LDAP server.
13. In the **Polling Interval** box, type the polling interval, in hours, for the interval between polls for the email server lookup.
14. In the **Search Base** field, specify the precision of the Phonebook LDAP search.

    For example, in a large enterprise of tens of thousand of people, it is not advisable to search for all users. In such a case, use a more restrictive search base, such as search for names in the local workgroup.
15. Click **Edit Server** to change the properties of the Phonebook LDAP server.
16. In the **Server Name** box, type the server name.
17. In the **Server Port** box, type the port number for the server.
18. Select **Use TLS** if you want Agent Desktop to communicate securely with the Phonebook LDAP server. The server specified must support TLS.
19. Click **Save**.
20. Click **Test** to test the user name, password, and search base, by connecting to the configured server to retrieve contacts.
21. Click **Save**.

Configuring email recipient addresses

Before you begin

- Ensure that you understand for which contact types your Contact Center is licensed.

About this task

Configure the recipients in your contact center to handle email, voice mail, fax, scanned documents, and SMS contacts. Each type of contact is scanned and attached to an email that is received by the contact center and routed. You must configure the recipient mailboxes to ensure the contacts are routed.

Note:

This procedure does not apply to voice-only solutions.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Open the Contact Center Manager Administration application.
3. Type your user ID and password.
4. On the **Launchpad**, click **Multimedia**.
5. In the left pane, select the server to which you want to log on.
6. Click **Launch Multimedia Client**.

   The system opens the CCMM Administration application.
7. In the left column, select **E-mail**.
8. Click **Recipient Addresses**.
9. Click **New**.
10. From the **Mailbox Type** list, select **Mail Store** or **Alias**.
11. Enter the mailbox details.
12. Click **Save**.

Variable definitions

Name	Description
Display name	The name to appear in the Email From address.
E-mail Domain	The domain for your email server.

Table continues…

Name	Description
Mail Store or Alias	Select the Mail Store or Alias option. • Select Mail Store to include the email mailbox in the set of mailboxes from which incoming email is retrieved. • Select Alias to configure this mailbox as an alias. The address of an alias can be used in rules configuration and outbox mapping, but a recipient box configured as an alias address not contain email.
Mailbox Name	The name of the mailbox that receives incoming email to the Contact Center. If the Contact Center Multimedia server is not in the same domain as the email server, you must also include the domain. Include the domain in the format domain\user (Windows 2000) or user@domain (post- Windows 2000) in the Mailbox Name box. Example: To enter the email address `sales@avaya.com`, in the Mailbox Name box, type sales, and in the E-mail Domain box, type avaya.com. Example: To enter the email address `sales@europe.avaya.com`, in the Mailbox Name box, type europe\sales or `sales@europe.avaya.com`, and in the E-mail Domain box, type europe.avaya.com.
Inbound (POP3 or IMAP) Server	The name of the email server, either POP3 or IMAP, that handles email messages coming into the Contact Center.
Inbound Mail Threshold	The maximum number of email messages the mailbox can accept every time it scans the database. You can enter a different value for this variable for each mailbox. The default value is 10.
Rule Group	The name of the rule group that applies to this recipient mailbox.
Outbound (SMTP) Server	The name of the mail server that handles email messages leaving the Contact Center.
Use alternative user name for SMTP Authentication	Select this box if you are configure an inbox as an alias. If SMTP authentication is enabled on your email Server, and you use aliases, you log on to the SMTP server with a different user name.

Table continues…

Name	Description
Username	The logon name for the SMTP server. You can have mailboxes on multiple email servers. You can have multiple email servers for email or fax messages, load balancing, and managing email subtypes. Each email server is polled for the mailboxes that it hosts. Configure additional email servers using the Server Configuration window. For instructions about configuring additional email servers, see *Avaya Aura® Contact Center Server Administration*.

Configuring email attachment file locations

About this task

Configure the locations for inbound and outbound email attachments.

Note:

This procedure does not apply to voice-only solutions.

Before you begin

- Avaya recommends that you enforce a limit on the incoming attachment size on your email servers, based on your business requirements. This helps prevent the use of storage on the CCMM server by SPAM email messages with large attachments.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Open the Contact Center Manager Administration application.
3. Type your user ID and password.
4. On the **Launchpad**, click **Multimedia**.
5. In the left pane, select the server to which you want to log on.
6. Click **Launch Multimedia Client**.

   The system opens the CCMM Administration application.
7. In the left column, select **E-mail**.
8. Click **General Settings**.
9. Under **Attachment Files**, in the **Inbound URL** box, type the URL for files attached to inbound email messages.
10. Under **Attachment Files**, in the **Inbound Share** box, type the share location for files attached to inbound email messages.

11. Under **Attachment Files**, in the **Outbound URL** box, type the URL for files attached to outbound email messages.
12. Under **Attachment Files**, in the **Outbound Share** box, type the share location for files attached to outbound email messages.
13. Click **Save**.

Variable definitions

Name	Description
Inbound URL	The URL for files attached to inbound email messages. For contact centers using the Avaya Aura® Contact Center High Availability feature, Avaya recommends using: http://<managedIPAddress>/InboundAttachment Where managedIPAddress is the managed IP address of the CCMM server.
Inbound Share	The share location for files attached to inbound email messages. Avaya recommends using: <driveLetter>:\Avaya\Contact Center\Email Attachments\Inbound
Outbound URL	The URL for files attached to outbound email messages. For contact centers using the Avaya Aura® Contact Center High Availability feature, Avaya recommends using: http://<managedIPAddress>/OutboundAttachment Where managedIPAddress is the managed IP address of the CCMM server.
Outbound Share	The share location for files attached to outbound email messages. Avaya recommends using: <driveLetter>:\Avaya\Contact Center\Email Attachments\Outbound

Configuring the multimedia skillsets

Before you begin

- Ensure that you understand for which contact types your Contact Center is licensed.
- Configure the route points in Contact Center Manager Administration that you plan to use for the multimedia skillsets.

About this task

Configure multimedia skillsets to ensure that you can route multimedia contacts in your contact center. Multimedia contacts include email, fax, scanned documents, SMS text messages, voice mail, Web communications, and outbound contacts. Instant messages are manually scripted in Orchestration Designer. For more information about instant messaging configuration, see Creating an Orchestration Designer application to route from an IM route point to an IM skillset on page 205.

You must configure a route point for each default skillset, and add any other skillset you intend to use for routing contacts.

Note:

This procedure does not apply to voice-only solutions.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Open the Contact Center Manager Administration application.
3. Type your user ID and password.
4. On the **Launchpad**, click **Multimedia**.
5. In the left pane, select the server to which you want to log on.
6. Click **Launch Multimedia Client**.

   The system opens the CCMM Administration application.
7. In the left column, select **General Administration**.
8. Click **Skillset Settings**.
9. Select the skillset to update.

   Important:

   You must configure at least one skillset for each type of contact for which your contact center is licensed. You must configure the default skillset.
10. In the **Route Point** box, select a Route Point for the skillset.
11. Repeat step 7 on page 204 and step 8 on page 204 for each default skillset.

Variable definitions

Name	Description
Route Point	An equivalent routing number for a non voice contact. You must configure Route points in Contact Center Manager Administration.

Table continues…

Name	Description
Skillsets	You must configure at least one skillset for each contact type for which you are licensed. • Email skillsets have the prefix EM_. You can also configure an optional automatic response for an email skillset that is used to respond immediately to an email message from a customer. • Outbound skillsets have the prefix OB_. • Predictive Outbound skillsets have the prefix PO_. • Web Communication skillsets have the prefix WC_. • Social Networking skillsets have the prefix SN_. • SMS text message skillsets have the prefix SM_. • Instant Message skillsets have the prefix IM_. • Voice mail skillsets have the prefix VM_. • Fax skillsets have the prefix FX_. • Scanned document skillsets have the prefix SD_.

Creating an Orchestration Designer application to route from an IM route point to an IM skillset

Before you begin

- You are familiar with creating and editing flows in Orchestration Designer. See *Using Contact Center Orchestration Designer*.
- You have access to an Orchestration Designer client and privileges to create flows for this contact center.

About this task

Create an application in Orchestration Designer to route IM contacts from the IM route point to an IM skillset.

Procedure

1. In Orchestration Designer, create a new flow to route IM contacts.
2. Edit the flow elements to route IM contacts received on the IM route point to an IM skillset.

Configuring the MIME types

Before you begin

- Install Contact Center Multimedia server software.
- Log on to the Contact Center Multimedia server.

About this task

Configure the Multipurpose Internet Mail Extension (MIME) types to ensure that agents can access email message attachments.

In Agent Desktop, agents can access only attachments with extensions listed in the Internet Information Services (IIS) MIME Types. The extensions listed in this procedure are the minimum required for email messages accessed in Agent Desktop. If agents in your contact center need access to files with extensions not listed in the IIS MIME Types, add those additional types.

Procedure

1. On the **Start** screen, click **Administrative Tools**.
2. Double-click **Computer Management**.
3. In the Computer Management dialog box, expand **Services and Applications** > **Internet Information Services** > **Sites**.
4. Select **Default Web Site**.
5. Under **IIS**, select **MIME Types**.
6. Double-click **MIME Types**.
7. On the **Actions** list on the right, click **Add**.
8. In the **File name extension** box, type `.dic`.
9. In the **MIME Type** box, type `application/octet-stream`.
10. Click **OK**.
11. On the **Actions** list on the right, click **Add**.
12. In the **File name extension** box, type `.eml`.
13. In the **MIME Type** box, type `application/octet-stream`.
14. Click **OK**.
15. On the **Actions** list on the right, click **Add**.
16. In the **File name extension** box, type `.dat`.
17. In the **MIME Type** box, type `application/octet-stream`.
18. Click **OK**.
19. On the **Actions** list on the right, click **Add**.
20. In the **File name extension** box, type `.msg`.

21. In the **MIME Type** box, type `application/octet-stream`.
22. Click **OK**.
23. Close the Computer Management window.

Variable definitions

Name	Description
Extension	The minimum Multipurpose Internet Mail Extension (MIME) types required by Agent Desktop are: • .dic • .eml • .dat • .msg If agents in your contact center need access to files with extensions not listed in the IIS MIME Types, add those additional extensions.
MIME Type	The Multipurpose Internet Mail Extension (MIME) information required by Agent Desktop: application/octet-stream.

Configuring the client OS setting for Citrix deployments

About this task

Configure Contact Center Multimedia to support Agent Desktop in Citrix deployments. If your contact center solution does not use Citrix, skip this procedure.

Procedure

1. Log on to Contact Center Manager Administration with administrator privileges.
2. On the Launchpad, click **Multimedia**.
3. In the left pane, select the server to which you want to log on.
4. Click **Launch Multimedia Client**.
5. In the left column, select **Agent Desktop Configuration**.
6. Click **Common Settings**.
7. Select **Suppress OS not supported popup**.
8. Click **Save**.

Adding an email address of an administrator in CCMM Dashboard

Before you begin

- Ensure that the Extended Email Capacity feature is disabled in Contact Center.

About this task

Add an email address of an administrator so that the administrator receives notifications when the number of email messages in the queue is approaching the threshold. If the number of email messages that have the New status is more than 10 000 in a standalone CCMM configuration and 4 000 in a co-resident configuration, Email Manager sends an email to the administrator to enable the Extended Email Capacity feature.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Multimedia Dashboard**.
3. In the **Administrator e-mail address (for notifications)** field, type the email address of the administrator to whom you want Email Manager to send notification messages.
4. Click **Save**.

Chapter 18: Avaya Aura® Media Server Zoning commissioning

Avaya Aura® Media Server (Avaya Aura® MS) Zoning allows contact center administrators to target a specific Avaya Aura® MS instance or prioritized list of instances when anchoring incoming contact center calls. Avaya Aura® MS Zoning sees the introduction of a new ATTACH TO MEDIA SERVER command and Flow Editor Template block named Media Server in Avaya Orchestration Designer (OD). The new command allows administrators to select a list of Avaya Aura® MS instances to be used to anchor incoming calls for a particular zone. This command, with the exception of general logic blocks, must be the first command in your flow application. This is because Avaya Aura® MS cannot play treatments to the customer until a call is anchored.

If Avaya Aura® MS Zoning is enabled on your AACC server but the ATTACH TO MEDIA SERVER command or Media Server template block is not used in your scripted or flow applications, AACC anchors calls on Avaya Aura® MS using the existing round-robin algorithm. If the ATTACH TO MEDIA SERVER command or Media Server template block is present in the scripted or flow application but is placed after some other treatment command, or if Avaya Aura® MS Zoning is disabled, the command is ignored.

The ATTACH TO MEDIA SERVER command and Media Server template block requires a single string parameter containing a comma-separated list of your Avaya Aura® MS names. This list can contain up to five Avaya Aura® MS servers that are used to anchor calls for that zone. You can configure the list of Avaya Aura® MS names to be used to anchor customer calls using the List Builder tool. This allows you to add any of the Avaya Aura® MS instances from the Media Servers list to the List Builder. Alternatively, you can use the mediaservice string variable in OD with the list of Avaya Aura® MS instances populated as values. Regardless of the method you use to configure the list of Avaya Aura® MS instances, the list is priority ordered. The name that appears first in the list is the Avaya Aura® MS that the ATTACH TO MEDIA SERVER script command identifies as the preferred media server to anchor calls on.

Important:

If you use the mediaservice string variable to list the Avaya Aura® MS instances, you must ensure the string variable values are configured with the Avaya Aura® MS names exactly as the names appear in CCMA.

OD includes the Media_Server_Selection flow application that demonstrates the basic logic for Avaya Aura® MS selection and call anchoring. The sample content in this script represents a starting point for administrators to define their own media server selection rules.

Avaya Aura® MS Zoning and the OD Master Script

The Media_Server_Selection flow application works in conjunction with the Master Script. The default OD Master Script provides basic ringback treatment requests for incoming calls before invoking a flow application configured by the administrator. This custom flow application provides all further treatments for each call.

If you use the Contact Router in OD to route contacts, you must update the Master Script to enable Avaya Aura® MS Zoning. After the update, the Master Script includes additional logic that invokes the Media_Server_Selection flow application. The Media_Server_Selection flow application selects the Avaya Aura® Media Server from a list and anchors the call, before returning control of the call to the Master Script, which in turn continues as normal (for example, the Master Script might then invoke a flow application mapped to a CDN).

The Media Server template block, which selects which Avaya Aura® MS to use to anchor incoming calls, must be invoked before any treatment requests are issued. If you do not use the Contact Router (for example, your Master Script is a flow or script), you must include the Media Server template block in the Master Script flow before the existing ringback treatment is invoked. You can use the Media_Server_Selection flow application as it used by the Contact Router. However, it's also possible to manually configure your Master Script with media server selection logic using the Media Server template block or ATTACH TO MEDIA SERVER command.

Note:

This chapter describes only the procedures to commission Avaya Aura® MS Zoning in a Contact Center that uses the Contact Router to route contacts, or uses a Master Script flow application that invokes the Media_Server_Selection flow application. It does not describe the steps to manually configure your Master Script with media server selection logic using the Media Server template block or ATTACH TO MEDIA SERVER command.

For more information on Avaya Orchestration Designer, flow applications and scripting commands, see *Using Contact Center Orchestration Designer*.

Avaya Aura® Media Server Zoning commissioning procedures

About this task

This task flow shows you the sequence of procedures you perform to commission Avaya Aura® Media Server Zoning.

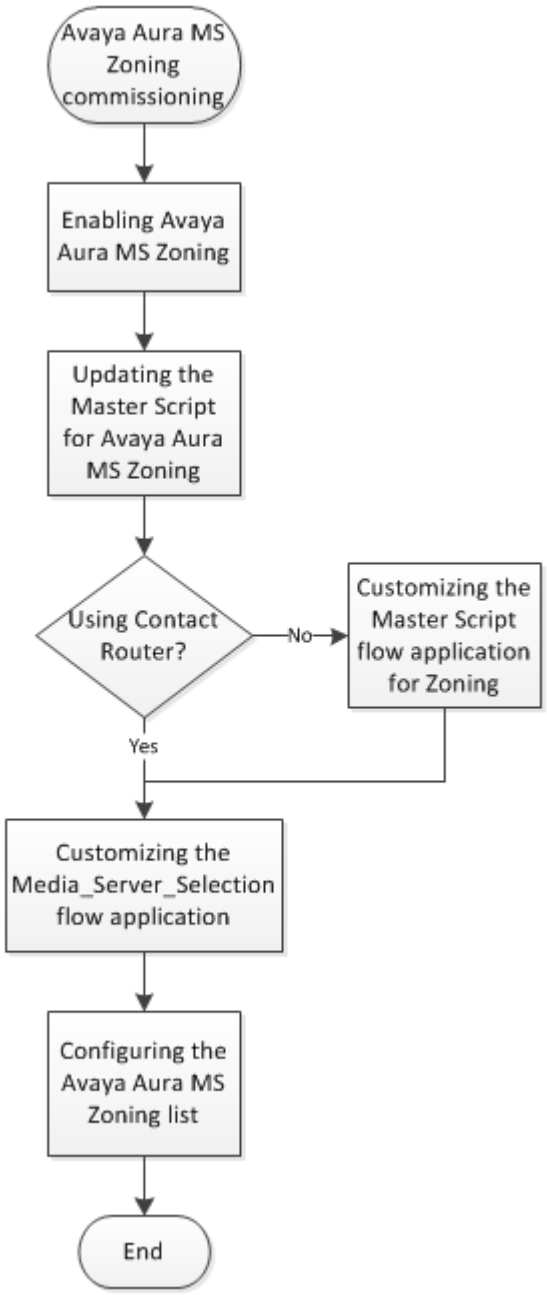


Figure 26: Avaya Aura® Media Server Zoning commissioning procedures

Enabling Avaya Aura® Media Server Zoning

Before you begin

- Log on to Contact Center Manager Administration. See Logging on to Contact Center Manager Administration for the first time on page 127.
- Avaya Aura® Media Server Zoning is a licensed feature. Ensure your Contact Center is licensed for Avaya Aura® Media Server Zoning.

About this task

Perform the following procedure to enable the Avaya Aura® Media Server Zoning feature in your Contact Center. This feature is disabled by default.

Procedure

1. On the CCMA Launchpad, click **Configuration**.
2. In the left pane, expand the Contact Center Manager Server on which to enable Avaya Aura® MS Zoning.
3. Click **Global Settings**.
4. Select the **Media Server Zoning** check box.
5. Click **Save**.
6. In the left pane, select the Contact Center Manager Server.
7. On the **Server** menu, click **Refresh Server**.

Updating the Master Script for Avaya Aura® MS Zoning

Before you begin

- Enable Avaya Aura® MS Zoning in CCMA.

About this task

You must update the Master Script in Avaya Orchestration Designer (OD) after enabling the Avaya Aura® MS Zoning feature.

Note:

The procedure applies only if you use the contact router in OD to route contacts. If your Master Script is a flow application, you must manually edit the Master Script flow to support the Avaya Aura® MS Zoning feature.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the CCMA Launchpad, click **Scripting**.
3. Click **Orchestration Designer** > **Launch Orchestration Designer**.

4. In the Contact Center view, right-click on the CCMA server name and click **Refresh**.
5. In the Contact Center view, expand the CCMA server name and right-click on an active Contact Center Manager Server node.
6. Click **Copy to Local view**.
7. In the **CCMA Name** box, select the name of the Contact Center Manager Administration server in the Local view where you want to copy the Contact Center Manager Server.

   Note:

   If no CCMA already exists in the Local View, you must create a CCMA instance. Right-click in the Local View pane, select **New** > **CCMA**, and type the name of the Contact Center Manager Administration server in the **CCMA Name** box.
8. In the **CCMS Name** box, type the name of the Contact Center Manager Server.

   To ensure consistency, ensure that the name of the Contact Center Manager Server in the Local view is the same as the Contact Center Manager Server in the Contact Center view.
9. Click **Finish**.
10. In the Local view, expand the Contact Center Manager Server server name.
11. Expand the **Applications** folder.
12. Double-click **Master_Script**.
13. On the dialog box, click **Yes** to update the Master Script for Avaya Aura® MS Zoning support.
14. In the Local view, right-click the Contact Center Manager Server and select **Synchronize**.

    The Synchronization view lists the changes made to the applications in the Local view.
15. In the Synchronization view, expand the CCMA and CCMS server names.
16. Expand **Applications**.
17. Right-click **Master_Script** and select **Update in Contact Center**.
18. Click **OK** to confirm.
19. In the Contact Center view, expand the CCMA and CCMS server names.
20. Expand **Applications**.
21. Double-click **Master_Script**.

    The **Media Server** tab appears on the Contact_Router.

Customizing the Master Script flow application for Zoning

About this task

Customize your Master Script flow application to reflect your own zoning requirements. If your Master Script is a flow, you can use the Media_Server_Selection flow application as it is used by the Contact Router. This task provides an example which describes the features of the Master Script when enabled for Avaya Aura® MS Zoning.

Note:

If you use the contact router in OD to route contacts, skip this procedure.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the CCMA Launchpad, click **Scripting**.
3. Click **Orchestration Designer** > **Launch Orchestration Designer**.
4. In Orchestration Designer, in the Contact Center view, expand the CCMA and CCMS server names.
5. Expand **Applications**.
6. Double-click **Master_Script**.

   If your Master Script is configured as a flow, the Master_Script flow application opens in the right pane.
7. Apply your custom changes to the Master_Script flow application to reflect the zoning requirements for your Contact Center solution.

Example

The following is an example of a Master Script enabled for Avaya Aura® MS Zoning. When enabled for Avaya Aura® MS Zoning, the Master Script must invoke the Media_Server_Selection script when a new voice contact arrives. The Media_Server_Selection script selects the Avaya Aura® Media Server from a list and anchors the call, before returning control of the call to the Master Script. The additional logic introduced for Avaya Aura® MS Zoning ensures the Master Script only invokes the Media_Server_Selection script once for each call.

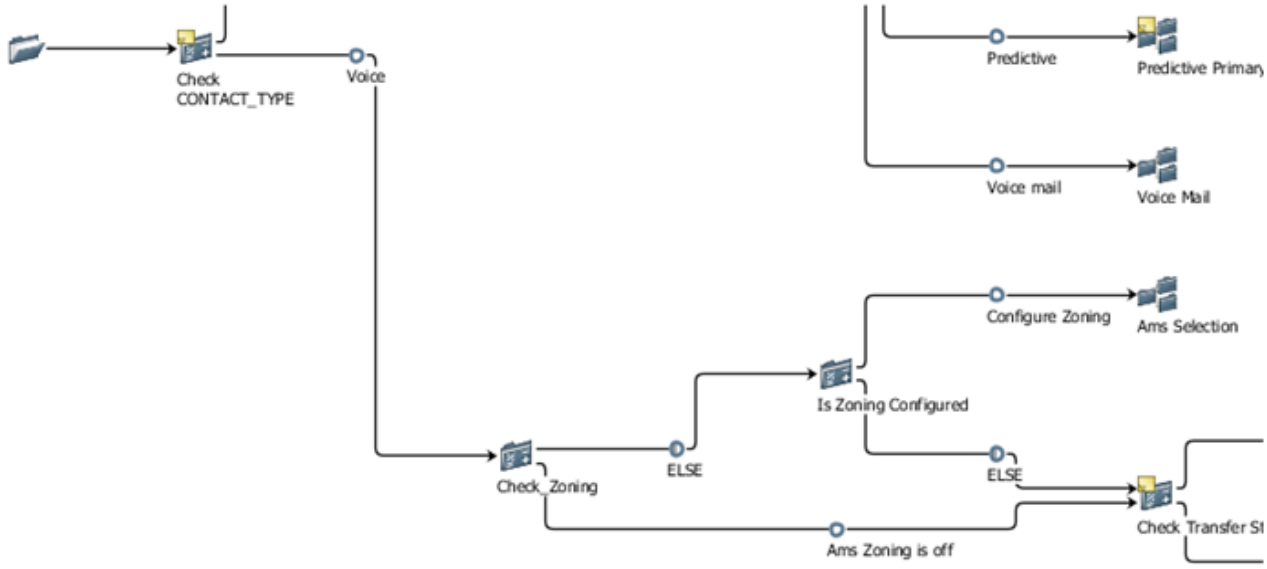


Figure 27: A diagram of an example of a Master Script enabled for Avaya Aura® MS Zoning. In the example the Media_Server_Selection flow application is used.

- The script relies on a call variable named ‘cc_ams_selection_enabled’, which is set to 1 by default.
- Based on the value of the ‘cc_ams_selection_enabled’ variable, the **Check_Zoning** block branches one of two ways:
  - If the value is set to 0, the Avaya Aura® MS Zoning logic is ignored and control moves directly to the **Check Transfer State** block.
  - Otherwise, control moves to the **Is Zoning Configured** block.
- The **Is Zoning Configured** block similarly branches based upon the value of the ‘cc_ams_selection_enabled’ variable and with similar logic as above. However, the **Is Zoning Configured** block includes an additional processing step on the **Configure Zoning** branch to update the variable value to 2. This results in the **Check Transfer State** block being reached after the Media_Server_Selection script returns control of the call to the Master Script (for example, the second pass through the Master Script).

Note:

In the example Master Script above, the **AMS Selection** block is the point at which the Master Script invokes the Media_Server_Selection application.

Customizing the Media_Server_Selection flow application

About this task

Customize the Media_Server_Selection flow application to reflect your own zoning requirements. This task provides an example of a customized Media_Server_Selection flow application.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the CCMA Launchpad, click **Scripting**.
3. Click **Orchestration Designer** > **Launch Orchestration Designer**.
4. In Orchestration Designer, in the Contact Center view, expand the CCMA and CCMS server names.
5. Expand **Applications**.
6. Double-click the **Media_Server_Selection** application.

   The Media_Server_Selection flow application opens in the right pane.
7. Apply your custom changes to the Media_Server_Selection flow application to reflect the zoning requirements for your Contact Center solution.

Example

The following is an example of a customized Media_Server_Selection flow application which uses two criteria for selecting Avaya Aura® MS servers — CDN country code and SIP location. In this example, there are four Avaya Aura® MS servers and any number of CDNs.

Note:

The primary data center is located in the UK, but is not located in the South East.

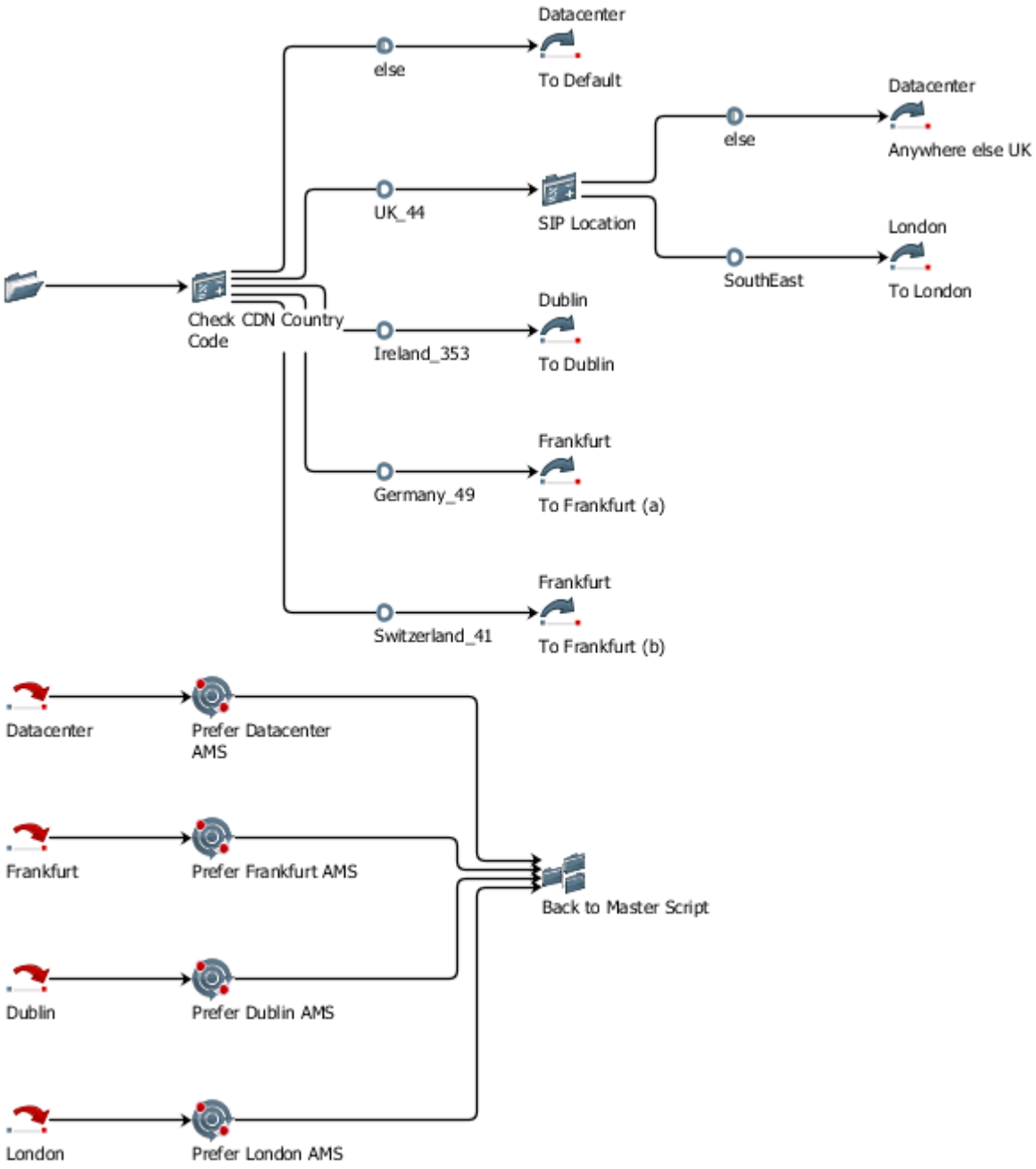


Figure 28: A diagram of an example of a customized Media_Server_Selection flow application which uses two criteria for selecting Avaya Aura® MS servers — CDN country code and SIP location.

- The script first checks the CDN country code and chooses an Avaya Aura® MS server within the matching country where possible.
- In the Switzerland case there is an ingress point with CDNs to dial; however as there is no Avaya Aura® MS present there, the Media_Server_Selection flow application selects the Frankfurt server as it is closest.
- In the UK case, there are two Avaya Aura® MS servers – one at the data center and one in London. The country code alone is not enough to make a decision, so the

Media_Server_Selection flow application uses the SIP Location field in the incoming INVITE to decide which UK Avaya Aura® MS server to anchor the incoming call on.

- This example Media_Server_Selection flow application includes a ‘catch-all’ rule for the CDNs. This allows you to subsequently introduce ingress points for other countries.

Configuring the Avaya Aura® MS Zoning list

Before you begin

- Ensure your Avaya Aura® Media Servers are added in CCMA. See Adding media servers on page 131.
- Configure your Media_Server_Selection flow application to reflect your own media server selection rules. See Customizing the Media_Server_Selection flow application on page 215.

About this task

Configure the Avaya Aura® MS Zoning list to allow your flow application to target up to five Avaya Aura® MS instances to anchor calls for a particular zone.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the CCMA Launchpad, click **Scripting**.
3. Click **Orchestration Designer** > **Launch Orchestration Designer**.
4. In Orchestration Designer, in the Contact Center view, expand the CCMA and CCMS server names.
5. Expand **Applications**.
6. Double-click the **Media_Server_Selection** application.
7. In the **Media_Server_Selection** pane, double-click the Media Server icon () that you want to configure the zoning list for.
8. Under **Media Server Options**, click **Select**.
9. On the **Avaya MS Zoning Configuration Wizard** window, select **List Builder** or **Variable Chooser** and click **Next**.
10. If you select **List Builder**:
    a. Under Available Media Servers, expand **Application Manager Data** and **Media Servers**.
    b. Select the Media Servers you want to target for specific calls and click **Add**.

    Note:

    You can add a maximum of five Media Servers to the configured list. This allows up to five Avaya Aura® MS servers to be used to anchor calls for a specific zone.

c. Use the **Up** and **Down** buttons to set the priority order of the Media Servers.

d. Click **Finish**.

11. If you select **Variable Chooser**:

a. Expand **Application Variables** and **STRING**.

b. Select the string variable that selects the preferred Avaya Aura® MS instance. For example, select **mediaservice**.

c. Click **Next**.

d. Click **Finish**.

Note:

When you use a variable in the Media Server block, the preceding logic within the Media_Server_Selection application must set the value of the variable to a comma-separated list of your Avaya Aura® MS names.

Example

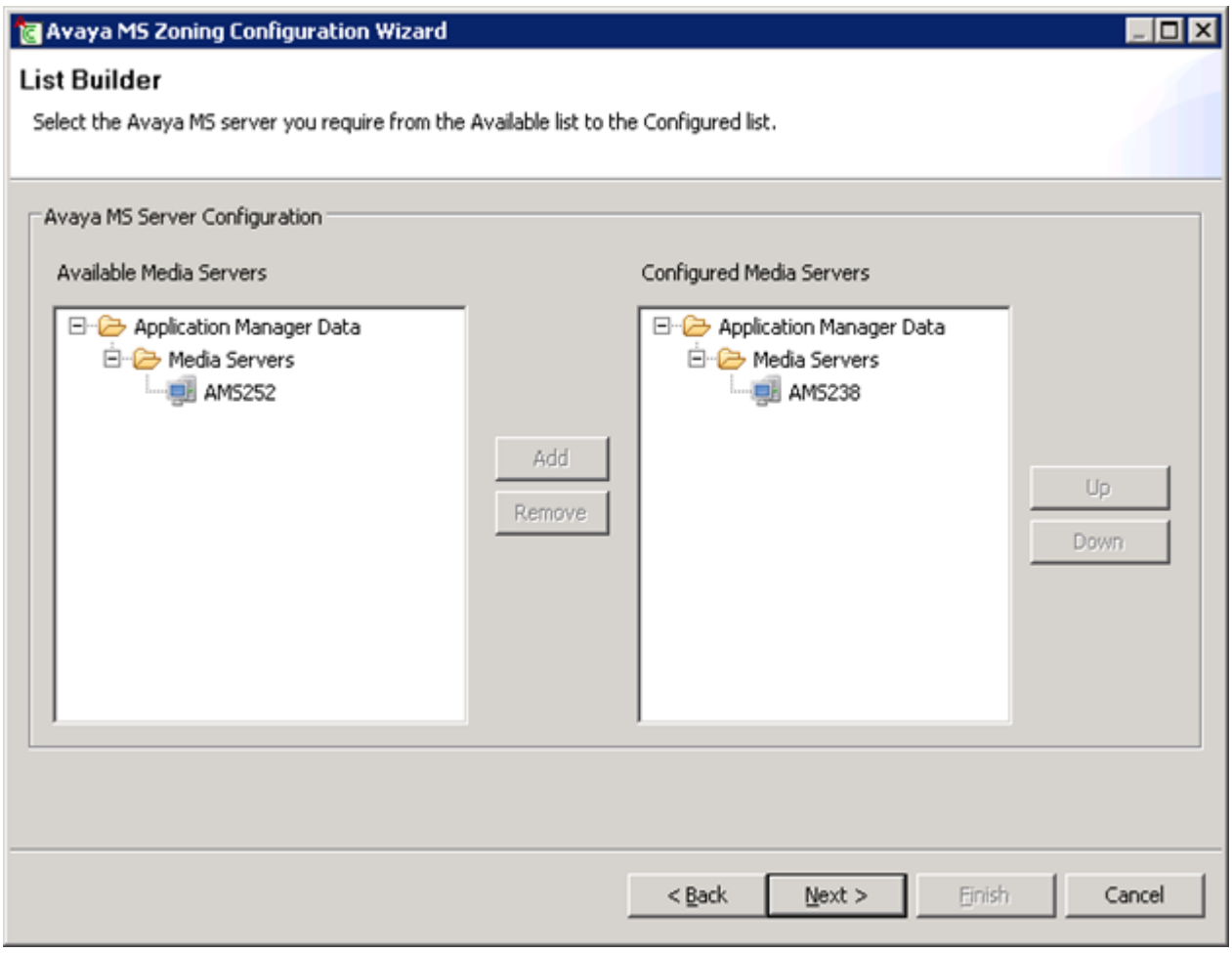


Figure 29: Example of configuring the Avaya Aura® MS Zoning list using the List Builder

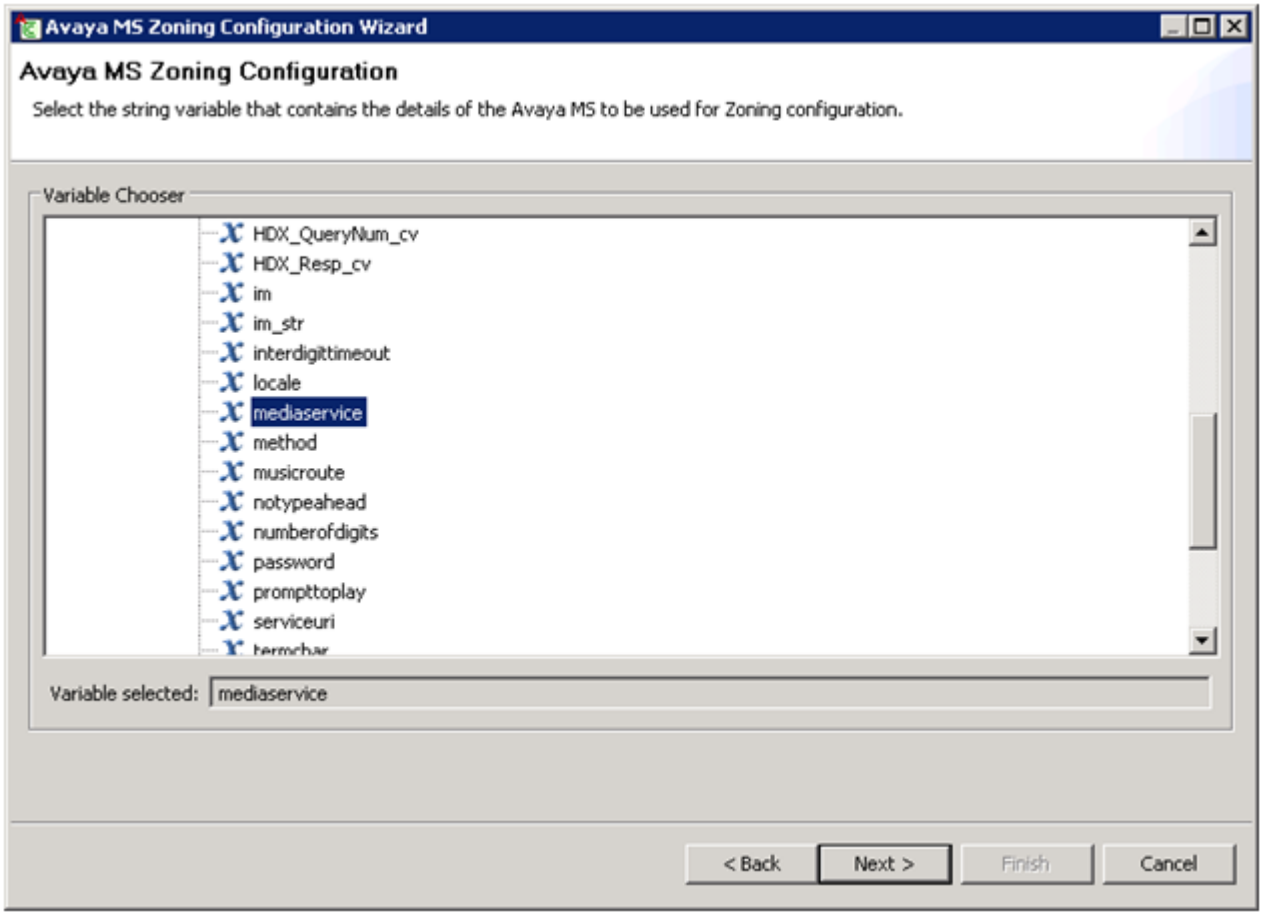


Figure 30: Example of configuring the Avaya Aura® MS Zoning list using a string variable

Chapter 19: Agent Greeting commissioning

The Agent Greeting feature allows agents to record personal greetings that the system can play automatically when an agent answers a voice contact. Agents can also record time of the day greetings (if the administrator has configured the Time of Day settings). Only SIP-enabled contact centers support Agent Greeting.

Important:

If you delete an agent or supervisor using Contact Center Manager Administration, you can then use Avaya Aura® Media Server - Element Manager to delete their recorded greetings. Using Avaya Aura® Media Server - Element Manager to manipulate Agent Greeting prompts is not supported. Use Element Manager only to delete recorded greetings. Agent Greeting prompt manipulation is supported only when using the Agent Greeting telephony prompt menu.

When you license and configure Agent Greeting, you can also configure Announcement Recorder. The Announcement Recorder application is a Telephony User Interface (TUI) that supervisors and supervisor agents can use to change prompts used in Contact Center flow applications. To configure Announcement Recorder, create an additional dial pattern to route calls to the Announcement Recorder application. Supervisors and supervisor agents that want to use the application must be enabled for Agent Greeting.

You must complete all the procedures in this section in sequential order.

Prerequisites for Agent Greeting commissioning

- Install and commission your SIP contact center including all Avaya Aura® MS configuration.
- Enable the Agent Greeting license on the Contact Center License Manager.

Agent Greeting commissioning checklist

The following is a list of key configuration items required for Agent Greeting commissioning.

Item	Your value	Description
Ensure that Contact Center is licensed for Agent Greeting		Agent Greeting is a licensed feature that you must enable in Contact Center Manager Server-Server Configuration.
System Manager User ID		The user ID you use to log on to the System Manager Web interface.
System Manager Password		The password you use to log on to the System Manager Web interface.
Contact Center server IP Address		The IP address of the Contact Center server.
Contact Center standby server IP Address		If your Contact Center implements HA, the IP address of the standby Contact Center server.
Agent Greeting endpoint number		A telephone number that you want agents to dial to access the Agent Greeting application.
Announcement Recorder endpoint number		A telephone number that you want supervisors and supervisor agents to dial to access the Announcement Recorder application.
CCMA Username		The username of a CCMA user with full administration permissions.
CCMA Password		The password of a CCMA user with full administration permissions.

Creating a SIP Entity for the Contact Center Agent Greeting endpoint

Before you begin

- Ensure you create a routing domain and a routing location.

About this task

Create a SIP Entity for the Contact Center server Agent Greeting endpoint.

If your Contact Center implements High Availability (HA), then you must create a second Contact Center SIP Entity which uses the standby server IP address.

Procedure

1. On the System Manager console, select **Routing** > **SIP Entities**.
2. Click **New**.

3. In the **Name** box, type a name for the Contact Center server agent greeting endpoint SIP Entity. Avaya recommends that you type a descriptive name for your Contact Center server Agent Greeting endpoint SIP Entity.
4. In the **FQDN or IP address** box, type the IP address of the Contact Center server.
5. From the **Type** list, select **Other**.
6. In the **Location** box, select the location for this Contact Center.
7. Under SIP Link Monitoring, use the drop-down menu to select one of the following:

   —Use Session Manager Configuration - Use the settings under **Session Manager – Session Manager Administration**.
   —Link Monitoring Enabled - Enables link monitoring on this SIP entity.
   —Link Monitoring Disabled - Disables link monitoring on this SIP entity.
8. Click **Commit**.
9. If your Contact Center implements High Availability (HA), repeat this procedure to create a second SIP entity, using the IP address of the standby server.

Variable definitions

Name	Description
Name	SIP entity name. This name must be unique and can have between 3 and 64 characters.
FQDN or IP Address	Fully qualified domain name or IP address of the Contact Center server SIP entity. If your Contact Center server does not implement High Availability (HA), then use the Contact Center server IP Address. If your Contact Center server implements High Availability (HA) then use the Contact Center active server IP address for one SIP Entity Link. Use the Contact Center standby server IP address for a second SIP Entity Link.
Type	SIP entity type; use Other.
Notes	Additional notes about the SIP entity.
Location	SIP entity location. Select from previously defined locations.
Time Zone	Time zone for the SIP entity.

Creating a SIP Entity Link to the Contact Center Agent Greeting endpoint

Before you begin

- Ensure you have created a SIP entity for the Contact Center Agent Greeting endpoint.

About this task

Session Manager enables you to create an entity link between the Session Manager and any other administered SIP entity.

Create a SIP entity link from the Session Manager to the Contact Center server Agent Greeting endpoint. You must configure an entity link between a Session Manager and any entity that you have administered, if you want the Session Manager to be able to send messages to, or receive messages from, that entity directly. To communicate with other SIP entities, each Session Manager instance must know the port and the transport protocol of its entity link to these SIP entities in the network.

If your Contact Center implements High Availability (HA), then you must create a two SIP entity links, one for each of the SIP entities for the active and standby servers.

Procedure

1. On the System Manager console, select **Routing** > **Entity Links**.
2. Click **New**.
3. In the **Name** box, type the name for this SIP entity link. Avaya recommends that you type a descriptive name for your SIP entity link.
4. Under **SIP Entity 1**, select the Session Manager SIP entity from the drop-down list, and provide the required port number 5080.
5. From the Protocol list, select **TCP**.
6. Under **SIP Entity 2**, select the required Contact Center server Agent Greeting endpoint SIP entity from the drop-down list, and provide the required port number 5080.
7. Select **Trusted** from the **Connection Policy** field. Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.
8. Click **Commit**.
9. If your Contact Center implements HA, repeat this procedure to create a second SIP entity link using the standby server Agent Greeting endpoint SIP entity.

Creating a routing policy from Session Manager to Contact Center

About this task

Create a routing policy from Session Manager to Contact Center for Agent Greeting. Session Manager uses the data configured in the Routing Policy to find the best match against the number (or address) of the called party.

Routing policies can include the “Origination of the caller”, the “dialed digits” of the called party, the “domain” of the called party, and the actual time the call occurs. Optionally, instead of “dialed digits”, and the “domain” of the called party, the administrator can define a “regular expression” to create a routing policy.

Depending on one or multiple inputs Session Manager determines a destination to which to route the call. Optionally, the destination can be qualified by “deny” which means that the call is not routed.

If your Contact Center implements High Availability (HA), then you must create two routing policies, one for each of the SIP entity links for the active and standby servers. The first routing policy must have a ranking of 0, and the second must have a ranking of 1.

Procedure

1. On the System Manager console, select **Routing** > **Routing Policies**.
2. Click **New**.

   The Routing Policy Details screen appears.
3. In the **General** section, in the **Name** box, type the name for the Routing Policy. Avaya recommends that you type a descriptive name for your Routing Policy.
4. In the **Notes** box, type your notes about this Routing Policy.
5. In the **SIP Entities as Destination** section, click **Select**.
6. From the list of SIP Entities, select the SIP entity for your Contact Center Agent Greeting endpoint.
7. Click **Select**.
8. If your Contact Center implements HA, under **Time of Day** settings, set **Ranking** to 0.
9. Click **Commit**.
10. If your Contact Center implements HA, repeat this procedure to create a second routing policy using the standby server Agent Greeting endpoint SIP entity. On the second policy, under **Time of Day** settings, set **Ranking** to 1.

Creating a dial pattern to route calls to the Contact Center Agent Greeting endpoint

About this task

Create a dial pattern using the Session Manager to Contact Center Routing Policy. Session Manager uses this dial pattern to route calls to the Contact Center server for Agent Greeting.

A dial pattern specifies which routing policy or routing policies Session Manager uses to route a call based on the digits dialed by a user. The originating location of the call and the domain in the request-URI also determine how Session Manager routes the call.

Session Manager tries to match the request-URI of a request to a row in the dial pattern table. The rows considered for the match are all rows where:

- the domain in the dial pattern table matches the domain in the request-URI
- the originating location in the dial pattern table row matches the originating location of the request, or, if there are no rows matching the originating location, the originating location in the table is set to -ALL-, or, if there was no originating location, the originating location in the table is -ALL-
- the digit pattern in the row matches the user-part of the request-URI, ignoring any parameters that are in the user part of the request-URI

If your Contact Center implements High Availability (HA), then you must associate both the routing policies for the Agent Greeting endpoints on the active and standby servers.

Procedure

1. On the System Manager console, select **Routing** > **Dial Patterns**.
2. Click **New**.

   The Dial Pattern Details screen appears.
3. In the **Pattern** field, type the number that agents dial to access the Agent Greeting recorder application.
4. In both the **Min** and **Max** fields, type the number of digits in the number you typed in the **Pattern** field.

   For example, if **Pattern** contains `123123`, then type `6` in the **Min** and **Max** fields.
5. If you want to restrict the Dial Pattern to a specific domain, select the domain from the **Domain** field.
6. Under the **Originating Locations and Routing Policies** section, click **Add**.
7. Under **Originating Location**, select all the Locations that you want associated with the Dial Pattern by selecting the check box in front of each item.
8. Under **Routing Policies**, select the Routing Policy from Session Manager to the Contact Center server for Agent Greeting.
9. If your Contact Center implements HA, select the Routing Policy from Session Manager to the Contact Center standby server for Agent Greeting.

10. Click **Select**.
11. If you want to deny calls to the Agent Greeting application from specified locations, on the Dial Pattern Details, click **Add** under the **Denied Originating Locations** section.
12. Select all the Locations from which calls to Agent Greeting are denied, and click **Select**.
13. Click **Commit**.

Creating a dial pattern to route calls to the Contact Center Announcement Recorder endpoint

About this task

If you plan to use the Announcement Recorder application, create a dial pattern using the Session Manager to Contact Center Routing Policy. Session Manager uses this dial pattern to route calls to the Contact Center server for Announcement Recorder.

If your Contact Center implements High Availability (HA), then you must associate both the routing policies for the Agent Greeting endpoints on the active and standby servers.

Procedure

1. On the System Manager console, select **Routing** > **Dial Patterns**.
2. Click **New**.

   The Dial Pattern Details screen appears.
3. In the **Pattern** field, type the number that supervisors and supervisor agents dial to access the Announcement Recorder application.
4. In both the **Min** and **Max** fields, type the number of digits in the number you typed in the **Pattern** field.

   For example, if **Pattern** contains `123123`, then type `6` in the **Min** and **Max** fields.
5. If you want to restrict the Dial Pattern to a specific domain, select the domain from the **Domain** field.
6. Under the **Originating Locations and Routing Policies** section, click **Add**.
7. Under **Originating Location**, select all the Locations that you want associated with the Dial Pattern by selecting the check box in front of each item.
8. Under **Routing Policies**, select the Routing Policy from Session Manager to the Contact Center server for Agent Greeting.
9. If your Contact Center implements HA, select the Routing Policy from Session Manager to the Contact Center standby server for Agent Greeting.
10. Click **Select**.

11. If you want to deny calls to the Announcement Recorder application from specified locations, on the Dial Pattern Details, click **Add** under the **Denied Originating Locations** section.
12. Select all the Locations from which calls to Announcement Recorder are denied, and click **Select**.
13. Click **Commit**.

Next steps

You must enable the Agent Greeting in CCMA for supervisors and supervisor agents who want to use Announcement Recorder.

Configuring the Voice XML Interpreter on Avaya Aura® Media Server

About this task

Ensure that the Avaya Aura® Media Server VoiceXML Interpreter is enabled and configured with the number of instances to support the required number of simultaneous Agent Greeting recorder sessions.

Procedure

1. Log on to the Avaya Aura® Media Server Element Manager.
2. In the navigation pane, click **System Configuration** > **Server Profile** > **Advanced Settings**.
3. Select **VoiceXML Interpreter**.
4. If you need more than 100 simultaneous Agent Greeting recorder sessions, in the **Additional Scalability Instances** field, select the number of additional instances that you require.

   Each additional instance allows 100 simultaneous Agent Greeting recorder sessions.
5. Click **Save**.
6. Restart the server for the changes to take effect.

Enabling Agent Greeting on CCMS

Before you begin

Important:

You need to restart the CCMS server to complete this procedure.

About this task

Follow this procedure to enable Agent Greeting on CCMS, if you did not enable it in the Ignition Wizard during initial configuration.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Server Configuration**.
3. Click the **Licensing** tab.
4. From the **Features** list, select **Agent Greeting**.
5. Click **Apply All**.
6. On the **Restart Required** dialog, click **Yes** to restart the server.

Configuring Agent Greeting on CCMA

Before you begin

Important:

Changes to these settings can take up to ten minutes to take effect.

About this task

Follow this procedure to set the general system settings for Agent Greeting on CCMA. These system wide settings control the operation of the Agent Greeting feature. The playback configuration settings apply to all Agent Greeting playbacks.

Modifying these settings on an existing Agent Greeting solution does not affect greetings already in progress.

Procedure

1. Log on to Contact Center Manager Administration with administrator privileges.
2. On the **Launchpad**, click **Configuration**.
3. In the system tree, expand the server on which to configure Agent Greeting.
4. In the left pane, click **Agent Greeting**.
5. Under **General Settings**, select the options that you want to enable.
6. Under **Time of Day Settings**, select the options that you want to enable.
7. Click **Save**.

Variable definitions

Name	Description
Agent Greeting enabled	Select to enable Agent Greeting.
Mute agent on greeting playback	Select to automatically mute the agent while the greeting plays.
“No greeting” warning tone	Select to ensure a warning tone is played, audible to the agent and the caller, if an agent answers a call for which no greeting is available.
Allow an agent to interrupt the greeting	Select to allow an agent to terminate the greeting to speak directly to the caller. For more information on interrupting the greeting, see *Using Agent Desktop for Avaya Aura® Contact Center* .
Maximum allowed greeting length	The maximum length of the greeting that the agent is allowed to record. Valid values: 12 to 30 seconds. This setting can take up to ten minutes to take effect. Reducing the maximum allowed greeting length does not affect greetings that are already recorded, even if they are longer than the new allowed maximum.
Agent Greeting Recording Number	This is the number on the PABX that routes to the Agent Greeting application on the Contact Center server. Enter the number that you configured the dial pattern to route calls to the Agent Greeting endpoint. This setting can take up to ten minutes take effect.
Prompt language	Lists the languages from which you can choose a language for the application prompts. Agents hear the selected language when they dial into the recording application. This setting can take up to ten minutes take effect.
Enable time of day greetings	Select to enable or disable the playback of time of day greetings.
Morning start time	Select to specify the time after which the system plays morning greetings.
Afternoon start time	Select to specify the time after which the system plays afternoon greetings.
Evening start time	Select to specify the time after which the system plays evening greetings.

Table continues…

Name	Description
Playback position	Select to specify whether the time of the day greeting plays before or after the main greeting.

Enabling Agent Greeting for individual agents and supervisors

About this task

You must enable Agent Greeting for each individual agent. By default, Agent Greeting is disabled for each agent. Therefore, even if Agent Greeting is globally enabled, Agent Greeting plays for the individual agents only when you enable it for each of them.

If you want supervisors and supervisor agents to use the Announcement Recorder application, you must enable Agent Greeting for them.

Procedure

1. Log on to Contact Center Manager Administration with administrative privileges.
2. On the Launchpad, click **Contact Center Management**.
3. In the left pane, expand the Contact Center Manager Server on which you want to modify the agent, supervisor agent, or supervisor.
4. Select the agent and scroll to the **Agent Greeting** tab. Select the **Agent Greeting Enabled** check box.
5. Type a numeric password in the **Agent Greeting Password** box. This is the password the agent, supervisor agent, or supervisor uses to log on to the Agent Greeting recording or Announcement Recorder applications.
6. Click **Submit**.

Performing an end-to-end test

Before you begin

- Ensure you complete all relevant installation and commissioning procedures in both this guide and *Avaya Aura® Contact Center Client Administration*.
- Ensure your contact center is operational.

About this task

After completing all the commissioning steps in this chapter, configure an agent for Agent Greeting and test that the agent can log in to Agent Greeting and record their greetings. Place a test call to the contact center to ensure the greeting plays as intended.

If you configured the Announcement Recorder endpoint, configure a supervisor or supervisor agent for Agent Greeting and test that they can log in to Announcement Recorder.

Procedure

1. Enable Agent Greeting for an agent.
2. Use the agent details to log on to the contact center.
3. Dial the number you configured for the Agent Greeting recording application.
4. Verify that you can access the Agent Greeting recording application.
5. Configure the default greeting for the agent, and optionally one or more skillset greetings.
6. Place a call to the contact center for this agent's skillset.
7. Verify that the agent's greeting plays when the agent answers the call.
8. If you configured Announcement Recorder:
    a. Enable Agent Greeting for a supervisor or supervisor agent.
    b. Dial the number you configured for the Announcement Recorder application.
    c. Verify that you can log in to the Announcement Recorder application as the supervisor or supervisor agent, and that you can navigate the menu system.

Chapter 20: Microsoft instant messaging server commissioning

Commission the Microsoft Lync Server or Microsoft Skype for Business Server to provide Instant Messaging (IM) and Presence services to Avaya Aura® Contact Center (AACC). Configure the Microsoft instant messaging server to route Customer IM messages that match the AACC route point requirements, to AACC for treatment. AACC uses TCP transport to communicate with the Microsoft instant messaging server. Avaya Agent Desktop uses TLS transport to communicate with the Microsoft instant messaging server.

Microsoft instant messaging server User Interfaces

Microsoft instant messaging servers have a number of user interfaces. The following are the main configuration interfaces you use to integrate the Microsoft instant messaging server with Avaya Aura® Contact Center:

- **Control Panel:** The Control Panel is a Web-based graphical user interface (GUI) used to manage the configuration of the Microsoft instant messaging servers, in addition to the users, clients, and other IM-aware devices in your organization.
- **Topology Builder:** Use the Topology Builder tool to define, validate and publish the required domains, sites, file shares, and pools that form a Microsoft instant messaging server environment. The Topology Builder stores this configuration information in a topology document. A topology document basically contains information mapping the various server roles, services and components in the Microsoft instant messaging infrastructure.
- **Management Shell:** Use this to configure Application Pools, Trusted Applications, Static Routes, and enable TCP ports. You can also use Management Shell to make and publish changes to the Microsoft instant messaging server topology. The Management Shell uses cmdlets. A cmdlet (pronounced "command-let") is a lightweight command that is used in the Management Shell environment to perform configuration actions. Typically, cmdlets return a Microsoft .NET Framework object for use by the next command.

You must complete all the procedures in this section in sequential order.

Note:

The procedures in this chapter use sample commands from Microsoft Lync Server 2010. Follow your Microsoft Lync Server 2013 or Microsoft Skype for Business documentation for equivalent steps in the later releases.

Microsoft instant messaging server prerequisites

Before you begin

- Install and commission the Microsoft Lync Server or Microsoft Skype for Business Server software.
- Using the Contact Center Manager Server (CCMS) Server Configuration utility, configure the IM Proxy Server settings. Configure the Microsoft instant messaging server IP address and TCP port number, and set the IM Provider type to Microsoft Lync.

Microsoft instant messaging server commissioning checklist

The following is a list of key configuration items required for Microsoft instant messaging server commissioning.

Item	Your value	Description
Microsoft instant messaging server version		The version of Microsoft instant messaging server you are using.
Microsoft instant messaging server IP address		The IP address of the Microsoft instant messaging server.
Microsoft instant messaging server TCP port number		The TCP port number of the Microsoft instant messaging server.
Microsoft instant messaging server log on details		The details you use to log on to the Microsoft instant messaging server.
AACC server IP address		The IP address of the AACC server.

Creating a Trusted Application Pool for Contact Center

About this task

Create a Trusted Application Pool that includes Avaya Aura® Contact Center. Microsoft instant messaging servers communicate only with trusted applications. To enable communication between a Microsoft instant messaging server and Contact Center, you must add Contact Center to the list of applications trusted by the Microsoft instant messaging server. A Trusted Application Pool is a list of applications that the Microsoft instant messaging server trusts. Contact Center must belong to a Trusted Application Pool (which is associated to a registrar pool) and be a Trusted Application Server in that application pool.

The Microsoft instant messaging server Management Shell *New-CsTrustedApplicationPool* cmdlet creates a new Trusted Application Pool to contain the servers that host trusted applications. If the Trusted Application Pool already exists as part of the topology, this cmdlet creates the external service associated with that pool. If the Trusted Application Pool does not exist, this cmdlet

creates the pool and the corresponding service. Creating a new trusted application pool also creates a new trusted application server assigned to that pool.

The *TreatAsAuthenticated* parameter determines if authentication is required for trusted applications connecting to servers within the pool.

Set the *ThrottleAsServer* parameter to true. Throttling a connection restricts the number of simultaneous transactions that can occur and improves overall solution stability.

This example creates a new pool, and uses the Identity parameter to specify the new Contact Center IP address of 47.166.110.90. The example uses a Registrar parameter with a value of lync133.sipccx.com to associate the new pool with the Registrar service at that FQDN. In this example the Registrar is on a Microsoft Lync Server lync133.sipccx.com. The example uses the Site parameter with a value of 1 and enables *TreatAsAuthenticated* and *ThrottleAsServer*.

For more information about the *New-CsTrustedApplicationPool* cmdlet, see the Microsoft instant messaging server Management Shell documentation.

Procedure

1. Log on to the Microsoft instant messaging server.
2. Access the Management Shell. For example, click **Start** > **All Programs** > **Microsoft Lync Server 2010** > **Lync Server Management Shell**.
3. Use the New-CsTrustedApplicationPool shell cmdlet to create a Trusted Application Pool for Contact Center:

   ```
   New-CsTrustedApplicationPool -Identity AACCServerIPAddress
   -Registrar registrar:LyncServer.Domain.com -Site 1
   -TreatAsAuthenticated $true -ThrottleAsServer $true
   ```

   Where AACCServerIPAddress is the IP address of the Contact Center server. LyncServer.Domain.com is a Lync server FQDN with which Contact Center registers.

   For example:

   ```
   New-CsTrustedApplicationPool -Identity 47.166.110.90 -Registrar
   Registrar:lync133.sipccx.com -Site 1 -TreatAsAuthenticated $true
   -ThrottleAsServer $true
   ```

4. In the Management Shell, enter the following:

   ```
   Enable-CsTopology
   ```

Creating a Trusted Application for Contact Center

About this task

Create a trusted application for Avaya Aura® Contact Center and add it to the Microsoft instant messaging server Trusted Application Pool. Contact Center must belong to a Microsoft instant messaging server Trusted Application Pool and be a Trusted Application Server in that application pool.

The Server Management Shell *New-CsTrustedApplication* cmdlet adds a trusted application to a trusted application pool and assigns a port number to that trusted application.

This example creates a trusted application with the Application ID “newTCP”. Use the *TrustedApplicationPoolFqdn* parameter to specify which trusted application pool the Contact Center application is in. In this example, the pool has the IP address 47.166.110.90. You must also specify a port for the application; this example uses port 5060. Note that running this cmdlet by specifying an ApplicationId and a *TrustedApplicationPoolFqdn* automatically generates an Identity that you can use later to retrieve, modify, or remove this application.

When you specify the port value with this cmdlet, the cmdlet does not open the port. You must open the port in the Windows firewall and any corporate firewalls in order for the trusted application to make contact with networks outside the firewall.

For more information about the *New-CsTrustedApplication* cmdlet, see the Server Management Shell documentation.

Procedure

1. Log on to the Microsoft instant messaging server.
2. Access the Management Shell. For example, click **Start** > **All Programs** > **Microsoft Lync Server 2010** > **Lync Server Management Shell**.
3. Use the New-CsTrustedApplication shell cmdlet to create a Trusted Application for Contact Center:

   ```
   New-CsTrustedApplication -applicationID IMRoute
   -TrustedApplicationPoolFqdn AACCServerIPAddress -port 5060
   ```

   Where IMRoute is the identifier for the route, and AACCServerIPAddress is the IP address of the Contact Center server.

   For example:

   ```
   New-CsTrustedApplication -ApplicationId newTCP
   -TrustedApplicationPoolFqdn 47.166.110.90 -Port 5060 -EnableTcp
   ```

4. In the Management Shell, enter the following cmdlet:

   ```
   Enable-CsTopology
   ```

Configuring the Contact Center Trusted Application server

About this task

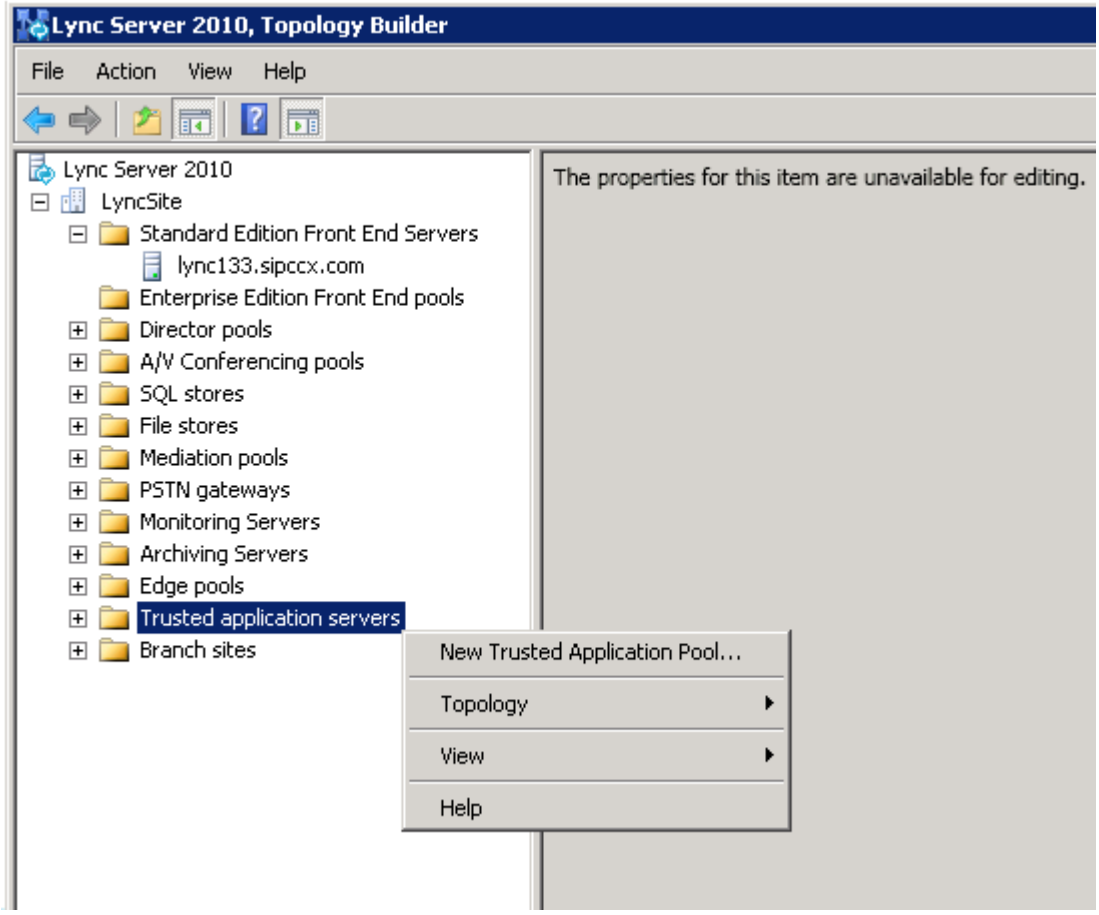
Configure the IP address of the Avaya Aura® Contact Center trusted application server. This server IP address is used by the Microsoft instant messaging server to process Contact Center application IM contacts.

Procedure

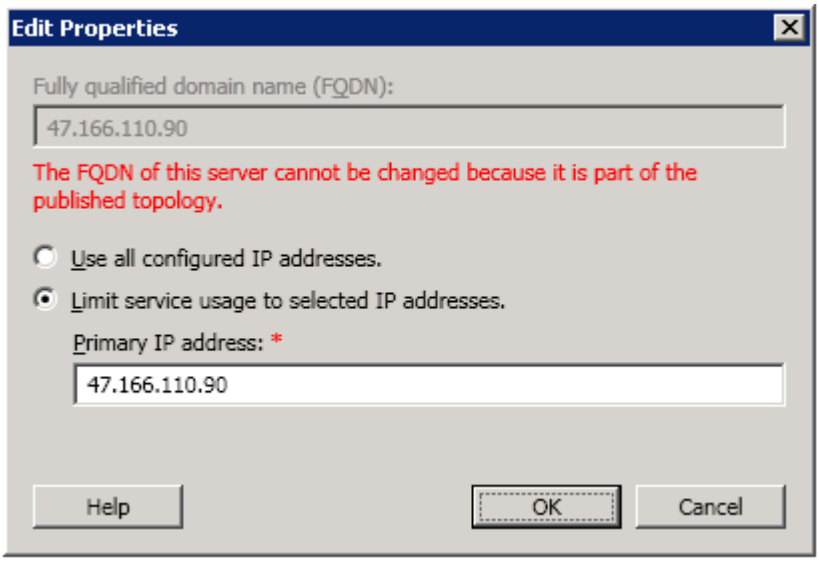
1. Log on to the Microsoft instant messaging server.

2. Access the Topology Builder. For example, click **Start** > **All Programs** > **Microsoft Lync Server 2010** > **Lync Server Topology Builder**.
3. Select the source of the Microsoft instant messaging server topology document and load it.

   The Topology Builder loads and displays the configured solution topology.
4. In the left pane, expand the Microsoft instant messaging server topology tree.
5. Expand the **Trusted application servers**.



6. Select your Contact Center trusted server, right-click and select **Edit Properties**.
7. Select **Limit service usage to selected IP addresses**. This configures Contact Center services to be provided by this single IP address within the Microsoft instant messaging server deployment.
8. In the **Primary IP address** box, type the IP address of the Contact Center server.



9. Click **OK**.
10. Select the top node, for example **Lync Server 2010**, and from the **Actions** pane, select **Publish**.

Configuring a static route to Contact Center

About this task

Configure a new static route from the Microsoft instant messaging server to Avaya Aura® Contact Center. In networks with static routing, message paths (routes) are predetermined by System Administrators. Static routes help ensure the timely and accurate delivery of messages, and with minimal overheard placed on servers.

Configure the Microsoft instant messaging server to check the message “To” address when it receives an IM message and then, where it matches the Contact Center IM Route Point (CDN), forward the IM message to Contact Center.

The Management Shell *New-CsStaticRoute* cmdlet creates new static routes. After you use the *New-CsStaticRoute* cmdlet to create a route, you must then use the *Set-CsStaticRoutingConfiguration* cmdlet to add the route to a collection of routing configuration settings.

This example creates an in-memory-only route that uses TCP as its transport protocol. The route points to the Contact Center server IP address 47.166.110.90 and uses port 5060. Any IM messages matching the URI domain suffix are routed to Contact Center. The resulting route object returned by this cmdlet is temporarily stored in a variable named $TCPRoute. This example then uses the *Set-CsStaticRoutingConfiguration* cmdlet to add that route to the global static routing configuration collection. The global route is one alternative. If required, you can use a specific route.

The *MatchUri* parameter is the domain suffix used to determine if the IM message is to be sent to the application handled by this static route. For example, configure the domain suffix as "companyX.com". Instant Messages to this domain suffix "companyX.com" are routed to the Avaya Aura® Contact Center server 47.166.110.90 using TCP port 5060.

For more information about the *New-CsStaticRoute* cmdlet, see the Microsoft instant messaging server Management Shell documentation.

Procedure

1. Log on to the Microsoft instant messaging server.
2. Access the Management Shell. For example, click **Start** > **All Programs** > **Microsoft Lync Server 2010** > **Lync Server Management Shell**.
3. Use the New-CsStaticRoute shell cmdlet to create a static route to Contact Center:

   ```
   $TCPRoute = New-CsStaticRoute -TCPRoute -Destination
   AACCServerIPAddress -port 5060 -MatchUri
   URISuffixToMatchAndRoute.com
   ```

   Where AACCServerIPAddress is the IP address of the Contact Center server, using format xxx.xxx.xxx.xxx and URISuffixToMachAndRoute is any URI that comes into the Microsoft instant messaging server that matches a particular format. For example, companyX.com routes to the Contact Center IP address specified in the command.

   ```
   $TCPRoute = New-CsStaticRoute -TCPRoute -Destination 47.166.110.90
   -Port 5060 -MatchUri companyX.com
   ```

4. Add the route to the global static routing configuration collection using the Set-CsStaticRoutingConfiguration shell cmdlet:

   ```
   Set-CsStaticRoutingConfiguration -Identity global -Route $TCPRoute
   ```

   where global is the unique identifier of the static routing configuration collection to be modified and TCPRoute is the individual static route maintained within the collection.
5. Access the Topology Builder. For example, click **Start** > **All Programs** > **Microsoft Lync Server 2010** > **Lync Server Topology Builder**.
6. Select the source of the Microsoft instant messaging server topology document and load it.

   The Topology Builder loads and displays the configured solution topology.
7. In the left pane, expand the Microsoft instant messaging server topology tree.
8. Select the top node, for example, **Lync Server 2010**, and from the **Actions** pane, select **Publish**.

Enabling the TCP port on the instant messaging server

About this task

On the Microsoft instant messaging server, enable the TCP port 5060 so Avaya Aura® Contact Center and the instant messaging server can communicate with each other. By default, the Microsoft instant messaging server software disables port 5060.

The Management Shell *Get-CsService –Registrar* cmdlet returns information about the Registrars used by the instant messaging server. Registrars are used to authenticate applications and to keep track of an application's status. You configured the registrar when you configured the Trusted Application Pool. The example *New-CsTrustedApplicationPool* cmdlet uses a Registrar parameter set to "Registrar:lync133.sipccx.com".

For more information about the *Get-CsService –Registrar* cmdlet, see the instant messaging server Management Shell documentation.

Procedure

1. Log on to the Microsoft instant messaging server.
2. Access the Management Shell. For example, click **Start** > **All Programs** > **Microsoft Lync Server 2010** > **Lync Server Management Shell**.
3. Find the instant messaging server (on which to enable the TCP port) using the Get-CsService shell cmdlet:

   ```
   Get-CsService –Registrar
   ```

   This returns information about the Registrars used by instant messaging. For example, to identify the Registrar, look for the following line in the returned text:

   Identity : Registrar:lync133.sipccx.com
4. Use the Set-CsRegistrar shell cmdlet to enable the TCP port 5060 for this Registrar:

   ```
   Set-CsRegistrar -Identity registrar:LyncServer.Domain.com –
   SipServerTcpPort 5060
   ```

   Where LyncServer.Domain.com is the Registrar.

   For example:

   ```
   Set-CsRegistrar -Identity registrar:lync133.sipccx.com
   -SipServerTcpPort 5060
   ```
5. In the Management Shell, enter the following cmdlet:

   ```
   Enable-CsTopology
   ```
6. In the Management Shell, enter the following cmdlet:

   ```
   Publish-CsLisConfiguration
   ```
7. In the Management Shell, enter the following cmdlet:

   ```
   Publish-CsTopology
   ```

Restarting the instant messaging service

About this task

Restart the Microsoft instant messaging services to apply the configuration changes. The instant messaging Management Shell *Stop-CsWindowsService* and *Start-CsWindowsService* cmdlets stop and start the Microsoft instant messaging services.

Procedure

1. Log on to the Microsoft instant messaging server.
2. Access the Management Shell. For example, click **Start** > **All Programs** > **Microsoft Lync Server 2010** > **Lync Server Management Shell**.
3. In the Management Shell, enter the following cmdlet:

   ```
   Stop-CsWindowsService
   ```

4. In the Management Shell, enter the following cmdlet:

   ```
   Start-CsWindowsService
   ```

Chapter 21: Avaya Aura® Presence Services Instant Messaging commissioning

Commission Instant Messaging to allow customers to send Instant Messaging contacts to Contact Center.

This chapter contains procedures to commission the contact center solution to route Instant Messaging contacts from Presence Services to Contact Center agents. You must complete all the procedures in this section in sequential order.

Presence Services Instant Messaging commissioning prerequisites

About this task

- Install and commission the System Manager server and the Avaya Aura® Presence Services server.
- Be familiar with System Manager user administration and maintenance. See documentation on administering Avaya Aura® Presence Services.
- Create a customer user account on the Presence Services server. For more information, see the Presence Services administration documentation.
- Use an IM client, such as Avaya one-X® Communicator, to test sending and receiving instant messages to the Presence Services server.

Avaya Aura® Presence Services Instant Messaging commissioning checklist

The following is a list of key configuration items required for Avaya Aura® Presence Services commissioning.

Item	Your value	Description
Avaya Aura® Presence Services version		The version of Avaya Aura® Presence Services you are using.
System Manager - User ID		The user ID you use to log on to the System Manager Web interface.
System Manager - Password		The password you use to log on to the System Manager Web interface.
Name of the domain you are mapping from		The System Manager user domain.
Name of the domain you are mapping to		The Presence Services XMPP domain.
CCMA IM route point name for Presence Services		The name of the route point configured in CCMA Configuration.
PS_domain		The domain name of the Presence Services server.
IP_Address		The IP address of the Presence Services server
Port_number		The port number of the Presence Services server, normally 5222.
Username		The username of the sample Web chat application user you created on the System Manager for the Web server.
Password		The password of the sample Web chat application user you created on the System Manager for the Web server.
Routepoint_1		The Instant Messaging route point XMPP address configured in CCMA and System Manager.

Verifying the substitution rule to map the System Manager user login domain to the Presence Services domain

About this task

Use this procedure to verify the substitution rule that maps the System Manager user login domain to the Presence Services domain. If you are using System Manager Release 7.0 or later, you can skip this procedure.

The domain substitution rule ensures that System Manager provisions a matching account on the Presence Services server for each user created. When this rule is in place, if you add a SIP handle to a user’s communication profile System Manager automatically provisions an XMPP handle in Presence Services.

The XMPP handle is what Presence Services uses to communicate with the IM Route Points, agent URIs, and the IM chat server address.

Normally the substitution rule exists on a fully commissioned Presence Services server.

Procedure

1. Log on to the System Manager console.
2. Under **Elements**, select **Presence** > **Configuration**.
3. If the substitution rule is not correct for your implementation, complete steps 4 to 7.
4. Click **Edit**.
5. In the **Domain Substitution - From** field, type the domain you are mapping from (System Manager user domain).
6. In the **Domain Substitution - To** field, type the Presence Services XMPP domain.
7. Click **Save**.

Variable definitions

Name	Description
Domain Substitution - From	The domain you are mapping from (System Manager user domain).
Domain Substitution - To	The Presence Services XMPP domain.

Creating a Presence Services user in System Manager for the route point

About this task

Use this procedure to create a user in System Manager which the Presence Services server uses to route instant messages to the contact center.

Procedure

1. Log on to the System Manager console.
2. Under **Users**, select **Manage users**.
3. Click **New**.
4. On the **Identity** tab, complete the user details.
5. Select the **Communications Profile** tab.
6. Under **Communications Address**, click **New**.
7. Complete the **Shared Communication Profile Password**, **Type** and **Fully Qualified Address** fields.

8. Click **Add**.
9. Click **Commit**.

Variable definitions

Name	Description
Last Name	Avaya recommends that you enter a descriptive name that identifies the user as being for a route point. For example, “routepoint”.
First Name	Avaya recommends that you enter a descriptive name that identifies the user as being for a route point. For example, use the route point number.
Description	Avaya recommends that you enter a description that identifies the user as being for a route point, and how the contact center uses the route point.
Login Name	Enter a login name for the route point user in the following format: <username>@<domain>.<com> The domain specified must have a substitution rule in System Manager mapping it to the Presence Services domain.
Authentication Type	The authentication type defines how the system performs this user’s authentication. Select **Basic**.
Password	Enter a password for the user.
Confirm Password	Confirm the password for the user.
Shared Communication Profile Password	For a Route Point the password must be a hyphen “-”.
Type	Select Avaya SIP.
Fully Qualified Address	The SIP domain handle for this user account (entering this automatically provisions an XMPP handle for the Presence Services server.)

Adding an IM route point on CCMA for Presence Services

Before you begin

- Log on to CCMA and open the Configuration component.

About this task

Use this procedure to add an Instant Message route point on CCMA.

Procedure

1. In the left pane, expand the Contact Center Manager Server to which to add the CDN (Route Point).
2. Select the **CDNs (Route Points)** folder.
3. In the right pane, in the **Name** box, type the name of the CDN (Route Point) as you want it to appear in reports.
4. In the **Number** box, type the CDN (Route Point) number.
5. In the **URI** box, type the XMPP handle for the user you created for this route point on the System Manager. For example, type `IM_CDN@CCMSx.DomainY.com`.
6. From the **Call Type** list, select **Local**.
7. Click any other row of the table to add the CDN (Route Point).

   Not Acquired appears in the **Status** column.
8. Select the **Acquired?** check box for the CDN (Route Point) Landing Pad.
9. Click any other row of the table to acquire the CDN (Route Point) Landing Pad.
10. Click **Refresh Status** to view the current status.

Creating a Presence Services user in System Manager for an agent

About this task

Use this procedure to create a user in System Manager for a contact center agent. Each agent that handles IM contacts must have a Presence Services user.

Procedure

1. Log on to the System Manager console.
2. Under **Users**, select **Manage users**.
3. Click **New**.
4. On the **Identity** tab, complete the user details.
5. Select the **Communications Profile** tab.
6. Under **Communications Address**, click **New**.
7. Complete the **Shared Communication Profile Password**, **Type** and **Fully Qualified Address** fields.
8. Click **Add**.
9. Click **Commit**.

Variable definitions

Name	Description
Last Name	Enter the agent's last name.
First Name	Enter the agent's first name.
Login Name	Enter a login name for the agent in the following format: <username>@<domain>.<com> The domain specified must have a substitution rule in System Manager mapping it to the Presence Services domain.
User Type	Select Agent.
Authentication Type	The authentication type defines how the system performs this user's authentication. Select Basic.
Login Password	Enter a password for the agent.
Confirm Password	Confirm the password for the agent.
Shared Communication Profile Password	Enter the password for this agent to use to log on in the Presence Services tab on Agent Desktop.
Type	Select Avaya SIP.
Fully Qualified Address	The SIP domain handle for this user account (entering this automatically provisions an XMPP handle for the Presence Services server.)

Adding the login ID to an agent's settings in CCMA

Before you begin

- Log on to CCMA and open the Contact Center Management component.
- Ensure that you have access to the agent record that you want to change.

About this task

Use this procedure to link an agent's Presence Services user account to their contact center configuration.

Procedure

1. From the **View/Edit** menu, select **Supervisors**.
2. In the left pane, click the server on which to work with the supervisor/agent profile.

   The list of supervisors configured on the server appears.
3. Click the supervisor to whom the agent is assigned.

   The tree expands to show the list of agents assigned to this supervisor.

4. Right-click the agent whose profile you want to edit, and then select **View Agent Details**.

   The Supervisor/Agent Details window appears.

5. In the **IM URI** menu, enter the XMPP handle of the user you created on System Manager for this agent.

Creating a Presence Services user in System Manager for the IM web server

About this task

Use this procedure to create a user in System Manager which the Presence Services server uses to exchange messages with the IM web interface.

Procedure

1. Log on to the System Manager console.
2. Under **Users**, select **Manage users**.
3. Click **New**.
4. On the **Identity** tab, complete the user details.
5. Select the **Communications Profile** tab.
6. Under **Communications Address**, click **New**.
7. Complete the **Shared Communication Profile Password**, **Type** and **Fully Qualified Address** fields.
8. Click **Add**.
9. Click **Commit**.

Variable definitions

Name	Description
Last Name	Avaya recommends that you enter a descriptive name that identifies the user as being for the IM Web server.
First Name	Avaya recommends that you enter a descriptive name that identifies the user as being for the IM Web server.
Description	Avaya recommends that you enter a description that identifies the user as being for the IM Web server.

Table continues…

Name	Description
Login Name	Enter a login name for the Web server user in the following format: <username>@<domain>.<com> The domain specified must have a substitution rule in System Manager mapping it to the Presence Services domain.
User Type	Select Agent.
Authentication Type	The authentication type defines how the system performs this user's authentication. Select Basic.
Login Password	Enter a password for the user.
Confirm Password	Confirm the password for the user.
Shared Communication Profile Password	Enter the password for the sample Web chat application user. If you create your own application, you need to use this password in that application.
Type	Select Avaya SIP.
Fully Qualified Address	The SIP domain handle for this user account (entering this automatically provisions an XMPP handle for the Presence Services server.)

Creating an Orchestration Designer application to route from an IM route point to an IM skillset

Before you begin

- You are familiar with creating and editing flows in Orchestration Designer. See *Using Contact Center Orchestration Designer*.
- You have access to an Orchestration Designer client and privileges to create flows for this contact center.

About this task

Create an application in Orchestration Designer to route IM contacts from the IM route point to an IM skillset.

Procedure

1. In Orchestration Designer, create a new flow to route IM contacts.
2. Edit the flow elements to route IM contacts received on the IM route point to an IM skillset.

Sending an Instant Message to the contact center and verifying the routing to an agent

Before you begin

- Complete all configuration procedures in this chapter.
- Create an agent enabled for Presence Services and for the IM contact type, and assign the agent to an IM skillset.

About this task

Test the Instant Message functionality and routing by sending an IM to the Presence Services user you created for the route point. Check that this IM routes to an agent.

Procedure

1. On a client PC, open Agent Desktop and log in as an agent enabled for IM contact types and assigned to the skillset that you want to test.
2. Make the agent Ready on Agent Desktop.
3. On another client PC, use an IM client, such as Avaya one-X® Communicator, to send an IM to the Presence Services user you created for the route point.
4. Check that expected IM treatments from the contact center, such as comfort messaging, appear in the chat client.
5. Check that the IM contact presents to the agent.
6. Accept the IM contact on Agent Desktop, and type a response.
7. Verify that the response appears in the chat window on the IM client.
8. Send a response from the IM client.
9. Verify that the response appears in the Agent Desktop.
10. End the chat session.

Chapter 22: Mission Critical High Availability Voice and Multimedia Contact Server commissioning

This section describes how to configure Mission Critical High Availability (HA) resiliency for a pair of Voice and Multimedia Contact Servers, which include Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT) and Contact Center Multimedia (CCMM), in a campus SIP-enabled contact center environment. Avaya Aura® Contact Center Mission Critical High Availability is supported with three different Contact Center solutions running on the Avaya Aura® Unified Communications platform. Mission Critical High Availability is supported in a campus SIP-enabled contact center environment that uses:

- Two Avaya Aura® Communication Managers and two Avaya Aura® Session Managers.

  OR

- An Avaya Aura® Communication Manager and an Avaya Aura® Session Manager (simplex).

  OR

- Two Avaya Aura® Solution for Midsize Enterprise (ME) servers, configured for High Availability.

Note:

Geographic High Availability is not supported for solutions using Midsize Enterprise (ME).

You must complete all the procedures in this section in sequential order.

Mission Critical High Availability campus overview:

In a Voice and Multimedia Contact Server HA configuration, one server is the active server and one is the standby server. The active Voice and Multimedia Contact Server actively processes scripts and contacts and records statistics. The standby server shadows the active server. The standby server copies all configuration changes made on the active server and monitors the active server status. If the active server fails, the standby server, running in Mission Critical standby mode, recognizes the failure and starts processing contacts. After the switchover, High Availability is disabled on the original active server.

The active and standby servers are part of the same Avaya Aura® Contact Center and they must be in the same subnet IP address range for campus High Availability resiliency to work.

The standby server must be configured the same as the active server. The standby and active servers must have the same patch level and the same hard disk drive partitions. Configuration changes made to the active server during normal operation are automatically copied to the standby server so that the standby server can take over processing from the active server when necessary.

In a Mission Critical campus High Availability solution, a CCMS or CCT service failure, or a CCMS, CCT or CCMM hardware, network, or database failure can initiate a switchover but only in the following situations:

- The active server is in the active mode.
- The active server is running. All the critical CCMS and CCT services are running.
- The active server has Enable Switchover enabled.
- The active and standby servers can communicate with the trusted server.
- The active server database and standby server database are synchronized. The standby server database is shadowing the active server database, and the critical services are running on the standby server.

If the Contact Center Administrator uses the Windows Service Control Manager (SCM) to stop a monitored service on an Active server, a switchover occurs.

If a critical service on the Standby server stops or is stopped, the Standby server stops all services and the contact center solution is no longer resilient. To reinstate High Availability resiliency, use System Management and Monitoring Component (SMMC) to “Start HA System” on the Standby server.

High Availability Utility:

Configure High Availability resiliency for CCMS, CCT and CCMM using the High Availability (HA) Utility in the Database Utilities. The High Availability Utility is used to configure which server is the active and which is the standby server. The HA utility also configures the Managed IP of the active server.

The High Availability Utility on an Active Server has the following dialogs under the Configuration tab:

- Server Mode
  - Configure the IP address for the Active and Standby servers
  - Configure the IP address for Trusted servers
  - Configure the IP address for the optional Remote Geographic Node
  - Identify if the server is Active, Standby, Remote Geographic Node, or Non HA
  - Enable Switchover
  - Configure the switchover time-out. This is the wait time if a network outage occurs before an automatic switchover occurs
  - Temporally set as Non-HA

- Notifications
  - Configure an email server for email notifications
  - Configure where and how often to send email notifications
  - Configure the email character set
- System
  - Display information on the system status
  - Verify that database shadowing is running

SMMC system tray:

The Contact Center System Management and Monitoring Component (SMMC) system tray gives quick access to action items in your High Availability environment, for example:

- Start HA System
- Stop HA System
- Disable Switchover
- Enable Switchover
- System Information
- Database Information
- Disable Next Auto Startup
- Select Standby Auto Startup Mode (Standby server only)
- Re-enable HA system (this option is available only when the active HA server is running but switchovers are disabled)

To access the SMMC system tray menu, right-click the SMMC icon on the Windows taskbar.

High Availability Utility and SMMC system tray:

Use the High Availability Utility to configure High Availability IP addresses and to configure which server is the active server and which is the standby server. Then use the System Management and Monitoring Component (SMMC) system tray to start database shadowing and High Availability functionality.

Determining the High Availability Network Timeout threshold:

The level of Contact Center application High Availability you achieve depends on your complete enterprise contact center solution, including the underlying network infrastructure.

It is important that you determine the optimum High Availability SMMC Network Timeout threshold value for your contact center network. If the threshold is set too high, High Availability might not recognize network outages, switchovers might not occur when necessary and call control might be lost. If the threshold is set too low, frequent and unnecessary switchovers might occur.

SMMC tests network connectivity between High Availability components and records the details of these connectivity tests in trace log files. The SMMC trace log files contain sufficient statistical data about SMMC communications in your network to characterize the networks behavior for a

High Availability contact center solution. You can use this SMMC statistical communications data to optimize your High Availability solution.

Avaya recommends that you analyze the SMMC trace log file and use the connectivity test results in it to optimize the High Availability settings for your network. For more information about using the Network Analyzer utility to optimize the High Availability configuration settings on network, see *Troubleshooting Avaya Aura® Contact Center*.

Prerequisites

- Ensure the Avaya Aura® Unified Communications platform is installed and patched to support Avaya Aura® Contact Center High Availability.
- The active and standby servers must meet the planning and engineering specifications. For more information, see *Avaya Aura® Contact Center Overview and Specification*.
- Ensure unused Network Interface Cards (NICs) are disabled.
- The Voice and Multimedia Contact Server is installed on the Active and Standby servers.
- CCMS is configured on the Active Server. For more information, see Contact Center Manager Server commissioning on page 49.
- Ensure the third-party networking utility is installed. For more information, see Installing the third-party networking utility on page 56.
- CCMA is configured on the Active Server. For more information, see Contact Center Manager Administration commissioning on page 100.
- CCT is configured on the Active Server. For more information, see Communication Control Toolkit commissioning for SIP-enabled Contact Center on page 183.
- CCMM is configured on the Active Server. For more information, see Contact Center Multimedia commissioning on page 192.
- The Active and Standby Server have a valid standby server license file, or, if you are using Avaya WebLM server, you have installed two Avaya WebLM server virtual guests and generated and applied the correct license files.
- Ensure the Voice and Multimedia Contact Server is on a domain. This is to allow the CCT clients such as Avaya Agent Desktop to communicate with both servers.
- Commission the Switchover Handling script. For more information about the Switchover Handling script, see *Avaya Aura® Contact Center Overview and Specification*.
- Before you commission High Availability, use System Control and Monitoring Utility (SCMU) to shut down all CCMS and CCT services on both the active and standby servers.

High Availability commissioning checklist

The following is a list of key configuration items required for High Availability commissioning in a SIP-enabled contact center environment.

Item	Your value	Description
Ensure that Contact Center is licensed for High Availability		High Availability is a licensed feature and is enabled when you purchase a standby server license.
Active server host name		The name of your AACC active server.
Active server IP address		The IP address of your AACC active server.
Standby server host name		If you have HA at the campus site, the name of your AACC standby server.
Standby server IP address		If you have HA at the campus site, the IP address of your AACC standby server.
Managed name		If you have HA at the campus site, the managed name of your AACC campus HA pair.
Managed IP address		If you have HA at the campus site, the managed IP address of your AACC campus HA pair.
Using Hosts file or DNS?		If you are using the Hosts files to resolve Managed names to Managed IP addresses, ensure that you add the Managed names and Managed IP addresses to the Hosts file.
Trusted IP address		Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.
RGN server host name		If you have HA geographic redundancy, the name of your AACC RGN server.
RGN server IP address		If you have HA geographic redundancy, the IP address of your AACC RGN server.
Using email notification?		You can enable automatic email switchover notifications to alert the Contact Center administrator. When enabled, the specified email address receives an automatic email which provides switchover information to the recipient.

Table continues…

Item	Your value	Description
SMTP server name		The name of your SMTP server for email notification after an automatic switchover occurs.
Email Username		The log on name of an email user configured on the email server.
Email Password		The password of an email user configured on the email server.
Email address to send notifications from		The email address that the email notification is sent from.
Email address to send notifications to		The email address that the email notification is sent to.
Database backup location		The location of the shared folder where you store database backups. This folder must not be on the active or standby servers.

Resolving the Managed name to the Managed IP Address

About this task

Complete the following procedure to resolve the Managed server name to the Managed IP address. If the server has two network interfaces, apply these settings to the CLAN network interface. Each Contact Center server in a domain requires a DNS static entry.

Important:

Avaya Aura® Contact Center High Availability solutions do not support Dynamic DNS.

Ask your System Administrator to add a Domain Name System (DNS) static entry for the active and standby servers and one additional DNS static entry for the each Managed name and associated Managed IP address.

In High Availability solutions, the managed IP address must be lower than the active and standby server IP addresses. For example, if the active server IP address is 1.2.3.4 and the standby server IP address is 1.2.3.5, the managed IP address is 1.2.3.3.

A typical High Availability campus solution with a pair of servers requires 3 DNS static entries; one DNS static entry for the active server, one DNS static entry for the standby server, and one DNS static entry for the Managed name and associated IP address.

If your solution is going to have a Remote Geographic Node, ask your System Administrator to add a Domain Name System (DNS) static entry for the Remote Geographic Node server.

Perform this procedure on the Active server. Perform this procedure on the Standby server if you have one. Perform this procedure on the Remote Geographic Node server if you have one.

Procedure

1. Open Windows Explorer.
2. Go to the folder C:\Windows\system32\drivers\etc.
3. Double-click on the **hosts** file, select **Open**, and select **Notepad**.

   The hosts file opens in Notepad.
4. Add the Managed IP address and the Managed server name to the hosts file.

   Important:

   The Managed name can be a full name or netbios server name.

Configuring CCMM General Administration

About this task

In a multimedia-enabled solution, Avaya Agent Desktop client software is typically downloaded from Contact Center Multimedia (CCMM). Agent Desktop then communicates with CCMM to handle email-based contacts. Agent Desktop communicates with Communication Control Toolkit (CCT) to handle voice contacts.

In a multimedia-enabled High Availability solution, use the CCMM Administration tool to configure standby CCMM and CCT details. Avaya Agent Desktop client software downloads these standby CCMM and CCT details and communicates with them if it cannot communicate with the active CCMM and CCT.

Important:

Before changes to the CCMM server settings take effect, you might need to restart the server.

Procedure

1. Log in to the Contact Center Manager Administration application.
2. Click **Multimedia**.
3. In the left column, select **General Administration**.
4. Click **Server Settings**.
5. Configure the **Contact Center Manager Server** entry with the managed IP address of the Voice and Multimedia Contact Server High Availability pair.
6. Configure the **Contact Center License Server** entry with the managed IP address or managed name of the Voice and Multimedia Contact Server High Availability pair.
7. Configure the **Contact Center Manager Administration** entry with the managed name of the Voice and Multimedia Contact Server High Availability pair.
8. Configure the **Contact Center Multimedia Server** entry with the managed IP address or managed name of the Voice and Multimedia Contact Server High Availability pair.

9. If your solution has a Remote Geographic Node Voice and Multimedia Contact Server, enter its name or IP address in the **Geographic Standby CCMM Server** field.
10. Configure the **Communication Control Toolkit Server** field with the IP address of your primary Voice and Multimedia Contact Server.
11. Configure the **Standby CCT Server** entry with the IP address of your standby Voice and Multimedia Contact Server.
12. If you are using a Remote Geographic Node server, configure the **Geographic Standby CCT Server** entry.

    Alternatively, if the Geographic Standby CCT Server does not exist, click **New** to create one.
13. Configure the **CC Web Stats** entry.

    If the Contact Center Web Statistics Server details do not exist and your solution uses Web Statistics, click **New**. Use the managed IP address of the optional Web Statistics server. The default port number is 9086.
14. In the left column, select **Email**.
15. Click **General Settings**.
16. Ensure that the Inbound URL is of the form `http://<ManagedIPAddress>/inboundattachment`.
17. Ensure that the Outbound URL is of the form `http://<ManagedIPAddress>/outboundattachment`.

Verifying services are ready for High Availability

About this task

Verify that all services stop before you configure High Availability. This ensures that all resources are available to the Active Server when it starts.

Perform this procedure using the System Management and Monitoring Component (SMMC) on the Active and Standby servers.

Procedure

1. Log on to the Active Server.
2. On the **Desktop** screen, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **Stop System**.
3. Repeat this procedure on the Standby Server.

Configuring campus High Availability on the active server

About this task

Configure campus High Availability resiliency on the active server using the High Availability utility. The active server is the server that normally processes calls.

If you know the IP address of the Remote Geographic Node server, enter it now during campus configuration. The High Availability configuration utility user interface is disabled when the HA system is shadowing.

You must restart the server to apply the High Availability settings.

Procedure

1. Select one server to be the active server and log on.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Configuration**.
4. Click **Server Mode**.
5. Under **Server Mode**, select **Active (Campus)**.
6. Under **Switchover And Network Timeout Configuration**, select **Enable Switchover**.
7. Under **Switchover And Network Timeout Configuration**, in the **Network Timeout** box, type the maximum length of time the network connectivity tests can continue to fail consecutively before corrective action is considered.
8. Under **Switchover And Network Timeout Configuration**, from the drop down list, select the unit of time for the network connectivity tests.
9. Under **IP Configuration**, in the **Active CLAN** box, type the IP address for the active server.
10. Under **IP Configuration**, in the **Standby CLAN** box, type the IP address for the standby server.
11. Under **IP Configuration**, in the **Managed IP** box, type the managed IP address.
12. Under **IP Configuration**, in the **Trusted IP** box, type the IP address of a trusted server.
13. Under **SMMC Port Configuration**, in the **Local SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the local (active) server.
14. Under **SMMC Port Configuration**, in the **Remote SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the remote (standby) server.
15. Click **Save**.
16. Reboot the active server to apply the changes.

Variable definitions

Name	Description
Network Timeout	The High Availability feature tests network connectivity between HA components by default every 100 milliseconds (100ms). The High Availability—Network Timeout value sets the maximum length of time these network connectivity tests can continue to fail consecutively before corrective action is considered. The minimum Network Timeout value is 200 milliseconds (200ms) and the maximum Network Timeout value is 5 seconds. For example, if Network Timeout is set to 400ms, HA requires 4 consecutive failed network connectivity tests before the remote system is marked as unreachable. In this case, if switchovers are enabled, an attempt to switch over is made. Avaya recommends that you set Network Timeout high enough to be tolerant of normal network latency, but low enough to be responsive if a failure occurs.
Active CLAN	The IP address for the server initially configured in Active mode.
Standby CLAN	The IP address for the server initially configured in Standby mode.
Managed IP	The virtual Managed IP (MIP) address that is used by the Active Server for campus resiliency. A MIP is used only when the Active and Standby servers are in the same subnet.
Trusted IP	The Active and Standby servers use the Trusted IP address to verify network connectivity. If the Active server cannot communicate with the Standby server it attempts to communicate with the Trusted IP address. If the Active server cannot communicate with the Trusted IP address, if shadowing and switchover are enabled, then the Active server stops processing contacts and shuts down. The Standby server starts processing contacts if it cannot communicate with the Active server but can communicate with the Trusted IP address. Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.

Table continues…

Name	Description
Remote Geographic Node	The IP address of the optional Remote Geographic Node.
Local SMMC Port	The port number for System Management and Monitoring Component (SMMC) on the local (active) server. The default port number is 57012.
Remote SMMC Port	The port number for System Management and Monitoring Component (SMMC) on the remote (standby) server. The port number entered here must match the port number set on the remote (standby) server. The default port number is 57012.

Configuring email notification on the Active Server

Before you begin

- If anonymous users are allowed, a user name and password might not be required. Check with the Administrator of the email server for setup configuration.

About this task

If an automatic switchover occurs, the High Availability utility can send email messages to configured users at a defined interval.

The default email notification character set is US_ASCII. The following character sets are also supported:

- ISO-8859-1
- UTF-8
- UTF-16BE
- UTF-16LE
- UTF-16

Procedure

1. Log on to the Active Server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Configuration**.
4. Double-click **Notification**.
5. Select the **Email** check box.
6. Type the **SMTP Server** name.
7. Type the **Username**.
8. Type the **Password**.

9. Type the **From Address**.
10. Type the **To Address** or **Addresses**.
11. Click **Save** to save the data.

Variable definitions

Name	Description
Email	Enables or disables email notifications.
SMTP Server	The SMTP Server name, which is automatically verified when saving the data.
Username	Email User log on name.
Password	Email User log on password.
Charset	Email character set to use.
From Address	Email address to send notifications from.
To Address	Email address to send notifications to.

Backing up the database on the Active Server

About this task

The Active Server is configured for High Availability. Now the Standby Server must be prepared for High Availability resiliency. Back up the Active Server to create a snapshot of the database which is then restored to the Standby Server. On the active Voice and Multimedia Contact Server all databases must be backed-up.

Important:

You must backup the Active server database, restore it onto the Standby server, and enable shadowing within 24 hours. If the difference in time between the Active and Standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the Active server database and restore it onto the Standby server before re-enabling shadowing. Ensure that the system clock time on the Active and Standby servers are synchronized.

Important:

Do not use a folder on the Active or Standby servers as the backup location.

Procedure

1. Log on to the Active Server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. Click **Backup Locations**.
4. Click **Create**.

5. From the **Driver Letter** list, select the network drive on which you want to store the CCMS, CCT, CCMM, ADMIN, CCMA, and Offline databases.
6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Backup Location. This location must be a shared folder with correct permissions.
7. In the **User Name** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the Windows password.
9. Click **Save**.
10. In the left pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Application** section, select **Offline**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.

Restoring the database on the standby server

Before you begin

- Know the location of the backup database. Use the Database Maintenance utility to create a backup location on the standby server.
- Ensure no traffic is running on the standby server.
- Stop shadowing if shadowing is running on the standby server.
- Stop all Contact Center services using the SCMU utility, if services are running.
- Ensure the patch level on the standby server is the same as the active server.

Important:

Not all CCT data is stored in the database; therefore the following data must be configured on the Standby Server, CCT License, CCT Contact Management Framework, CCT SOA configuration (CCT Web Services), and CCT logging location.

Important:

You must restore all databases on a Voice and Multimedia Contact server. Restoring only CCMS and not CCT, CCMM, ADMIN, or CCMA can leave an inconsistent server, and HA cannot shadow data correctly.

Important:

Restoring the ADMIN database can change configuration of backup locations on the standby server if the active server and standby server backup locations are different.

Therefore, after you restore the ADMIN database, close and reopen the Database and Maintenance utility.

About this task

If you have HA at the campus, restore the database from the active server to the standby server to ensure the databases are consistent. The Database Maintenance utility can restore all application databases at once. You must restore the CCMS, CCT, CCMM, ADMIN, and CCMA database onto the standby server.

Important:

You must backup the active server database, restore it onto the standby server, and enable shadowing within 24 hours. If the difference in time between the active and standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the active server database and restore it onto the standby server before re-enabling shadowing. Ensure that the system clock times on the active and standby servers are synchronized.

Procedure

1. Log on to the standby server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. In the **Database Maintenance** dialog box, in the left pane, click **Restore**.
4. In the right pane, under **Media Type**, select the media type on which the backup is restored.
5. If the backup file is on the network drive, in the **Backup Location** list, select the backup location.
6. Under **Application**, select CCMS, CCT, CCMM, ADMIN, and CCMA.
7. Under **Restore contents**, select **Data** and **Offline**.
8. Click **Restore**.
9. Use the **Information** field to monitor the progress of the restoration.
10. Click **Exit** to close the Database Maintenance utility.

Variable definitions

Name	Description
Application	The database and applications of Contact Center that you can back up.
Backup Location	The destination of the network disk. The values are configured in the Backup Locations.

Table continues…

Name	Description
Restore contents	The type of content that is stored in the database. Data is data in the database. Schema (read only) is the data for the database structure, tables and procedures. Offline is the Multimedia Offline database.
Media type	The type of media used for your backup file. You can use a network disk location or a tape drive. If you use a network disk location, you must configure a destination before you can back up the file.

Configuring High Availability on the Standby Server

Before you begin

- The Active Server databases are restored on to the Standby Server.

About this task

Configure High Availability resiliency on the Standby Server using the High Availability utility. The Standby Server shadows the Active Server and takes over processing if the Active Server fails.

You must restart the server to apply the High Availability settings.

Procedure

1. Log on to the Standby Server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Configuration**.
4. Double-click **Server Mode**.
5. Under **Server Mode**, select **Standby**.
6. Under **IP Configuration**, in the **Active CLAN** box, type the IP address for the active server.
7. Under **IP Configuration,** in the **Standby CLAN** box, type the IP address for the standby server.
8. Under **IP Configuration**, in the **Managed IP** box, ensure the managed IP address appears.
9. Under **IP Configuration**, in the **Trusted IP** box, type the IP address of a trusted server.

10. Under **SMMC Port Configuration**, in the **Remote SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the remote (active) server.
11. Under **SMMC Port Configuration**, in the **Local SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the local (standby) server.
12. Click **Save**.
13. Reboot the standby server to apply the changes.

Variable definitions

Name	Description
Active CLAN	The IP address for the server initially configured in Active mode.
Standby CLAN	The IP address for the server initially configured in Standby mode.
Managed IP	The virtual Managed IP (MIP) address that is used by the Active Server for campus resiliency. A MIP is used only when the Active and Standby servers are in the same subnet.
Trusted IP	The Active and Standby servers use the Trusted IP address to verify network connectivity. If the Active server cannot communicate with the Standby server it attempts to communicate with the Trusted IP address. If the Active Server cannot connect to the Trusted IP address on startup then no Contact Center services start on that server. If the Active server cannot communicate with the Trusted IP address, if shadowing and switchover are enabled, then the Active server stops processing contacts and shuts down. The Standby server starts processing contacts if it cannot communicate with the Active server but can communicate with the Trusted IP address. Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.
Local SMMC Port	The Network Management port number for System Management and Monitoring Component (SMMC) on the local (standby) server. The default port number is 57012.

Table continues…

Name	Description
Remote SMMC Port	The Network Management port number for System Management and Monitoring Component (SMMC) on the remote (active) server. The port number entered here must match the port number set on the remote (active) server. The default port number is 57012.

Verifying server details on the standby server

Before you begin

- The active server databases are restored on to the standby server.

About this task

After you restore the active server database on to the standby server, verify that the standby server is configured correctly.

Procedure

1. Log on to the standby server.
2. From the **Start** menu, in the Avaya area, click **Server Configuration**.
3. In the **Server Configuration** dialog box, click the **Local Settings** tab.
4. Verify the standby server local settings.
5. If you made any changes to the local settings, click **Apply All**.
6. On the **Restart Required** dialog, click **No**.
7. In the **Server Configuration** dialog box, click the **Licensing** tab.
8. Verify the standby server licensing details.
9. If you made any changes to the licensing details, click **Apply All**.
10. On the **Restart Required** dialog, click **No**.
11. In the **Server Configuration** dialog box, under **SIP**, click the **Network Settings** tab.
12. Verify the standby server **SIP Network Settings** details.
13. If you made any changes to the SIP Network Settings, click **Apply All**.
14. On the **Restart Required** dialog, click **No**.
15. In the **Server Configuration** dialog box, under **SIP**, click the **Local Subscriber** tab.
16. Verify the standby server **SIP Local Subscriber** details.
17. If you made any changes to the SIP Local Subscriber settings, click **Apply All**.
18. On the **Restart Required** dialog, click **Yes**.

If you did not make changes to any settings, CCMS does not display the **Restart Required** dialog.

19. Click **Exit**.

Variable definitions

Name	Description
Avaya Server Subnet IP Address	The IP address of the subnet that connects the Contact Center servers (Contact Center Manager Server, Network Control Center, Contact Center Manager Administration, and Contact Center Multimedia).
Voice Proxy Server • IP Address • Port • Network Transport	Information about the server that provides support for inbound and outbound calls, such as routing a call to an agent telephone. If the contact center uses an Avaya Aura® Session Manager, enter the IP address for the primary Session Manager. The server listening port. The default port is 5060. The SIP Network Transport communication protocol.
CTI Proxy Server • IP Address • Port • Network Transport	Information about the server that provides support for SIP Computer Telephony Integration (CTI) so that Agent Desktop can acquire and control agent telephones for TR87. Enter the IP address of the Avaya Aura® Application Enablement Services server. For an Application Enablement Services server the default SIP CTI Proxy Server port is 4723. The SIP Network Transport communication protocol. For an Application Enablement Services server, the default Network Transport communication protocol is TLS.

Table continues…

Name	Description
Backup Voice Proxy Server • IP Address • Port • Network Transport	Information about the server that provides backup support for inbound and outbound calls, such as routing a call to an agent telephone. Avaya Aura® Contact Center must have a Standby Server license to support a Backup Voice Proxy Server. The only type of Backup Voice Proxy Server supported by Avaya Aura® Contact Center is an Avaya Aura® Session Manager when it used with an Avaya Aura® Communication Manager. Enter the IP address for the backup Session Manager. The server listening port. The default port is 5060. The Backup Voice Proxy Server transport protocol.
IM Proxy Server • IP Address • Port • Network Transport	Information about the server that supports the deployment of Instant Message over SIP. The IP address of the SIP IM Proxy Server. The default SIP IM Proxy Server port is 5222. The IM SIP Proxy Server transport protocol.
IM Provider	Select your IM Provider, Aura Presence Services or Microsoft Lync (for Microsoft Skype for Business, select Microsoft Lync).
XMPP Domain	If using an Avaya Aura® Presence Services server, enter the domain name of the Extensible Messaging and Presence Protocol (XMPP) server.
Local SIP Subscriber • Contact Center Name • Domain Name	Information about the environment of the SIP-enabled contact center and how to identify the server within the network. The registration user name on the registration proxy. Use a suitable user name following the standards in your system. Associated domain name for the SIP- enabled contact center.
Web Service Ports	The Web Service Ports group box appears only if you select Avaya Aura® Presence Services as the IM Provider. Server Port default is 9100 Client Port default is 9120

Table continues…

Name	Description
SIP Server Type	Type of SIP proxy for the contact center integration. Depending on the switch type you select in the Application Selection window, the system automatically sets the specific SIP Server Type as the default.
MS Locale	Locale (including language and dialects) of the system environment.
Local Listening Ports	The SIP Communication protocol accepted by the system for incoming calls. TCP/UDP Port default is 5060 TLS Port default is 5061

Starting the Active Server

About this task

Start the Active Server using the System Management and Monitoring Component (SMMC) system tray. Starting the Active Server starts Contact Center applications and system processes.

Procedure

1. Log on to the Active Server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Configuration**.
4. Under **Switchover And Network Timeout Configuration**, select **Enable Switchover**.
5. Click **Save**.
6. On the **Desktop** screen of the active server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start HA System**. If the active server was previously rebooted, the system might already be started.
7. From the **Start** menu, in the Avaya area, click **System Control and Monitor Utility**.
8. Verify that Contact Center services are running.

Starting shadowing on the standby server

About this task

Start shadowing on the standby server using the System Management and Monitoring Component (SMMC) system tray.

The Standby server shadows the active server, maintaining a near real-time local copy of the Contact Center applications and Administration databases. Therefore, the standby server is configured with the most recent data and it can take over from the active server if necessary.

Important:

You must backup the active server database, restore it onto the standby server, and enable shadowing within 24 hours. If the difference in time between the active and standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the active server database and restore it onto the standby server before re-enabling shadowing. Ensure that the system clock times on the active and standby servers are synchronized.

Procedure

1. Log on to the standby server.
2. On the **Desktop** screen of the standby server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start HA System**.
3. From the **Start** menu, in the Avaya area, click **System Control and Monitor Utility**.
4. Check that the Contact Center services are running.

   Note:

   The following services do not start on the standby server:

   - CCMS_MasterService
   - CCMA - IceRTDService
   - CCMM - EmailManager, MCMC, CCMMOAM, Campaign Scheduler Service

Verifying High Availability is running

About this task

Verify that the Standby server is shadowing the active server using the High Availability Utility. The System dialog box of the High Availability utility displays system information about the active and the standby servers.

The dialog box displays the followings information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information
- Remote server connection status
- Remote server port information

- License information
- Databases shadowed
- Time of last record shadowed
- Database namespaces
- Local and remote information on system status, switchover, shadowing and network
- CC Application install information
- Database space and journaling information
- Database processes information

Procedure

1. Log on to the active server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. In the left pane, expand **Configuration**.
4. Select **System**.
5. Select **Get System Configuration**.

   The most recent system information appears.

Example

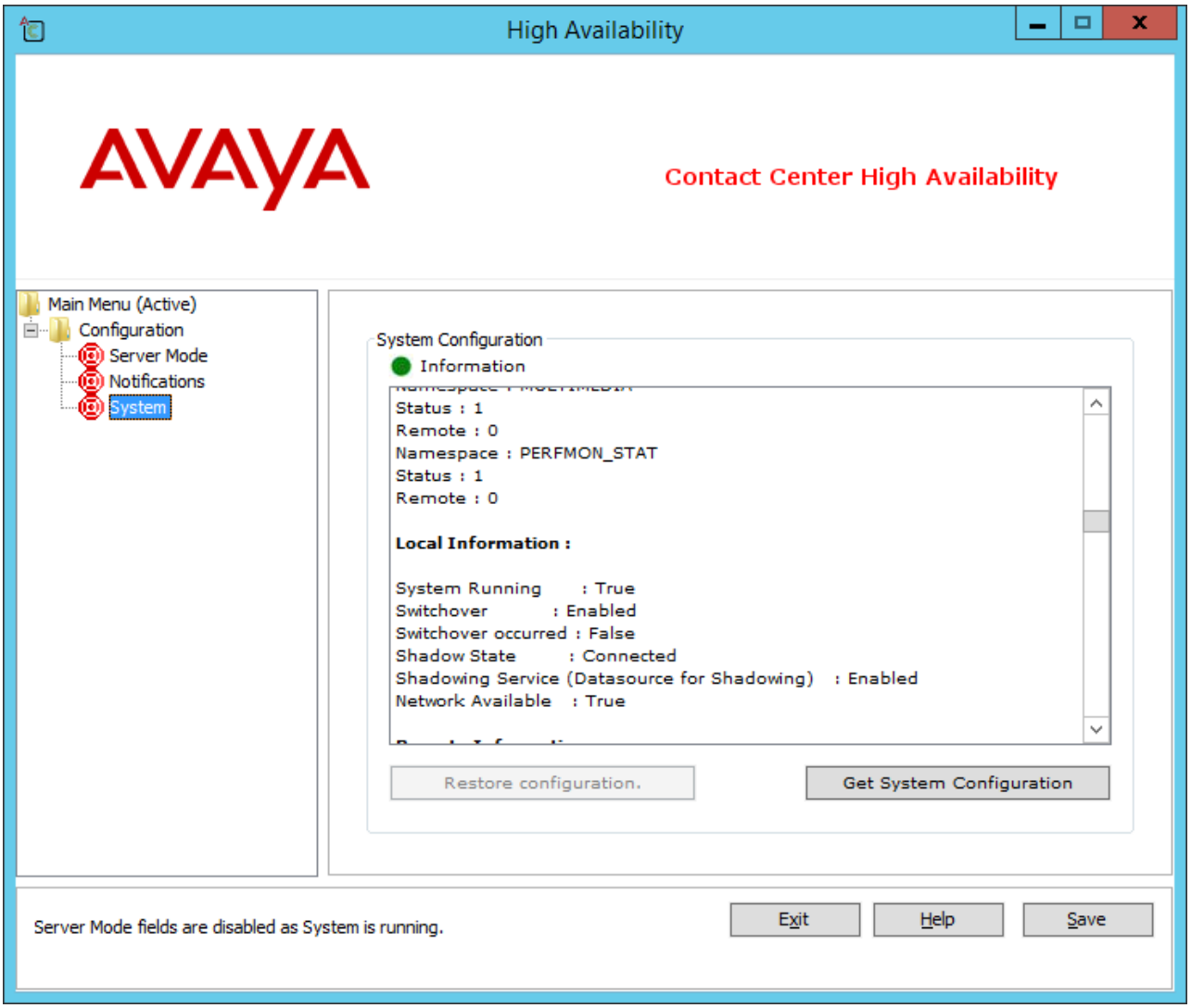


Figure 31: Example of an active server with the HA system running

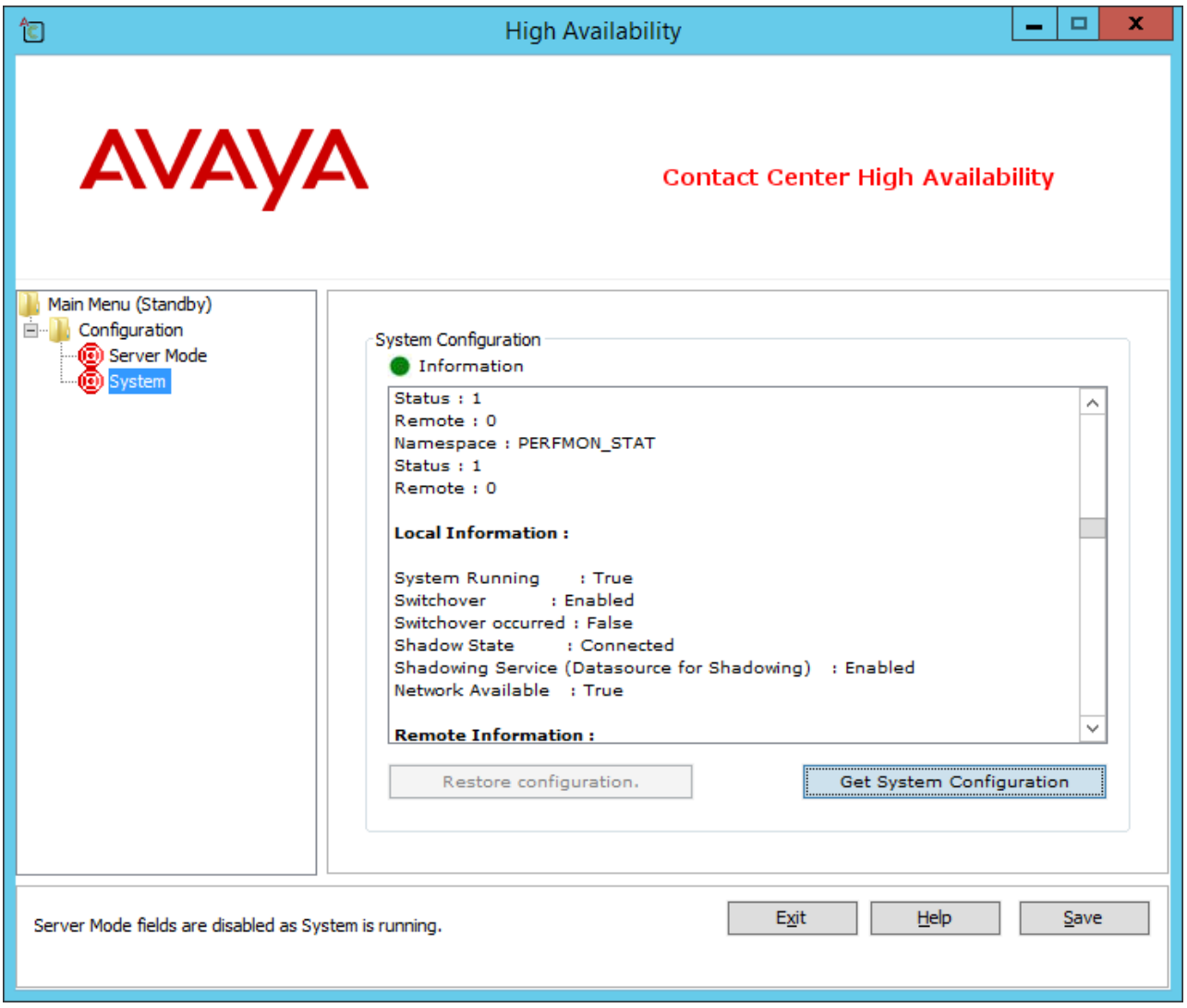


Figure 32: Example of a standby server with the HA system running

Note the **Server Mode fields are disabled as System is running** notice on the HA user interface.

Changing server details in Contact Center Manager Administration

About this task

In Contact Center Manager Administration, change the Contact Center Manager Server, Communication Control Toolkit and Contact Center Multimedia details to use the High Availability Managed IP address and Managed name details.

The High Availability Managed IP address and Managed name details entered here must match those configured in the hosts file.

Procedure

1. Log on to the active server.
2. Log on to the Contact Center Manager Administration application with administrative privileges.
3. On the **Launchpad**, click **Configuration**.
4. From the list of servers in the system tree, right-click on CCMS, and select **Edit Properties**.
5. In the **Server Name** box, type the High Availability Managed name of the active server.
6. In the **IP Address** box, type the High Availability Managed IP address of the active server.
7. In the **Display Name** box, type the name of Contact Center Manager Server as you want it to appear in the system tree of Contact Center Administration.
8. Click **Submit**.
9. From the list of servers in the system tree, right-click on CCT, and select **Edit Properties**.
10. In the **Server Name** box, type the High Availability Managed name of the active server.
11. In the **IP Address** box, type the High Availability Managed IP address of the active server.
12. In the **Display Name** box, type the name of Communication Control Toolkit as you want it to appear in the system tree of Contact Center Administration.
13. Click **Submit**.
14. From the list of servers in the system tree, right-click on CCMM, and select **Edit Properties**.
15. In the **Server Name** box, type the High Availability Managed name of the active server.
16. In the **IP Address** box, type the High Availability Managed IP address of the active server.
17. In the **Display Name** box, type the name of Contact Center Multimedia as you want it to appear in the system tree of Contact Center Administration.
18. Click **Submit**.

Using the Contact Center Manager Administration managed name

About this task

Use the High Availability managed name of Contact Center Manager Administration to access the CCMA application. When the Avaya Aura® Contact Center High Availability feature is configured

and enabled, redirect all Contact Center Manager Administration client web browsers to use the managed name of the server where CCMA is installed.

If you have a High Availability campus solution, Avaya recommends that you log in to the CCMA web client using the managed name of the active server. If an active application or server fails, the CCMA client web browser continues to use the managed name and you can continue working without interruption.

Important:

Do not type the real or managed IP address because this results in problems with Scripting, Historical Reporting, Configuration, Contact Center Management, and Access and Partition Management.

Before you begin

- Configure High Availability on the Active and Standby servers.
- Change the server details in CCMA.
- Ensure that you have the user ID and password to log in to CCMA.
- To access CCMA and other Contact Center applications, ensure that you are using Microsoft Edge in Internet Explorer mode.

Procedure

1. In your web browser, type the URL of the CCMA server managed name.

   For example, type `https://<server name>`, where <*server name*> is the managed name of the High Availability server pair. If you turned off Web Services security, type `http://<server name>`.

2. In the **User ID** field, type your user ID.
3. In the **Password** field, type your password.
4. Click **Login**.

Testing switchovers

Before you begin

- Configure High Availability on the Active and Standby servers.

About this task

Test the High Availability feature and infrastructure by making a manual switchover from the Active server to the Standby server.

Procedure

1. Log on to the current Active Server.
2. On the **Desktop** screen, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Manual Switchover**.

3. Make a call using the CCT Reference Client to test the Standby Server configuration, when the Standby Server becomes the new Active Server.

   For more details, see Verifying CCT using Reference Client on page 190.

4. Send a test email to one of the CCMM configured mailboxes.

   After the email is received on the new Active Server, the test is successfully completed.

Next steps

Avaya recommends that you analyze your network performance after running HA for a number of days. Use the Network Analyzer utility to analyze the SMMC logs and verify whether your Network Timeout value is set correctly for your network performance. For more information about using the Network Analyzer utility to optimize the High Availability configuration settings on network, see *Troubleshooting Avaya Aura® Contact Center*.

A network outage triggers a switchover. There are test scenarios you can use to trigger a network outage, for example:

- A physical NIC cable break. This applies when Avaya Aura® Contact Center is installed on a physical server or on a virtual machine.
- Disconnecting the virtual NIC of an Avaya Aura® Contact Center virtual machine.

Chapter 23: Remote Geographic Node High Availability Voice and Multimedia Contact Server commissioning

This section describes how to configure geographic High Availability resiliency for Voice and Multimedia Contact Servers in an Avaya Aura® Communication Manager and an Avaya Aura® Session Manager based contact center. Avaya Aura® Contact Center geographic High Availability supports data resiliency and disaster recovery.

You must complete all the procedures in this section in sequential order.

In geographic Wide Area Network solutions the standby server on the remote geographic site is called a Remote Geographic Node server. The active server and the Remote Geographic Node server are part of the same Avaya Aura® Contact Center solution but they are typically in different geographic locations and subnets.

The active server can also have a local standby server in the same campus location. The standby server shadows the active server. If the active server fails the local standby server takes over call processing on the local site. The active server need not have a standby server. Avaya Aura® Contact Center supports an active server with a Remote Geographic Node server and without a standby server. This chapter assumes that if your solution has campus HA, campus HA commissioning is complete.

The Remote Geographic Node (RGN) server on the remote site shadows the server on the campus site, maintaining a near real-time local copy of the active server databases. Therefore, the RGN server is configured with the most recent data and it can take over if the campus site fails. Where the campus site has High Availability, the RGN server shadows the active server on the campus site, using the Managed IP address.

Remote Geographic Node server commissioning overview:

In a geographic Voice and Multimedia Contact Server HA configuration, there is an active server and a Remote Geographic Node server. The active Voice and Multimedia Contact Server actively processes scripts and contacts and records statistics. The Remote Geographic Node server shadows the active server. The Remote Geographic Node server does not automatically take over if the active system fails. You must start the Remote Geographic Node server manually. The Remote Geographic Node and active servers must have the same patch level and the same hard disk drive partitions.

High Availability Utility:

Configure High Availability resiliency for CCMS, CCMA, CCT and CCMM using the High Availability (HA) Utility in the Database Utilities. Use the High Availability Utility to configure which server is the active and which is the Remote Geographic Node server. Where the campus site has High Availability, the HA utility also configures the campus standby server details and the Managed IP address of the campus HA pair.

The High Availability Utility on an active server has the following dialogs under the Configuration tab:

- Server Mode
  - Configure the IP address for the active and standby servers
  - Configure the IP address for Trusted servers
  - Configure the IP address for the optional Remote Geographic Node
  - Identify if the server is active, standby, Remote Geographic Node, or Non HA
  - Enable Switchover
  - Configure the switchover time-out. This is the wait time if a network outage occurs before an automatic switchover occurs
  - Temporally set as Non-HA
- Notifications
  - Configure an email server for email notifications
  - Configure where and how often to send email notifications
  - Configure the email character set
- System
  - Display information on the system status
  - Verify that database shadowing is running

SMMC system tray:

The Contact Center System Management and Monitoring Component (SMMC) system tray gives quick access to action items in your High Availability environment, for example:

- Start HA System
- Stop HA System
- Disable Switchover
- Enable Switchover
- System Information
- Database Information
- Disable Next Auto Startup
- Select standby Auto Startup Mode (standby server only)

- Re-enable HA system (this option is available only when the active HA server is running but switchovers are disabled)

Note:

These action items appear depending on the system state. For example, the Disable Switchover and Enable Switchover items never appear simultaneously.

To access the SMMC system tray menu, right-click the SMMC icon on the Windows taskbar.

High Availability Utility and SMMC system tray:

Use the High Availability Utility to configure High Availability IP addresses and to configure which server is the active server and which is the standby server. Then use the System Management and Monitoring Component (SMMC) system tray to start database shadowing and High Availability functionality.

Prerequisites

- The active and Remote Geographic Node servers must meet the planning and engineering specifications. For more information, see *Avaya Aura® Contact Center Overview and Specification*.
- Ensure unused Network Interface Cards (NICs) are disabled.
- The Voice and Multimedia Contact Server is installed on the active and Remote Geographic Node servers using the same drive specification on each server.
- CCMS is configured on the active server. For more information, see Contact Center Manager Server commissioning on page 49.
- Ensure the third-party networking utility is installed. For more information, see Installing the third-party networking utility on page 56.
- CCMA is configured on the active server. For more information, see Contact Center Manager Administration commissioning on page 100.
- CCT is configured on the active server. For more information, see Communication Control Toolkit commissioning for SIP-enabled Contact Center on page 183.
- CCMM is configured on the active server. For more information, see Contact Center Multimedia commissioning on page 192.
- The active server in the campus site is installed and commissioned. If you are using High Availability at the campus site, the standby server is installed and commissioned
- You have a valid standby server license file on the active server and the Remote Geographic Node server. If you are using Avaya WebLM server instead, you have installed an Avaya WebLM server virtual guest at the campus and another Avaya WebLM server virtual guest at the remote site, and generated and applied the correct license files.
- Ensure the Voice and Multimedia Contact Server is on a domain. This is to allow the CCT clients to automatically re-connect after a switchover.

- Add the RGN CCMS and CCMM as servers in CCMA.
- Ensure the Remote Geographic Node server IP addresses are configured in CCMM General Administration on the active server. For more information, see Configuring CCMM General Administration on page 257.
- Before you commission High Availability, use System Control and Monitoring Utility (SCMU) to shut down all CCMS and CCT services on both the active and Remote Geographic Node servers.

High Availability commissioning checklist

The following is a list of key configuration items required for High Availability commissioning in a SIP-enabled contact center environment.

Item	Your value	Description
Ensure that Contact Center is licensed for High Availability		High Availability is a licensed feature and is enabled when you purchase a standby server license.
Active server host name		The name of your AACC active server.
Active server IP address		The IP address of your AACC active server.
Standby server host name		If you have HA at the campus site, the name of your AACC standby server.
Standby server IP address		If you have HA at the campus site, the IP address of your AACC standby server.
Managed name		If you have HA at the campus site, the managed name of your AACC campus HA pair.
Managed IP address		If you have HA at the campus site, the managed IP address of your AACC campus HA pair.
Using Hosts file or DNS?		If you are using the Hosts files to resolve Managed names to Managed IP addresses, ensure that you add the Managed names and Managed IP addresses to the Hosts file.
Trusted IP address		Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.

Table continues…

Item	Your value	Description
RGN server host name		If you have HA geographic redundancy, the name of your AACC RGN server.
RGN server IP address		If you have HA geographic redundancy, the IP address of your AACC RGN server.
Using email notification?		You can enable automatic email switchover notifications to alert the Contact Center administrator. When enabled, the specified email address receives an automatic email which provides switchover information to the recipient.
SMTP server name		The name of your SMTP server for email notification after an automatic switchover occurs.
Email Username		The log on name of an email user configured on the email server.
Email Password		The password of an email user configured on the email server.
Email address to send notifications from		The email address that the email notification is sent from.
Email address to send notifications to		The email address that the email notification is sent to.
Database backup location		The location of the shared folder where you store database backups. This folder must not be on the active or standby servers.

Resolving the Managed name to the Managed IP Address

About this task

Complete the following procedure to resolve the Managed server name to the Managed IP address. If the server has two network interfaces, apply these settings to the CLAN network interface. Each Contact Center server in a domain requires a DNS static entry.

Important:

Avaya Aura® Contact Center High Availability solutions do not support Dynamic DNS.

Ask your System Administrator to add a Domain Name System (DNS) static entry for the active and standby servers and one additional DNS static entry for the each Managed name and associated Managed IP address.

In High Availability solutions, the managed IP address must be lower than the active and standby server IP addresses. For example, if the active server IP address is 1.2.3.4 and the standby server IP address is 1.2.3.5, the managed IP address is 1.2.3.3.

A typical High Availability campus solution with a pair of servers requires 3 DNS static entries; one DNS static entry for the active server, one DNS static entry for the standby server, and one DNS static entry for the Managed name and associated IP address.

If your solution is going to have a Remote Geographic Node, ask your System Administrator to add a Domain Name System (DNS) static entry for the Remote Geographic Node server.

Perform this procedure on the Active server. Perform this procedure on the Standby server if you have one. Perform this procedure on the Remote Geographic Node server if you have one.

Procedure

1. Open Windows Explorer.
2. Go to the folder C:\Windows\system32\drivers\etc.
3. Double-click on the **hosts** file, select **Open**, and select **Notepad**.

   The hosts file opens in Notepad.
4. Add the Managed IP address and the Managed server name to the hosts file.

   Important:

   The Managed name can be a full name or netbios server name.

Verifying services are ready for configuring High Availability

About this task

Verify that all Contact Center services stop before you configure High Availability. This ensures that all resources are available to the active server when it starts.

Perform this procedure using the System Management and Monitoring Component (SMMC) on the active server.

Procedure

1. Log on to the active server.
2. On the **Desktop** screen, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **Stop System**.

Configuring geographical redundancy on the active server

About this task

Configure High Availability geographical redundancy on the active server using the High Availability Utility. The active server is the server that normally processes contacts.

Procedure

1. Log on to the active server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Configuration**.
4. Click **Server Mode**.
5. Under **Server Mode**, select **Active (Campus)** if you have HA at the campus site or select **Active (RGN)** if you do not have HA at the campus site.
6. Under **IP Configuration**, in the **Active CLAN** box, type the IP address for the active server.
7. In the **Standby CLAN** box, type the IP address for the standby server if you have HA at the campus site.
8. In the **Managed IP** box, type the managed IP address.
9. In the **Trusted IP** box, type the managed IP address.
10. In the **Remote Geographic Node** box, type the IP address of the Remote Geographic Node.
11. Click **Save**.

Variable definitions

Name	Description
Active CLAN	The IP address for the server initially configured in active mode.
Standby CLAN	The IP address for the server initially configured in Standby mode.
Managed IP	The virtual Managed IP (MIP) address that is used by the active server for campus resiliency. A MIP is used only when the Active and Standby servers are in the same subnet.
Trusted IP	Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.
Remote Geographic Node	The IP address of the Remote Geographic Node.
Local SMMC Port	The port number for System Management and Monitoring Component (SMMC) on the active server. The default port number is 57012.
Remote SMMC Port	The port number for System Management and Monitoring Component (SMMC) on the RGN server. The port number entered here must match the port number set on the active server. The default port number is 57012.

Backing up the database on the active server

About this task

The active server is configured for High Availability. Now the Remote Geographic Node server must be prepared for High Availability resiliency. Back up the active server to create a snapshot of the database which you can restore to the Remote Geographic Node server. On the active Voice and Multimedia Server, you must back up all the databases.

Important:

Do not use a folder on the active or standby servers as the backup location.

Procedure

1. Log on to the active server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. Click **Backup Locations**.
4. Click **Create**.
5. From the **Drive Letter** list, select the network drive on which you want to store the CCMS, CCT, CCMM, ADMIN, CCMA, and Offline databases.
6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Backup Location. This location must be a shared folder with correct permissions.
7. In the **User Name** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the Windows password.
9. Click **Save**.
10. In the left pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Application** section, select **Offline**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.

Configuring RGN CCMM General Administration

About this task

Configure the Remote Geographic Node (RGN) CCMM to use local telephony and multimedia resources.

Important:

Changes to the RGN CCMM settings might require an RGN server restart before they take effect.

Procedure

1. In Contact Center Manager Administration, from **Launchpad**, select **Configuration** .
2. Add the RGN Contact Center Multimedia as a CCMM server.
3. From **Launchpad**, select **Multimedia**.
4. In the left column, click the RGN Multimedia server.
5. Click **Launch Multimedia Client**.
6. In the left column, select **General Administration**.
7. Click **Server Settings**.
8. Change the **Contact Center Manager Server** entry to the IP address or name of the Remote Geographic Node Voice and Multimedia Contact Server.
9. Change the **Contact Center License Server** entry to the IP address or name of the Remote Geographic Node Voice and Multimedia Contact Server.
10. Change the **Contact Center Manager Administrator** entry to the IP address or name of the Remote Geographic Node Voice and Multimedia Contact Server.
11. Change the **Contact Center Multimedia Server** entry to the IP address or name of the Remote Geographic Node Voice and Multimedia Contact Server.
12. Change the **Geographic Standby CCMM Server** entry to not configured.
13. Change the **Communication Control Toolkit Server** entry to the IP address or name of the Remote Geographic Node Voice and Multimedia Contact Server.
14. Change the **Standby CCT Server** entry to not configured.
15. Change the **Geographic Standby CCT Server** entry to not configured.
16. Configure the **CC Web Stats** entry.

    If the Contact Center Web Statistics Server details do not exist and your solution uses Web Statistics, click **New**. The default port number is 9086.
17. In the left column, select **Email**.
18. Click **General Settings**.
19. Ensure that the Inbound URL is of the form `http://<RGNIPAddress>/inboundattachment`, where *RGNIPAddress* is the IP address of the Remote Geographic Node Voice and Multimedia Contact Server.
20. Ensure that the Outbound URL is of the form `http://<RGNIPAddress>/outboundattachment`, where *RGNIPAddress* is the IP address of the Remote Geographic Node Voice and Multimedia Contact Server.

Configuring the Remote Geographic Node local resources

About this task

Configure the Remote Geographic Node (RGN) resources to allow the remote site to function as a standalone contact center if the campus site fails. To perform this procedure, Contact Center services must be running.

When High Availability shadowing is enabled, the RGN server shadows some of the configuration data from the campus site.

The RGN server does not shadow (replicate) information about the following resources from the campus site:

- Media Server and Media Services
- Default DN

On the RGN server, you must configure these resources to use local Avaya Aura® Media Servers and attendants.

Configure a Default DN to catch treated calls that are defaulted by the contact center script and to catch calls not answered by agents. Avaya recommends that you configure a local attendant at the RGN site as the Default DN.

Avaya Aura® Contact Center uses Avaya Aura® Media Server (MS) media processing capabilities to support conferencing, announcements, and dialogs. Configure each Avaya Aura® MS in at the RGN site as a Media Server. Contact Center uses the media processing capabilities of Avaya Experience Portal to support external Interactive Voice Response (IVR) dialogs (XDIALOG). If your RGN site uses local Avaya Experience Portal servers, add these here as Media Servers and configure them to provide external dialog (XDIALOG) services.

Procedure

1. Start Contact Center services on the RGN server.
2. On the RGN server, log on to Contact Center Manager Administration.
3. On the **Launchpad**, click **Configuration**.
4. In the left pane, expand the RGN Contact Center Manager Server on which to configure global settings.
5. Select the **Global Settings** folder.
6. Configure the global settings for your system based on the fields listed in the **Global Settings** window.
7. In the **Default DN** box, type the default DN to use when a script defaults or a treated call is not answered. Avaya recommends that you configure an attendant as the Default DN.
8. Click **Save**.
9. In the left pane, expand the RGN Contact Center Manager Server on which to configure a media server. Ensure that you select the local RGN CCMS server, not a campus server.
10. Select the **Media Servers** folder.

11. In the right pane, in the **Server Name** box, type the name of the Avaya Aura® MS server.
12. In the **IP address** box, type the IP address of the Avaya Aura® MS server.
13. In the **Port Number** box, type the port number for the Avaya Aura® MS server. The port number must match the Avaya Aura® MS port number. The default is 5060.
14. If the Avaya Aura® MS is going to manage prompts, select the **Master Content Store**. Avaya Aura® MS supports only one Master Content Store.
15. Click any other row in the table to save the changes.
16. In the left pane, expand the RGN Contact Center Manager Server on which to configure a media services.
17. Select the **Media Services and Routes** folder.
18. On the **Media Services & Routes** table, select a media service. For an Avaya Aura® MS, select **ACC_APP_ID**.
19. From the **Available** list, select an Avaya Aura® MS to associate with the selected conference media service.
20. Click the right arrow (>).

    The server moves to the **Selected** list.
21. Repeat step 8 on page 287 to step 20 on page 288 for each Avaya Aura® MS installed on the Remote site.
22. If you add more than one Avaya Aura® MS, use the up and down **Rank** arrows to order the selected servers.
23. Click **Submit**.
24. Stop Contact Center services on the RGN server.

Configuring High Availability on the Remote Geographic Node server

About this task

Configure High Availability resiliency on the Remote Geographic Node server using the High Availability utility. The Remote Geographic Node Server shadows the active server.

Procedure

1. Log on to the Remote Geographic Node server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Configuration**.
4. Click **Server Mode**.

5. Under **Server Mode**, select **RGN**.
6. If you do not have HA at the campus site, in the **Campus CLAN** box, type the IP address for the campus active server.
7. If you have HA at the campus site, in the **Campus CLAN** box, type the Managed IP address for the campus server pair.
8. Under **IP Configuration**, in the **RGN CLAN** box, type the IP address for the Remote Geographic Node server.
9. Ensure that the **Managed IP** box is empty.
10. Under **IP Configuration**, in the **Trusted IP** box, type the IP address of a trusted server.
11. Under **SMMC Port Configuration**, in the **Remote SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the campus active server.
12. Under **SMMC Port Configuration**, in the **Local SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the RGN server.
13. Click **Save**.
14. On the **High Availability** dialog box, click **OK**.

    Do not reboot the server at this point.

Variable definitions

Name	Description
Campus CLAN	If you do not have HA at the campus site, type the IP address of the campus active server. If you have HA at the campus site, type the virtual Managed IP address that is used by the campus server pair. The RGN server monitors the Managed IP address of the campus site. If the active server on the campus site fails, the standby server assumes the managed IP address and continues processing. The RGN server continues shadowing from this IP address.
RGN CLAN	The IP address for the Remote Geographic Node server.
Trusted IP	The IP address of a trusted server that is not likely to fail, so that both active and RGN servers have a server to ping regularly to verify the network connection. Avaya recommends that you use an IP address from your IT infrastructure as the Trusted IP address.

Table continues…

Name	Description
Local SMMC Port	The Network Management port number for System Management and Monitoring Component (SMMC) on the RGN server. The default port number is 57012.
Remote SMMC Port	The Network Management port number for System Management and Monitoring Component (SMMC) on the campus active server. The port number entered here must match the port number set on the campus active server. The default port number is 57012.

Restoring the database on the Remote Geographic Node server

Before you begin

- Know the location of the backup database.
- For a faster database restore, copy the active database backup to a network share that is local to the Remote Geographic Node (RGN) server.
- Using the Database maintenance utility, create a backup location on the RGN server that references the location of database backup to be restored.
- Stop all Contact Center services, if services are running.
- Ensure the patch level on the RGN server is the same as the active server.

Important:

Not all CCT data is stored in the database. The following data must be configured on the Remote Geographic Node server: CCT SOA configuration (CCT Web Services), and CCT logging location.

Important:

You must restore all databases on a Voice and Multimedia Contact Server. Restoring only CCMS and not CCT, CCMM, ADMIN, or CCMA might leave an inconsistent server and HA cannot shadow data correctly.

Important:

Restoring the ADMIN database can change configuration of backup locations on the RGN server if the active server and RGN server backup locations are different. Therefore, after you restore the ADMIN database, close and reopen the Database Maintenance utility.

About this task

Restore the database from the active server to the Remote Geographic Node server to ensure the databases are consistent. The Database Maintenance utility can restore all application databases at once. Restore the data for the CCMS, CCT, CCMM, ADMIN, and CCMA databases.

You must restore the CCMS, CCT, CCMM, ADMIN, and CCMA database onto the Remote Geographic Node server.

Procedure

1. Log on to the Remote Geographic Node server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. In the **Database Maintenance** dialog box, in the left pane, click **Restore**.
4. In the right pane, under **Media Type**, select the media type on which the backup is restored.
5. If the backup file is on the network drive, in the **Backup Location** list, select the backup location.
6. Under **Application**, select CCMS, CCT, CCMM, ADMIN, and CCMA.
7. Under **Restore contents**, select **Data** and **Offline**.
8. Click **Restore**.
9. Use the **Information** field to monitor the progress of the restoration.
10. When the restore completes, click **OK**.
11. Click **Exit** to close the Database Maintenance utility.

Variable definitions

Name	Description
Application	The database and applications of Contact Center that you can back up.
Backup Location	The destination of the network disk. The values are configured in the Backup Locations.
Restore contents	The type of content that is stored in the database. Data is in the database. Schema is the data for the database structure, tables and procedures.
Media type	The type of media used for your backup file. You can use a network disk location or a tape drive. If you use a network disk location, you must configure a destination before you can back up the file.

Configuring server details on the Remote Geographic Node

About this task

Configure the Remote Geographic Node server with server details that do not replicate from the active server.

Important:

Changes to the SIP Local Subscriber data require an Avaya Aura® Contact Center restart.

Procedure

1. Log on to the Remote Geographic Node server.
2. From the **Start** menu, in the Avaya area, click **Server Configuration**.
3. In the **Server Configuration** dialog box, click the **Local Settings** tab.
4. Update the Remote Geographic Node server local settings.
5. On the **Restart Required** dialog, click **No**.
6. In the **Server Configuration** dialog box, click the **Licensing** tab.
7. Update the Remote Geographic Node server licensing details.
8. On the **Restart Required** dialog, click **No**.
9. In the **Server Configuration** dialog box, under **SIP**, click the **Network Settings** tab.
10. Update the Remote Geographic Node server **SIP Network Settings** details. Ensure the Avaya Aura® Contact Center RGN server is configured to use a local RGN Avaya Aura® Unified Communications platform.
11. On the **Restart Required** dialog, click **No**.
12. In the **Server Configuration** dialog box, under **SIP**, click the **Local Subscriber** tab.
13. Update the Remote Geographic Node server **SIP Local Subscriber** details.
14. Click **Apply All**.
15. On the **Restart Required** dialog, click **Yes**.
16. Click **Exit**.

Variable definitions

Name	Description
Avaya Server Subnet IP Address	The IP address of the subnet that connects the Contact Center servers (Contact Center Manager Server, Network Control Center, Contact Center Manager Administration, and Contact Center Multimedia).
Voice Proxy Server • IP Address • Port • Network Transport	Information about the server that provides support for inbound and outbound calls, such as routing a call to an agent telephone. If the contact center uses an Avaya Aura® Session Manager, enter the IP address for the primary Session Manager here. The server listening port. The default port is 5060.
CTI Proxy Server • IP Address • Port • Network Transport • Port • Network Transport	Information about the server that provides support for SIP Computer Telephony Integration (CTI) so that Agent Desktop can acquire and control agent telephones for TR87. Enter the IP address of the Avaya Aura® Application Enablement Services server. For an Application Enablement Services server the default SIP CTI Proxy Server port is 4723. The SIP Network Transport communication protocol. For an Application Enablement Services server, the default Network Transport communication protocol is TLS. The server listening port. The default port is 5060. The Backup Voice Proxy Server transport protocol.
IM Proxy Server • IP Address • Port • Network Transport	Information about the server that supports the deployment of Instant Message over SIP. The IP address of the SIP IM Proxy Server. The default SIP IM Proxy Server port is 5222. The IM SIP Proxy Server transport protocol.
IM Provider	Select your IM Provider, Aura Presence Services or Microsoft Lync (for Microsoft Skype for Business, select Microsoft Lync).
XMPP Domain	If using an Avaya Aura® Presence Services server, enter the domain name of the Extensible Messaging and Presence Protocol (XMPP) server.

Table continues…

Name	Description
Local SIP Subscriber • Contact Center Name • Domain Name	Information about the environment of the SIP-enabled contact center and how to identify the server within the network. The registration user name on the registration proxy. Use a suitable user name following the standards in your system. Associated domain name for the SIP- enabled contact center.
Web Service Ports	The Web Service Ports group box appears only if you select Avaya Aura® Presence Services as the IM Provider. Server Port default is 9100 Client Port default is 9120
SIP Server Type	Type of SIP proxy for the contact center integration. Depending on the switch type you select in the Application Selection window, the system automatically sets the specific SIP Server Type as the default.
MS Locale	Locale (including language and dialects) of the system environment.
Local Listening Ports	The SIP Communication protocol accepted by the system for incoming calls. TCP/UDP Port default is 5060 TLS Port default is 5061

Starting the active server

About this task

Start the active server using the System Management and Monitoring Component (SMMC) system tray. Starting the active server starts Contact Center services and system processes.

Procedure

1. Log on to the active server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Configuration**.
4. Under **Switchover And Network Timeout Configuration**, select **Enable Switchover**.
5. Click **Save**.

6. On the **Desktop** screen of the active server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start HA System**.
7. From the **Start** menu, in the Avaya area, click **System Control and Monitor Utility**.
8. Verify that the Contact Center services are running.

Starting shadowing on the standby server

About this task

Start shadowing on the standby server using the System Management and Monitoring Component (SMMC) system tray.

The Standby server shadows the active server, maintaining a near real-time local copy of the Contact Center applications and Administration databases. Therefore, the standby server is configured with the most recent data and it can take over from the active server if necessary.

Important:

You must backup the active server database, restore it onto the standby server, and enable shadowing within 24 hours. If the difference in time between the active and standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the active server database and restore it onto the standby server before re-enabling shadowing. Ensure that the system clock times on the active and standby servers are synchronized.

Procedure

1. Log on to the standby server.
2. On the **Desktop** screen of the standby server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start HA System**.
3. From the **Start** menu, in the Avaya area, click **System Control and Monitor Utility**.
4. Check that the Contact Center services are running.

   Note:

   The following services do not start on the standby server:

   - CCMS_MasterService
   - CCMA - IceRTDService
   - CCMM - EmailManager, MCMC, CCMMOAM, Campaign Scheduler Service

Starting shadowing on the Remote Geographic Node Server

About this task

Start shadowing on the Remote Geographic Node (RGN) server using the System Management and Monitoring Component (SMMC) system tray.

The RGN server shadows the campus active server, maintaining a near real-time local copy of the Contact Center applications and Administration databases. The Remote Geographic Node server is therefore configured with the most recent data.

Important:

You must backup the active server database, restore it onto the RGN server, and enable shadowing within 24 hours. If the difference in time between the active and standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the active server database and restore it onto the RGN server before re-enabling shadowing. Ensure that the system clock times on the active and standby servers are synchronized.

Procedure

1. Log on to the Remote Geographic Node server.
2. On the **Desktop** screen of the standby server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start HA System**.
3. From the **Start** menu, in the Avaya area, click **System Control and Monitor Utility**.
4. Verify that the Contact Center services are **Shut down**. On an RGN server, Contact Center services are shut down while the RGN database shadows the active database. You must manually start an RGN server if required, there is no automatic switchover if the campus site fails.

Verifying the Voice and Multimedia Contact Server RGN settings

About this task

Verify the Voice and Multimedia Contact Server Remote Geographic Node (RGN) settings. The RGN server must be available and manually enabled to take over if the campus site fails.

Procedure

1. Log on to the active server.
2. Log on to the CCMA Web client. If you have HA at the campus, use the managed name.
3. On the Launchpad, select **Configuration**.

4. Ensure the list of servers in the left hand pane includes only the campus CCMS, CCT and CCMM server details. Remove any RGN server listings from the left hand pane.
5. From the server list, select the CCMS server. If you have HA at the campus, use the managed name.
6. On the CCMS server, select **Refresh Server**.
7. Ensure the **Remote Geographic Node** section displays the **RGN Server Name** and **RGN Server IP** of the Voice and Multimedia Contact Server RGN server.

Verifying Voice and Multimedia High Availability is running

About this task

Using the High Availability Utility, verify that the Remote Geographic Node (RGN) server is shadowing the active server. The System dialog box of the High Availability utility displays system information about the active and the Remote Geographic Node servers.

The dialog box displays the followings information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information
- Remote server connection status
- Remote server port information
- License information
- Databases shadowed
- Time of last record shadowed
- Database namespaces
- Local and remote information on system status, switchover, shadowing and network
- CC Application install information
- Database space and journaling information
- Database processes information

Procedure

1. Log on to the active server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. In the left pane, expand **Configuration**.
4. Select **System**.

5. Select **Get System Configuration**.

   The most recent system information appears.

Example

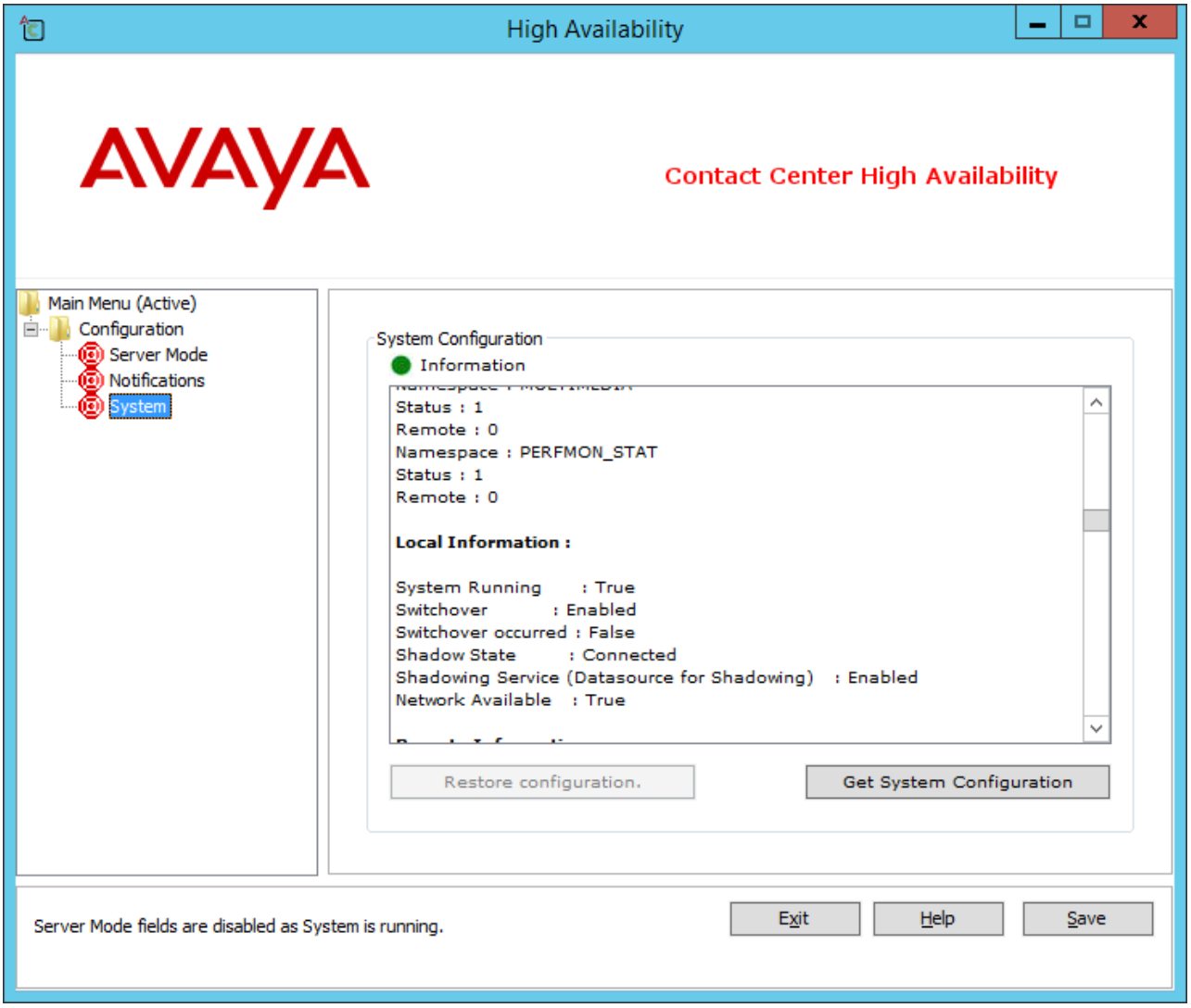


Figure 33: Example of an active server with the HA system running

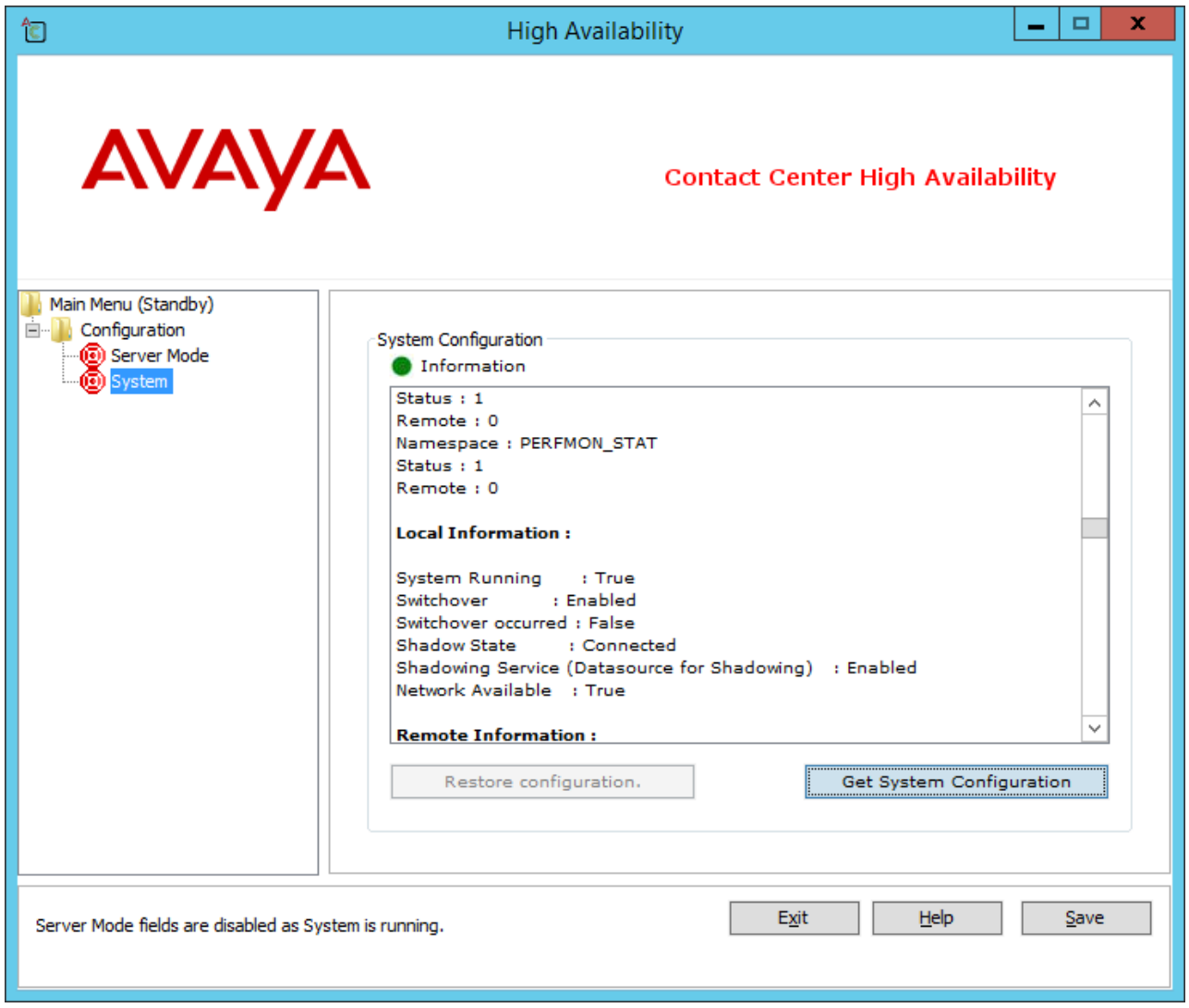


Figure 34: Example of an standby server with the HA system running

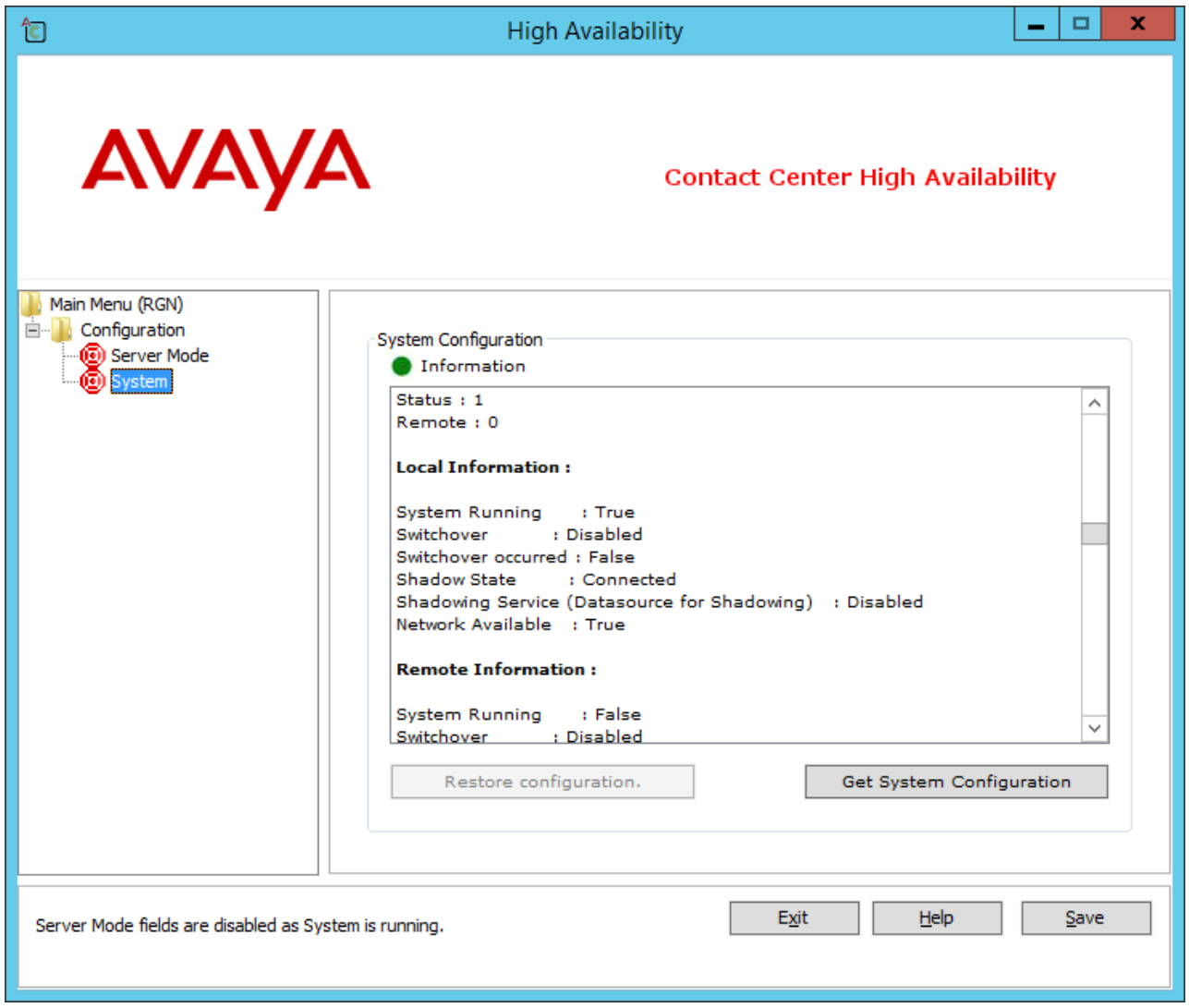


Figure 35: Example of an Remote Geographic Node server with the HA system running

Note the **Server Mode fields are disabled as System is running** notice on the HA user interface.

Chapter 24: Mission Critical High Availability Voice Contact Server commissioning

This section describes how to configure Mission Critical High Availability (HA) resiliency for a pair of Voice Contact Servers, which include Contact Center Manager Server (CCMS) and Communication Control Toolkit (CCT), in a campus SIP-enabled contact center environment. Avaya Aura® Contact Center Mission Critical High Availability is supported with three different Contact Center solutions running on the Avaya Aura® Unified Communications platform. Mission Critical High Availability is supported in a campus SIP-enabled contact center environment that uses:

- An Avaya Aura® Communication Manager and an Avaya Aura® Session Manager.

  OR

- Two Avaya Aura® Solution for Midsize Enterprise servers, configured for High Availability.

You must complete all the procedures in this section in sequential order.

Mission Critical High Availability campus overview:

In a Voice Contact Server HA configuration, one server is the active server and one is the standby server. The active Voice Contact Server actively processes scripts and contacts and records statistics. The standby server shadows the active server. The standby server copies all configuration changes made on the active server and monitors the active server status. If the active server fails, the standby server, running in Mission Critical standby mode, recognizes the failure and starts processing contacts. After the switchover, High Availability is disabled on the original active server.

The active and standby servers are part of the same Avaya Aura® Contact Center and they must be in the same subnet IP address range for campus High Availability resiliency to work.

The standby server must be configured the same as the active server. The standby and active servers must have the same patch level and the same hard disk drive partitions. Configuration changes made to the active server during normal operation are automatically copied to the standby server so that the standby server can take over processing from the active server when necessary.

In a Mission Critical campus High Availability solution, a CCMS or CCT service failure, hardware, network, or database failure can initiate a switchover but only in the following situations:

- The active server is in the active mode.
- The active server is running. All the critical CCMS and CCT services are running.

- The active server has Enable Switchover enabled.
- The active and standby servers can communicate with the trusted server.
- The active server database and standby server database are synchronized. The standby server database is shadowing the active server database, and the critical services are running on the standby server.

If the Contact Center Administrator uses the Windows Service Control Manager (SCM) to stop a monitored service on an Active server, a switchover occurs.

If a critical service on the Standby server stops or is stopped, the Standby server stops all services and the contact center solution is no longer resilient. To reinstate High Availability resiliency, use SMMC to “Start HA System” on the Standby server.

High Availability Utility:

Configure High Availability resiliency for CCMS and CCT using the High Availability (HA) Utility in the Database Utilities. The High Availability Utility is used to configure which server is the active and which is the standby server. The HA utility also configures the Managed IP of the active server.

The High Availability Utility on an Active Server has the following dialogs under the Configuration tab:

- Server Mode
  - Configure the IP address for the Active and Standby servers
  - Configure the IP address for Trusted servers
  - Configure the IP address for the optional Remote Geographic Node
  - Identify if the server is Active, Standby, Remote Geographic Node, or Non HA
  - Enable Switchover
  - Configure the switchover time-out. This is the wait time if a network outage occurs before an automatic switchover occurs
  - Temporally set as Non-HA
- Notifications
  - Configure an email server for email notifications
  - Configure where and how often to send email notifications
  - Configure the email character set
- System
  - Display information on the system status
  - Verify that database shadowing is running

SMMC system tray:

The Contact Center System Management and Monitoring Component (SMMC) system tray gives quick access to action items in your High Availability environment, for example:

- Start HA System
- Stop HA System
- Disable Switchover
- Enable Switchover
- System Information
- Database Information
- Disable Next Auto Startup
- Select Standby Auto Startup Mode (Standby server only)
- Re-enable HA system (this option is available only when the active HA server is running but switchovers are disabled)

To access the SMMC system tray menu, right-click the SMMC icon on the Windows taskbar.

High Availability Utility and SMMC system tray:

Use the High Availability Utility to configure High Availability IP addresses and to configure which server is the active server and which is the standby server. Then use the System Management and Monitoring Component (SMMC) system tray to start database shadowing and High Availability functionality.

Determining the High Availability Network Timeout threshold:

The level of Contact Center application High Availability you achieve depends on your complete enterprise contact center solution, including the underlying network infrastructure.

It is important that you determine the optimum High Availability SMMC Network Timeout threshold value for your contact center network. If the threshold is set too high, High Availability might not recognize network outages, switchovers might not occur when necessary and call control might be lost. If the threshold is set too low, frequent and unnecessary switchovers might occur.

SMMC tests network connectivity between High Availability components and records the details of these connectivity tests in trace log files. The SMMC trace log files contain sufficient statistical data about SMMC communications in your network to characterize the networks behavior for a High Availability contact center solution. You can use this SMMC statistical communications data to optimize your High Availability solution.

Avaya recommends that you analyze the SMMC trace log file and use the connectivity test results in it to optimize the High Availability settings for your network. For more information about using the Network Analyzer utility to optimize the High Availability configuration settings on network, see *Troubleshooting Avaya Aura® Contact Center*.

Prerequisites

- Ensure the Avaya Aura® Unified Communications platform is installed and patched to support Avaya Aura® Contact Center High Availability.
- The active and standby servers must meet the planning and engineering specifications. For more information, see *Avaya Aura® Contact Center Overview and Specification*.
- Ensure unused Network Interface Cards (NICs) are disabled.
- The Voice Contact Server is installed on the Active and Standby servers using the same drive specification on each server.
- CCMS is configured on the Active Server. For more information, see Contact Center Manager Server commissioning on page 49.
- Ensure the third-party networking utility is installed. For more information, see Installing the third-party networking utility on page 56.
- CCMA is configured on the Active Server. For more information, see Contact Center Manager Administration commissioning on page 100.
- CCT is configured on the Active Server. For more information, see Communication Control Toolkit commissioning for SIP-enabled Contact Center on page 183.
- The Active and Standby Server have a valid standby server license file, or, if you are using Avaya WebLM server, you have installed two Avaya WebLM server virtual guests and generated and applied the correct license files.
- Ensure the Voice Contact Server is on a domain. This is to allow the CCT clients such as Avaya Agent Desktop to communicate with both servers.
- Commission the Switchover Handling script. For more information about the Switchover Handling script, see *Avaya Aura® Contact Center Overview and Specification*.
- Before you commission High Availability, use System Control and Monitoring Utility (SCMU) to shut down all CCMS and CCT services on both the active and standby servers.

High Availability commissioning checklist

The following is a list of key configuration items required for High Availability commissioning in a SIP-enabled contact center environment.

Item	Your value	Description
Ensure that Contact Center is licensed for High Availability		High Availability is a licensed feature and is enabled when you purchase a standby server license.
Active server host name		The name of your AACC active server.

Table continues…

Item	Your value	Description
Active server IP address		The IP address of your AACC active server.
Standby server host name		If you have HA at the campus site, the name of your AACC standby server.
Standby server IP address		If you have HA at the campus site, the IP address of your AACC standby server.
Managed name		If you have HA at the campus site, the managed name of your AACC campus HA pair.
Managed IP address		If you have HA at the campus site, the managed IP address of your AACC campus HA pair.
Using Hosts file or DNS?		If you are using the Hosts files to resolve Managed names to Managed IP addresses, ensure that you add the Managed names and Managed IP addresses to the Hosts file.
Trusted IP address		Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.
RGN server host name		If you have HA geographic redundancy, the name of your AACC RGN server.
RGN server IP address		If you have HA geographic redundancy, the IP address of your AACC RGN server.
Using email notification?		You can enable automatic email switchover notifications to alert the Contact Center administrator. When enabled, the specified email address receives an automatic email which provides switchover information to the recipient.
SMTP server name		The name of your SMTP server for email notification after an automatic switchover occurs.
Email Username		The log on name of an email user configured on the email server.
Email Password		The password of an email user configured on the email server.
Email address to send notifications from		The email address that the email notification is sent from.
Email address to send notifications to		The email address that the email notification is sent to.

Table continues…

Item	Your value	Description
Database backup location		The location of the shared folder where you store database backups. This folder must not be on the active or standby servers.

Resolving the Managed name to the Managed IP Address

About this task

Complete the following procedure to resolve the Managed server name to the Managed IP address. If the server has two network interfaces, apply these settings to the CLAN network interface. Each Contact Center server in a domain requires a DNS static entry.

Important:

Avaya Aura® Contact Center High Availability solutions do not support Dynamic DNS.

Ask your System Administrator to add a Domain Name System (DNS) static entry for the active and standby servers and one additional DNS static entry for the each Managed name and associated Managed IP address.

In High Availability solutions, the managed IP address must be lower than the active and standby server IP addresses. For example, if the active server IP address is 1.2.3.4 and the standby server IP address is 1.2.3.5, the managed IP address is 1.2.3.3.

A typical High Availability campus solution with a pair of servers requires 3 DNS static entries; one DNS static entry for the active server, one DNS static entry for the standby server, and one DNS static entry for the Managed name and associated IP address.

If your solution is going to have a Remote Geographic Node, ask your System Administrator to add a Domain Name System (DNS) static entry for the Remote Geographic Node server.

Perform this procedure on the Active server. Perform this procedure on the Standby server if you have one. Perform this procedure on the Remote Geographic Node server if you have one.

Procedure

1. Open Windows Explorer.
2. Go to the folder C:\Windows\system32\drivers\etc.
3. Double-click on the **hosts** file, select **Open**, and select **Notepad**.

   The hosts file opens in Notepad.
4. Add the Managed IP address and the Managed server name to the hosts file.

   Important:

   The Managed name can be a full name or netbios server name.

Configuring CCMM General Administration

About this task

Avaya Agent Desktop client software is typically downloaded from a Multimedia Contact Server. Agent Desktop then communicates with that Multimedia Contact Server to handle customer contacts. Agent Desktop also communicates with Communication Control Toolkit (CCT) to handle voice contacts.

In a High Availability solution, use the CCMM Administration tool to configure standby server details. Agent Desktop client software downloads these standby server details and communicates with these standby servers if it cannot communicate with the active Voice Contact Server and Multimedia Contact Server.

Important:

Before changes to the CCMM server settings take effect, you might need to restart the Multimedia Contact Server.

Procedure

1. Log in to the Contact Center Manager Administration application.
2. Click **Multimedia**.
3. In the left column, select **General Administration**.
4. Click **Server Settings**.
5. Configure the **Contact Center Manager Server** entry with the managed IP address of the Voice and Multimedia Contact Server High Availability pair.
6. Configure the **Contact Center License Server** entry with the managed IP address or managed name of the Voice Contact Server High Availability pair.
7. Configure the **Contact Center Manager Administration** entry with the managed name of the Voice Contact Server High Availability pair.
8. Configure the **Contact Center Multimedia Server** entry with the managed IP address or managed name of the Multimedia Contact Server High Availability pair.
9. If your solution has a Remote Geographic Node Voice Contact Server, enter its name or IP address in the **Geographic Standby CCMM Server** field.
10. Configure the **Communication Control Toolkit Server** entry with the IP address of your primary Voice Contact Server.
11. Configure the **Standby CCT Server** entry with the IP address of your standby Voice Contact Server.
12. If you are using a Remote Geographic Node server, configure the **Geographic Standby CCT Server** entry.

    Alternatively, if the Geographic Standby CCT Server does not exist, click **New** to create one.
13. Configure the **CC Web Stats** entry.

If the Contact Center Web Statistics Server details do not exist and your solution uses Web Statistics, click **New**. Use the managed IP address of the optional Web Statistics server. The default port number is 9086.

14. In the left column, select **Email**.
15. Click **General Settings**.
16. Ensure that the Inbound URL is of the form `http://<ManagedIPAddress>/inboundattachment`.
17. Ensure that the Outbound URL is of the form `http://<ManagedIPAddress>/outboundattachment`.

Verifying services are ready for High Availability

About this task

Verify that all services stop before you configure High Availability. This ensures that all resources are available to the Active Server when it starts.

Perform this procedure using the System Management and Monitoring Component (SMMC) on the Active and Standby servers.

Procedure

1. Log on to the Active Server.
2. On the **Desktop** screen, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **Stop System**.
3. Repeat this procedure on the Standby Server.

Configuring campus High Availability on the active server

About this task

Configure campus High Availability resiliency on the active server using the High Availability utility. The active server is the server that normally processes calls.

If you know the IP address of the Remote Geographic Node server, enter it now during campus configuration. The High Availability configuration utility user interface is disabled when the HA system is shadowing.

You must restart the server to apply the High Availability settings.

Procedure

1. Select one server to be the active server and log on.

2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Configuration**.
4. Click **Server Mode**.
5. Under **Server Mode**, select **Active (Campus)**.
6. Under **Switchover And Network Timeout Configuration**, select **Enable Switchover**.
7. Under **Switchover And Network Timeout Configuration**, in the **Network Timeout** box, type the maximum length of time the network connectivity tests can continue to fail consecutively before corrective action is considered.
8. Under **Switchover And Network Timeout Configuration**, from the drop down list, select the unit of time for the network connectivity tests.
9. Under **IP Configuration**, in the **Active CLAN** box, type the IP address for the active server.
10. Under **IP Configuration**, in the **Standby CLAN** box, type the IP address for the standby server.
11. Under **IP Configuration**, in the **Managed IP** box, type the managed IP address.
12. Under **IP Configuration**, in the **Trusted IP** box, type the IP address of a trusted server.
13. Under **SMMC Port Configuration**, in the **Local SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the local (active) server.
14. Under **SMMC Port Configuration**, in the **Remote SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the remote (standby) server.
15. Click **Save**.
16. Reboot the active server to apply the changes.

Variable definitions

Name	Description
Network Timeout	The High Availability feature tests network connectivity between HA components by default every 100 milliseconds (100ms). The High Availability—Network Timeout value sets the maximum length of time these network connectivity tests can continue to fail consecutively before corrective action is considered. The minimum Network Timeout value is 200 milliseconds (200ms) and the maximum Network Timeout value is 5 seconds. For example, if Network Timeout is set to 400ms, HA requires 4 consecutive failed network connectivity tests before the remote system is marked as unreachable. In this case, if switchovers are enabled, an attempt to switch over is made. Avaya recommends that you set Network Timeout high enough to be tolerant of normal network latency, but low enough to be responsive if a failure occurs.
Active CLAN	The IP address for the server initially configured in Active mode.
Standby CLAN	The IP address for the server initially configured in Standby mode.
Managed IP	The virtual Managed IP (MIP) address that is used by the Active Server for campus resiliency. A MIP is used only when the Active and Standby servers are in the same subnet.
Trusted IP	The Active and Standby servers use the Trusted IP address to verify network connectivity. If the Active server cannot communicate with the Standby server it attempts to communicate with the Trusted IP address. If the Active server cannot communicate with the Trusted IP address, if shadowing and switchover are enabled, then the Active server stops processing contacts and shuts down. The Standby server starts processing contacts if it cannot communicate with the Active server but can communicate with the Trusted IP address. Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.

Table continues…

Name	Description
Remote Geographic Node	The IP address of the optional Remote Geographic Node.
Local SMMC Port	The port number for System Management and Monitoring Component (SMMC) on the local (active) server. The default port number is 57012.
Remote SMMC Port	The port number for System Management and Monitoring Component (SMMC) on the remote (standby) server. The port number entered here must match the port number set on the remote (standby) server. The default port number is 57012.

Configuring email notification on the Active Server

Before you begin

- If anonymous users are allowed, a user name and password might not be required. Check with the Administrator of the email server for setup configuration.

About this task

If an automatic switchover occurs, the High Availability utility can send email messages to configured users at a defined interval.

The default email notification character set is US_ASCII. The following character sets are also supported:

- ISO-8859-1
- UTF-8
- UTF-16BE
- UTF-16LE
- UTF-16

Procedure

1. Log on to the Active Server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Configuration**.
4. Double-click **Notification**.
5. Select the **Email** check box.
6. Type the **SMTP Server** name.
7. Type the **Username**.
8. Type the **Password**.

9. Type the **From Address**.
10. Type the **To Address** or **Addresses**.
11. Click **Save** to save the data.

Variable definitions

Name	Description
Email	Enables or disables email notifications.
SMTP Server	The SMTP Server name, which is automatically verified when saving the data.
Username	Email User log on name.
Password	Email User log on password.
Charset	Email character set to use.
From Address	Email address to send notifications from.
To Address	Email address to send notifications to.

Backing up the database on the Active Server

About this task

The Active Server is configured for High Availability. Now the Standby Server must be prepared for High Availability resiliency. Back up the Active Server to create a snapshot of the database which is then restored to the Standby Server. On the active server all databases must be backed-up.

Important:

You must back up the Active server database, restore it onto the Standby server, and enable shadowing within 24 hours. If the difference in time between the Active and Standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the Active server database and restore it onto the Standby server before re-enabling shadowing. Ensure that the system clock time on the Active and Standby servers are synchronized.

Important:

Do not use a folder on the Active or Standby servers as the backup location.

Procedure

1. Log on to the Active Server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. Click **Backup Locations**.
4. Click **Create**.

5. From the **Driver Letter** list, select the network drive on which you want to store the CCMS, CCT and ADMIN databases.
6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Backup Location. This location must be a shared folder with correct permissions.

   Important:

   Do not use the same backup folder for your Voice Contact Server and Multimedia Contact Server databases, as ADMIN databases stored in the same backup location overwrite each other.
7. In the **User Name** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the Windows password.
9. Click **Save**.
10. In the left pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. From the **Backup Location** list, select the network drive on which to store the backup.
13. Click **Backup**.

Restoring the database on the standby server

Before you begin

- Know the location of the backup database. Copy the database backups onto the Standby server.
- Ensure no traffic is running on the standby server.
- Stop shadowing if shadowing is running on the standby server.
- Stop all Contact Center services using the SCMU utility, if services are running.
- Ensure the patch level on the standby server is the same as the active server.

Important:

Not all CCT data is stored in the database; therefore the following data must be configured on the standby server, CCT License, CCT Contact Management Framework, CCT SOA configuration (CCT Web Services), and CCT logging location.

Important:

You must restore all databases on a Voice Contact Server. Restoring only CCMS and not CCT, ADMIN, or CCMA, can leave an inconsistent server and HA cannot shadow data correctly.

Important:

Restoring the ADMIN database can change configuration of Backup locations on the standby server if the active server and standby server backup locations are different. Therefore, after you restore the ADMIN database, close and reopen the Database and Maintenance utility.

About this task

If you have HA at the campus, restore the database from the active server to the standby server to ensure the databases are consistent. The Database Maintenance utility can restore all application databases at once. You must restore the CCMS, CCT, ADMIN, and CCMA databases onto the standby server.

Important:

You must backup the active server database, restore it onto the standby server, and enable shadowing within 24 hours. If the difference in time between the active and standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the active server database and restore it onto the standby server before re-enabling shadowing. Ensure that the system clock times on the active and standby servers are synchronized.

Procedure

1. Log on to the standby server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. In the **Database Maintenance** dialog box, in the left pane, click **Restore**.
4. In the right pane, under **Media Type**, select the media type on which the backup is restored.
5. If the backup file is on the network drive, in the **Backup Location** list, select the backup location.
6. Under **Application**, select CCMS, CCT, ADMIN, and CCMA.
7. Under **Restore contents**, select **Data**.

   Important:

   Do not select **Offline**.
8. Click **Restore**.
9. Use the **Information** field to monitor the progress of the restoration.
10. Click **Exit** to close the Database Maintenance utility.

Variable definitions

Name	Description
Application	The database and applications of Contact Center that you can back up.
Backup Location	The destination of the network disk. The values are configured in the Backup Locations.
Restore contents	The type of content that is stored in the database. Data is data in the database. Schema (read only) is the data for the database structure, tables and procedures. Offline is the Multimedia Offline database.
Media type	The type of media used for your backup file. You can use a network disk location or a tape drive. If you use a network disk location, you must configure a destination before you can back up the file.

Configuring High Availability on the Standby Server

Before you begin

- The Active Server databases are restored on to the Standby Server.

About this task

Configure High Availability resiliency on the Standby Server using the High Availability utility. The Standby Server shadows the Active Server and takes over processing if the Active Server fails.

You must restart the server to apply the High Availability settings.

Procedure

1. Log on to the Standby Server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Configuration**.
4. Double-click **Server Mode**.
5. Under **Server Mode**, select **Standby**.
6. Under **IP Configuration**, in the **Active CLAN** box, type the IP address for the active server.
7. Under **IP Configuration,** in the **Standby CLAN** box, type the IP address for the standby server.

8. Under **IP Configuration**, in the **Managed IP** box, ensure the managed IP address appears.
9. Under **IP Configuration**, in the **Trusted IP** box, type the IP address of a trusted server.
10. Under **SMMC Port Configuration**, in the **Remote SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the remote (active) server.
11. Under **SMMC Port Configuration**, in the **Local SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the local (standby) server.
12. Click **Save**.
13. Reboot the standby server to apply the changes.

Variable definitions

Name	Description
Active CLAN	The IP address for the server initially configured in Active mode.
Standby CLAN	The IP address for the server initially configured in Standby mode.
Managed IP	The virtual Managed IP (MIP) address that is used by the Active Server for campus resiliency. A MIP is used only when the Active and Standby servers are in the same subnet.
Trusted IP	The Active and Standby servers use the Trusted IP address to verify network connectivity. If the Active server cannot communicate with the Standby server it attempts to communicate with the Trusted IP address. If the Active Server cannot connect to the Trusted IP address on startup then no Contact Center services start on that server. If the Active server cannot communicate with the Trusted IP address, if shadowing and switchover are enabled, then the Active server stops processing contacts and shuts down. The Standby server starts processing contacts if it cannot communicate with the Active server but can communicate with the Trusted IP address. Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.

Table continues…

Name	Description
Local SMMC Port	The Network Management port number for System Management and Monitoring Component (SMMC) on the local (standby) server. The default port number is 57012.
Remote SMMC Port	The Network Management port number for System Management and Monitoring Component (SMMC) on the remote (active) server. The port number entered here must match the port number set on the remote (active) server. The default port number is 57012.

Verifying server details on the standby server

Before you begin

- The active server databases are restored on to the standby server.

About this task

After you restore the active server database on to the standby server, verify that the standby server is configured correctly.

Procedure

1. Log on to the standby server.
2. From the **Start** menu, in the Avaya area, click **Server Configuration**.
3. In the **Server Configuration** dialog box, click the **Local Settings** tab.
4. Verify the standby server local settings.
5. If you made any changes to the local settings, click **Apply All**.
6. On the **Restart Required** dialog, click **No**.
7. In the **Server Configuration** dialog box, click the **Licensing** tab.
8. Verify the standby server licensing details.
9. If you made any changes to the licensing details, click **Apply All**.
10. On the **Restart Required** dialog, click **No**.
11. In the **Server Configuration** dialog box, under **SIP**, click the **Network Settings** tab.
12. Verify the standby server **SIP Network Settings** details.
13. If you made any changes to the SIP Network Settings, click **Apply All**.
14. On the **Restart Required** dialog, click **No**.
15. In the **Server Configuration** dialog box, under **SIP**, click the **Local Subscriber** tab.

16. Verify the standby server **SIP Local Subscriber** details.
17. If you made any changes to the SIP Local Subscriber settings, click **Apply All**.
18. On the **Restart Required** dialog, click **Yes**.

    If you did not make changes to any settings, CCMS does not display the **Restart Required** dialog.
19. Click **Exit**.

Variable definitions

Name	Description
Avaya Server Subnet IP Address	The IP address of the subnet that connects the Contact Center servers (Contact Center Manager Server, Network Control Center, Contact Center Manager Administration, and Contact Center Multimedia).
Voice Proxy Server • IP Address • Port • Network Transport	Information about the server that provides support for inbound and outbound calls, such as routing a call to an agent telephone. If the contact center uses an Avaya Aura® Session Manager, enter the IP address for the primary Session Manager. The server listening port. The default port is 5060. The SIP Network Transport communication protocol.
CTI Proxy Server • IP Address • Port • Network Transport	Information about the server that provides support for SIP Computer Telephony Integration (CTI) so that Agent Desktop can acquire and control agent telephones for TR87. Enter the IP address of the Avaya Aura® Application Enablement Services server. For an Application Enablement Services server the default SIP CTI Proxy Server port is 4723. The SIP Network Transport communication protocol. For an Application Enablement Services server, the default Network Transport communication protocol is TLS.

Table continues…

Name	Description
Backup Voice Proxy Server • IP Address • Port • Network Transport	Information about the server that provides backup support for inbound and outbound calls, such as routing a call to an agent telephone. Avaya Aura® Contact Center must have a Standby Server license to support a Backup Voice Proxy Server. The only type of Backup Voice Proxy Server supported by Avaya Aura® Contact Center is an Avaya Aura® Session Manager when it used with an Avaya Aura® Communication Manager. Enter the IP address for the backup Session Manager. The server listening port. The default port is 5060. The Backup Voice Proxy Server transport protocol.
IM Proxy Server • IP Address • Port • Network Transport	Information about the server that supports the deployment of Instant Message over SIP. The IP address of the SIP IM Proxy Server. The default SIP IM Proxy Server port is 5222. The IM SIP Proxy Server transport protocol.
IM Provider	Select your IM Provider, Aura Presence Services or Microsoft Lync (for Microsoft Skype for Business, select Microsoft Lync).
XMPP Domain	If using an Avaya Aura® Presence Services server, enter the domain name of the Extensible Messaging and Presence Protocol (XMPP) server.
Local SIP Subscriber • Contact Center Name • Domain Name	Information about the environment of the SIP-enabled contact center and how to identify the server within the network. The registration user name on the registration proxy. Use a suitable user name following the standards in your system. Associated domain name for the SIP- enabled contact center.
Web Service Ports	The Web Service Ports group box appears only if you select Avaya Aura® Presence Services as the IM Provider. Server Port default is 9100 Client Port default is 9120

Table continues…

Name	Description
SIP Server Type	Type of SIP proxy for the contact center integration. Depending on the switch type you select in the Application Selection window, the system automatically sets the specific SIP Server Type as the default.
MS Locale	Locale (including language and dialects) of the system environment.
Local Listening Ports	The SIP Communication protocol accepted by the system for incoming calls. TCP/UDP Port default is 5060 TLS Port default is 5061

Starting the Active Server

About this task

Start the Active Server using the System Management and Monitoring Component (SMMC) system tray. Starting the Active Server starts Contact Center applications and system processes.

Procedure

1. Log on to the Active Server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Configuration**.
4. Under **Switchover And Network Timeout Configuration**, select **Enable Switchover**.
5. Click **Save**.
6. On the **Desktop** screen of the active server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start HA System**. If the active server was previously rebooted, the system might already be started.
7. From the **Start** menu, in the Avaya area, click **System Control and Monitor Utility**.
8. Verify that Contact Center services are running.

Starting shadowing on the standby server

About this task

Start shadowing on the standby server using the System Management and Monitoring Component (SMMC) system tray.

The Standby server shadows the active server, maintaining a near real-time local copy of the Contact Center applications and Administration databases. Therefore, the standby server is configured with the most recent data and it can take over from the active server if necessary.

Important:

You must backup the active server database, restore it onto the standby server, and enable shadowing within 24 hours. If the difference in time between the active and standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the active server database and restore it onto the standby server before re-enabling shadowing. Ensure that the system clock times on the active and standby servers are synchronized.

Procedure

1. Log on to the standby server.
2. On the **Desktop** screen of the standby server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start HA System**.
3. From the **Start** menu, in the Avaya area, click **System Control and Monitor Utility**.
4. Check that the Contact Center services are running.

   Note:

   The following services do not start on the standby server:

   - CCMS_MasterService
   - CCMA - IceRTDService
   - CCMM - EmailManager, MCMC, CCMMOAM, Campaign Scheduler Service

Verifying High Availability is running

About this task

Verify that the Standby server is shadowing the active server using the High Availability Utility. The System dialog box of the High Availability utility displays system information about the active and the standby servers.

The dialog box displays the followings information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information
- Remote server connection status
- Remote server port information

- License information
- Databases shadowed
- Time of last record shadowed
- Database namespaces
- Local and remote information on system status, switchover, shadowing and network
- CC Application install information
- Database space and journaling information
- Database processes information

Procedure

1. Log on to the active server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. In the left pane, expand **Configuration**.
4. Select **System**.
5. Select **Get System Configuration**.

   The most recent system information appears.

Example

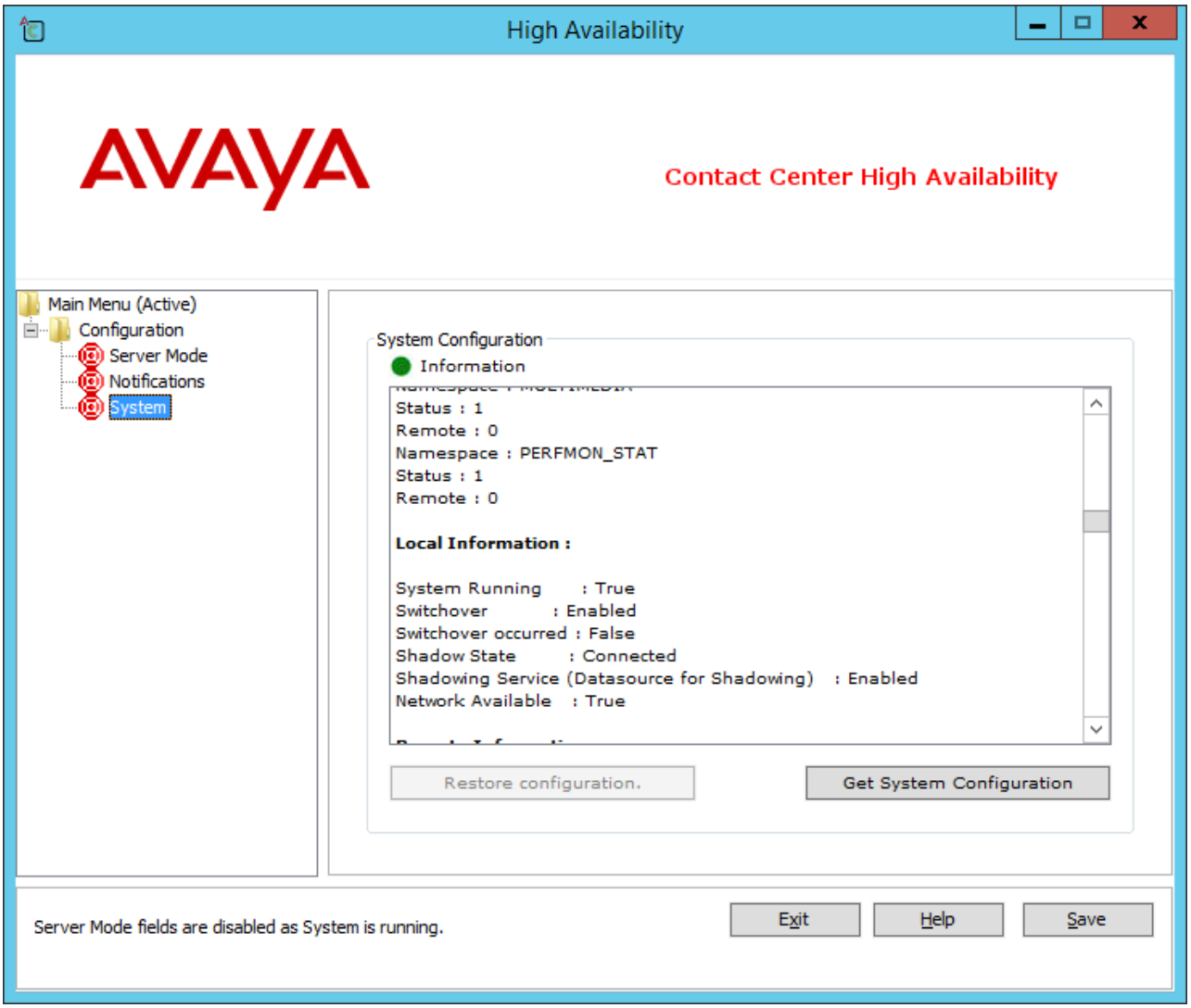


Figure 36: Example of an active server with the HA system running

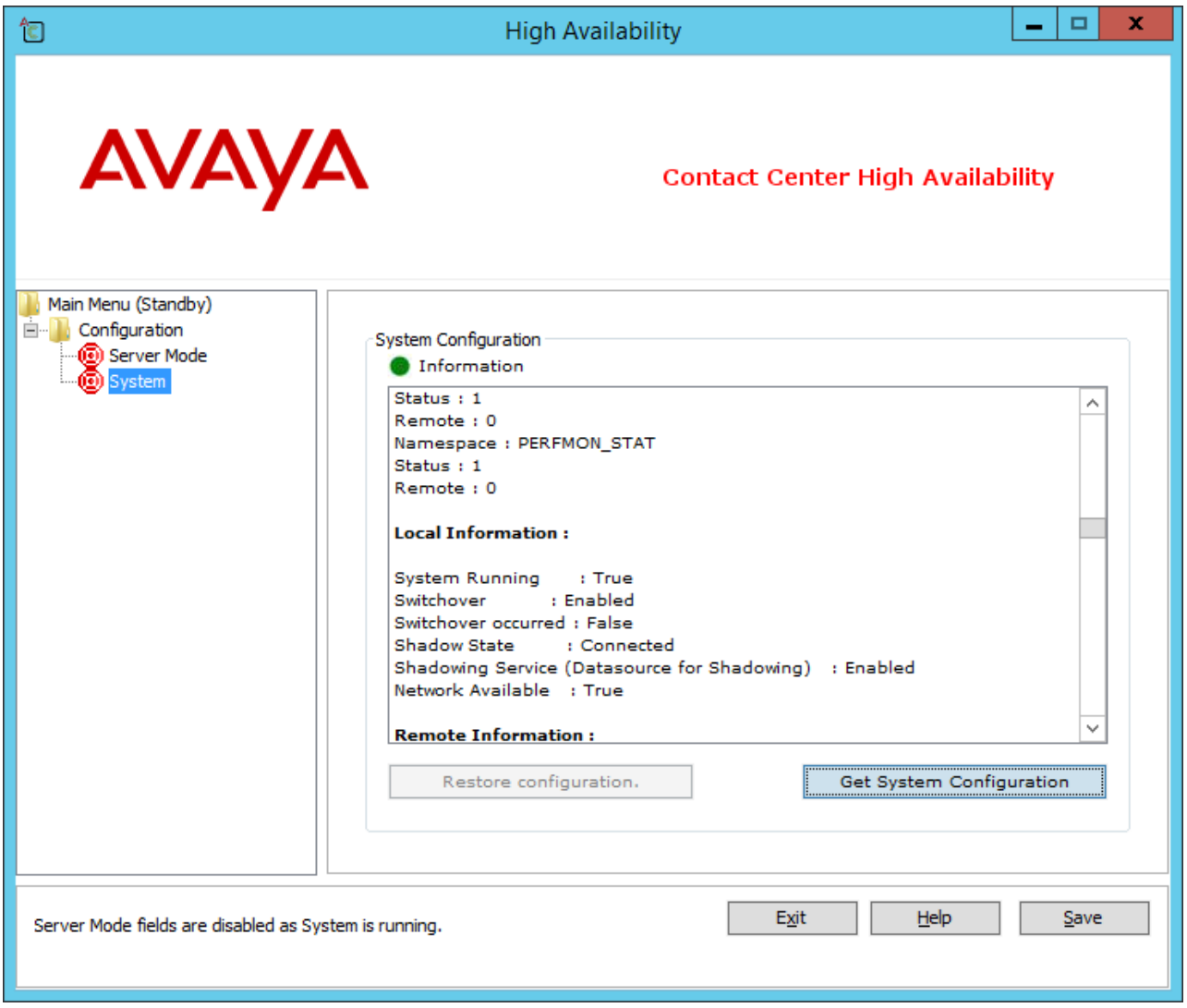


Figure 37: Example of a standby server with the HA system running

Note the **Server Mode fields are disabled as System is running** notice on the HA user interface.

Changing server details in Contact Center Manager Administration

About this task

In Contact Center Manager Administration, change the Contact Center Manager Server, Communication Control Toolkit and Contact Center Multimedia details to use the High Availability Managed IP address and Managed name details.

The High Availability Managed IP address and Managed name details entered here must match those configured in the hosts file.

Procedure

1. Log on to the active server.
2. Log on to the Contact Center Manager Administration application with administrative privileges.
3. On the **Launchpad**, click **Configuration**.
4. From the list of servers in the system tree, right-click on CCMS, and select **Edit Properties**.
5. In the **Server Name** box, type the High Availability Managed name of the active server.
6. In the **IP Address** box, type the High Availability Managed IP address of the active server.
7. In the **Display Name** box, type the name of Contact Center Manager Server as you want it to appear in the system tree of Contact Center Administration.
8. Click **Submit**.
9. From the list of servers in the system tree, right-click on CCT, and select **Edit Properties**.
10. In the **Server Name** box, type the High Availability Managed name of the active server.
11. In the **IP Address** box, type the High Availability Managed IP address of the active server.
12. In the **Display Name** box, type the name of Communication Control Toolkit as you want it to appear in the system tree of Contact Center Administration.
13. Click **Submit**.
14. From the list of servers in the system tree, right-click on CCMM, and select **Edit Properties**.
15. In the **Server Name** box, type the High Availability Managed name of the active server.
16. In the **IP Address** box, type the High Availability Managed IP address of the active server.
17. In the **Display Name** box, type the name of Contact Center Multimedia as you want it to appear in the system tree of Contact Center Administration.
18. Click **Submit**.

Using the Contact Center Manager Administration managed name

About this task

Use the High Availability managed name of Contact Center Manager Administration to access the CCMA application. When the Avaya Aura® Contact Center High Availability feature is configured

and enabled, redirect all Contact Center Manager Administration client web browsers to use the managed name of the server where CCMA is installed.

If you have a High Availability campus solution, Avaya recommends that you log in to the CCMA web client using the managed name of the active server. If an active application or server fails, the CCMA client web browser continues to use the managed name and you can continue working without interruption.

Important:

Do not type the real or managed IP address because this results in problems with Scripting, Historical Reporting, Configuration, Contact Center Management, and Access and Partition Management.

Before you begin

- Configure High Availability on the Active and Standby servers.
- Change the server details in CCMA.
- Ensure that you have the user ID and password to log in to CCMA.
- To access CCMA and other Contact Center applications, ensure that you are using Microsoft Edge in Internet Explorer mode.

Procedure

1. In your web browser, type the URL of the CCMA server managed name.

   For example, type `https://<server name>`, where <*server name*> is the managed name of the High Availability server pair. If you turned off Web Services security, type `http://<server name>`.

2. In the **User ID** field, type your user ID.
3. In the **Password** field, type your password.
4. Click **Login**.

Testing switchovers

Before you begin

- Configure High Availability on the Active and Standby servers.

About this task

Test the High Availability feature and infrastructure by making a manual switchover from the Active server to the Standby server.

Procedure

1. Log on to the current Active Server.
2. On the **Desktop** screen, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Manual Switchover**.

3. Make a call using the CCT Reference Client to test the Standby Server configuration, when the Standby Server becomes the new Active Server.

   For more details, see Verifying CCT using Reference Client on page 190.

Next steps

Avaya recommends that you analyze your network performance after running HA for a number of days. Use the Network Analyzer utility to analyze the SMMC logs and verify whether your Network Timeout value is set correctly for your network performance. For more information about using the Network Analyzer utility to optimize the High Availability configuration settings on network, see *Troubleshooting Avaya Aura® Contact Center*.

A network outage triggers a switchover. There are test scenarios you can use to trigger a network outage, for example:

- A physical NIC cable break. This applies when Avaya Aura® Contact Center is installed on a physical server or on a virtual machine.
- Disconnecting the virtual NIC of an Avaya Aura® Contact Center virtual machine.

Chapter 25: Remote Geographic Node High Availability Voice Contact Server commissioning

This section describes how to configure geographic High Availability resiliency for Voice Contact Servers in an Avaya Aura® Communication Manager and an Avaya Aura® Session Manager based contact center. Avaya Aura® Contact Center geographic High Availability supports data resiliency and disaster recovery.

Note:

Geographic High Availability is not supported for solutions using Midsize Enterprise (ME).

You must complete all the procedures in this section in sequential order.

In geographic Wide Area Network solutions the standby server on the remote geographic site is called a Remote Geographic Node server. The active server and the Remote Geographic Node server are part of the same Avaya Aura® Contact Center solution, but they are typically in different geographic locations and subnets.

The active server can also have a local standby server in the same campus location. The standby server shadows the active server. If the active server fails the local standby server takes over call processing on the local site. The active server need not have a standby server. Avaya Aura® Contact Center supports an active server with a Remote Geographic Node server and without a standby server. This chapter assumes that if your solution has campus HA, campus HA commissioning is complete.

The Remote Geographic Node (RGN) server on the remote site shadows the server on the campus site, maintaining a near real-time local copy of the server databases. Therefore, the RGN server is configured with the most recent data and it can take over if the campus site fails. Where the campus site has High Availability, the RGN server shadows the active server on the campus site, using the Managed IP address.

Remote Geographic Node server commissioning overview:

In a geographic Voice Contact Server HA configuration, one server is the active server and one is the Remote Geographic Node server. The active Voice and Multimedia Contact Server actively processes scripts and contacts and records statistics. The Remote Geographic Node server shadows the active server. The Remote Geographic Node server does not automatically take over if the active system fails. You must start the Remote Geographic Node server manually. The Remote

Geographic Node and active servers must have the same patch level and the same hard disk drive partitions.

High Availability Utility:

Configure High Availability resiliency using the High Availability (HA) Utility in the Database Utilities. The High Availability Utility is used to configure which server is the active and which is the Remote Geographic Node server. Where the campus site has High Availability, the HA utility also configures the Managed IP of the campus HA pair.

The High Availability Utility on an active server has the following dialogs under the Configuration tab:

- Server Mode
  - Configure the IP address for the Active and Standby servers
  - Configure the IP address for Trusted servers
  - Configure the IP address for the optional Remote Geographic Node
  - Identify if the server is Active, Standby, Remote Geographic Node, or Non HA
  - Enable Switchover
  - Configure the switchover time-out. This is the wait time if a network outage occurs before an automatic switchover occurs
  - Temporally set as Non-HA
- Notifications
  - Configure an email server for email notifications
  - Configure where and how often to send email notifications
  - Configure the email character set
- System
  - Display information on the system status
  - Verify that database shadowing is running

SMMC system tray:

The Contact Center System Management and Monitoring Component (SMMC) system tray gives quick access to action items in your High Availability environment, for example:

- Start HA System
- Stop HA System
- Disable Switchover
- Enable Switchover
- System Information
- Database Information
- Disable Next Auto Startup

- Select Standby Auto Startup Mode (standby server only)
- Re-enable HA system (this option is available only when the active HA server is running but switchovers are disabled)

Note:

These action items appear depending on the system state. For example, the Disable Switchover and Enable Switchover items never appear simultaneously.

To access the SMMC system tray menu, right-click the SMMC icon on the Windows taskbar.

High Availability Utility and SMMC system tray:

Use the High Availability Utility to configure High Availability IP addresses and to configure which server is the active server and which is the RGN server. Then use the System Management and Monitoring Component (SMMC) system tray to start database shadowing and High Availability functionality.

Prerequisites

- The active and Remote Geographic Node (RGN) servers must meet the planning and engineering specifications. For more information, see *Avaya Aura® Contact Center Overview and Specification*.
- Ensure unused Network Interface Cards (NICs) are disabled.
- The Voice Contact Server is installed on the active and RGN servers using the same drive specification on each server.
- CCMS is configured on the active server. For more information, see Contact Center Manager Server commissioning on page 49.
- Ensure the third-party networking utility is installed. For more information, see Installing the third-party networking utility on page 56.
- CCMA is configured on the active server. For more information, see Contact Center Manager Administration commissioning on page 100.
- CCT is configured on the active server. For more information, see Communication Control Toolkit commissioning for SIP-enabled Contact Center on page 183.
- If you have High Availability at the campus, the active and standby servers in the HA campus site are installed and HA is fully commissioned.
- You have a valid standby server license file on the active server and the Remote Geographic Node server. If you are using Avaya WebLM server instead, you have installed an Avaya WebLM server virtual guest at the campus and another Avaya WebLM server virtual guest at the remote site, and generated and applied the correct license files.
- Ensure the Voice Contact Server is on a domain. This is to allow the CCT clients to automatically re-connect after a switchover.

- Add the RGN CCMS and CCMM as servers in CCMA.
- Ensure the RGN server IP addresses are configured in CCMM General Administration on the active server. For more information, see Configuring CCMM General Administration on page 307.
- Before you commission HA, use System Control and Monitoring Utility (SCMU) to shut down all CCMS and CCT services on both the active and RGN servers.

High Availability commissioning checklist

The following is a list of key configuration items required for High Availability commissioning in a SIP-enabled contact center environment.

Item	Your value	Description
Ensure that Contact Center is licensed for High Availability		High Availability is a licensed feature and is enabled when you purchase a standby server license.
Active server host name		The name of your AACC active server.
Active server IP address		The IP address of your AACC active server.
Standby server host name		If you have HA at the campus site, the name of your AACC standby server.
Standby server IP address		If you have HA at the campus site, the IP address of your AACC standby server.
Managed name		If you have HA at the campus site, the managed name of your AACC campus HA pair.
Managed IP address		If you have HA at the campus site, the managed IP address of your AACC campus HA pair.
Using Hosts file or DNS?		If you are using the Hosts files to resolve Managed names to Managed IP addresses, ensure that you add the Managed names and Managed IP addresses to the Hosts file.
Trusted IP address		Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.
RGN server host name		If you have HA geographic redundancy, the name of your AACC RGN server.

Table continues…

Item	Your value	Description
RGN server IP address		If you have HA geographic redundancy, the IP address of your AACC RGN server.
Using email notification?		You can enable automatic email switchover notifications to alert the Contact Center administrator. When enabled, the specified email address receives an automatic email which provides switchover information to the recipient.
SMTP server name		The name of your SMTP server for email notification after an automatic switchover occurs.
Email Username		The log on name of an email user configured on the email server.
Email Password		The password of an email user configured on the email server.
Email address to send notifications from		The email address that the email notification is sent from.
Email address to send notifications to		The email address that the email notification is sent to.
Database backup location		The location of the shared folder where you store database backups. This folder must not be on the active or standby servers.

Resolving the Managed name to the Managed IP Address

About this task

Complete the following procedure to resolve the Managed server name to the Managed IP address. If the server has two network interfaces, apply these settings to the CLAN network interface. Each Contact Center server in a domain requires a DNS static entry.

Important:

Avaya Aura® Contact Center High Availability solutions do not support Dynamic DNS.

Ask your System Administrator to add a Domain Name System (DNS) static entry for the active and standby servers and one additional DNS static entry for the each Managed name and associated Managed IP address.

In High Availability solutions, the managed IP address must be lower than the active and standby server IP addresses. For example, if the active server IP address is 1.2.3.4 and the standby server IP address is 1.2.3.5, the managed IP address is 1.2.3.3.

A typical High Availability campus solution with a pair of servers requires 3 DNS static entries; one DNS static entry for the active server, one DNS static entry for the standby server, and one DNS static entry for the Managed name and associated IP address.

If your solution is going to have a Remote Geographic Node, ask your System Administrator to add a Domain Name System (DNS) static entry for the Remote Geographic Node server.

Perform this procedure on the Active server. Perform this procedure on the Standby server if you have one. Perform this procedure on the Remote Geographic Node server if you have one.

Procedure

1. Open Windows Explorer.
2. Go to the folder C:\Windows\system32\drivers\etc.
3. Double-click on the **hosts** file, select **Open**, and select **Notepad**.

   The hosts file opens in Notepad.
4. Add the Managed IP address and the Managed server name to the hosts file.

   Important:

   The Managed name can be a full name or netbios server name.

Verifying services are ready for configuring High Availability

About this task

Verify that all Contact Center services stop before you configure High Availability. This ensures that all resources are available to the active server when it starts.

Perform this procedure using the System Management and Monitoring Component (SMMC) on the active server.

Procedure

1. Log on to the active server.
2. On the **Desktop** screen, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **Stop System**.

Configuring geographical redundancy on the active server

About this task

Configure High Availability geographical redundancy on the active server using the High Availability Utility. The active server is the server that normally processes contacts.

Procedure

1. Log on to the active server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Configuration**.
4. Click **Server Mode**.
5. Under **Server Mode**, select **Active (Campus)** if you have HA at the campus site or select **Active (RGN)** if you do not have HA at the campus site.
6. Under **IP Configuration**, in the **Active CLAN** box, type the IP address for the active server.
7. In the **Standby CLAN** box, type the IP address for the standby server if you have HA at the campus site.
8. In the **Managed IP** box, type the managed IP address.
9. In the **Trusted IP** box, type the managed IP address.
10. In the **Remote Geographic Node** box, type the IP address of the Remote Geographic Node.
11. Click **Save**.

Variable definitions

Name	Description
Active CLAN	The IP address for the server initially configured in active mode.
Standby CLAN	The IP address for the server initially configured in Standby mode.
Managed IP	The virtual Managed IP (MIP) address that is used by the active server for campus resiliency. A MIP is used only when the Active and Standby servers are in the same subnet.
Trusted IP	Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.
Remote Geographic Node	The IP address of the Remote Geographic Node.
Local SMMC Port	The port number for System Management and Monitoring Component (SMMC) on the active server. The default port number is 57012.
Remote SMMC Port	The port number for System Management and Monitoring Component (SMMC) on the RGN server. The port number entered here must match the port number set on the active server. The default port number is 57012.

Backing up the database on the active server

About this task

The active server is configured for High Availability. Now the Remote Geographic Node server must be prepared for High Availability resiliency. Back up the active server to create a snapshot of the database which is then restored to the Remote Geographic Node server. On the active Voice Contact Server all databases must be backed up.

Important:

Do not use a folder on the Active or standby servers as the backup location.

Procedure

1. Log on to the active server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. Click **Backup Locations**.
4. Click **Create**.
5. From the **Driver Letter** list, select the network drive on which you want to store the CCMS, CCT, ADMIN, and CCMA databases.
6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Backup Location. This location must be a shared folder with correct permissions.

   Important:

   If your contact center includes a Multimedia Contact Server, do not use the same backup folder for your Voice Contact Server and Multimedia Contact Server databases, because ADMIN databases stored in the same backup location overwrite each other.
7. In the **User Name** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the Windows password.
9. Click **Save**.
10. In the left pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. From the **Backup Location** list, select the network drive on which to store the backup.
13. Click **Backup**.

Configuring the Remote Geographic Node local resources

About this task

Configure the Remote Geographic Node (RGN) resources to allow the remote site to function as a standalone contact center if the campus site fails. To perform this procedure, Contact Center services must be running.

When High Availability shadowing is enabled, the RGN server shadows some of the configuration data from the campus site.

The RGN server does not shadow (replicate) information about the following resources from the campus site:

- Media Server and Media Services
- Default DN

On the RGN server, you must configure these resources to use local Avaya Aura® Media Servers and attendants.

Configure a Default DN to catch treated calls that are defaulted by the contact center script and to catch calls not answered by agents. Avaya recommends that you configure a local attendant at the RGN site as the Default DN.

Avaya Aura® Contact Center uses Avaya Aura® Media Server (MS) media processing capabilities to support conferencing, announcements, and dialogs. Configure each Avaya Aura® MS in at the RGN site as a Media Server. Contact Center uses the media processing capabilities of Avaya Experience Portal to support external Interactive Voice Response (IVR) dialogs (XDIALOG). If your RGN site uses local Avaya Experience Portal servers, add these here as Media Servers and configure them to provide external dialog (XDIALOG) services.

Procedure

1. Start Contact Center services on the RGN server.
2. On the RGN server, log on to Contact Center Manager Administration.
3. On the **Launchpad**, click **Configuration**.
4. In the left pane, expand the RGN Contact Center Manager Server on which to configure global settings.
5. Select the **Global Settings** folder.
6. Configure the global settings for your system based on the fields listed in the **Global Settings** window.
7. In the **Default DN** box, type the default DN to use when a script defaults or a treated call is not answered. Avaya recommends that you configure an attendant as the Default DN.
8. Click **Save**.
9. In the left pane, expand the RGN Contact Center Manager Server on which to configure a media server. Ensure that you select the local RGN CCMS server, not a campus server.
10. Select the **Media Servers** folder.

11. In the right pane, in the **Server Name** box, type the name of the Avaya Aura® MS server.
12. In the **IP address** box, type the IP address of the Avaya Aura® MS server.
13. In the **Port Number** box, type the port number for the Avaya Aura® MS server. The port number must match the Avaya Aura® MS port number. The default is 5060.
14. If the Avaya Aura® MS is going to manage prompts, select the **Master Content Store**. Avaya Aura® MS supports only one Master Content Store.
15. Click any other row in the table to save the changes.
16. In the left pane, expand the RGN Contact Center Manager Server on which to configure a media services.
17. Select the **Media Services and Routes** folder.
18. On the **Media Services & Routes** table, select a media service. For an Avaya Aura® MS, select **ACC_APP_ID**.
19. From the **Available** list, select an Avaya Aura® MS to associate with the selected conference media service.
20. Click the right arrow (>).

    The server moves to the **Selected** list.
21. Repeat step 8 on page 336 to step 20 on page 337 for each Avaya Aura® MS installed on the Remote site.
22. If you add more than one Avaya Aura® MS, use the up and down **Rank** arrows to order the selected servers.
23. Click **Submit**.
24. Stop Contact Center services on the RGN server.

Configuring High Availability on the Remote Geographic Node server

About this task

Configure High Availability resiliency on the Remote Geographic Node server using the High Availability utility. The Remote Geographic Node Server shadows the active server.

Procedure

1. Log on to the Remote Geographic Node server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Configuration**.
4. Click **Server Mode**.

5. Under **Server Mode**, select **RGN**.
6. If you do not have HA at the campus site, in the **Campus CLAN** box, type the IP address for the campus active server.
7. If you have HA at the campus site, in the **Campus CLAN** box, type the Managed IP address for the campus server pair.
8. Under **IP Configuration**, in the **RGN CLAN** box, type the IP address for the Remote Geographic Node server.
9. Ensure that the **Managed IP** box is empty.
10. Under **IP Configuration**, in the **Trusted IP** box, type the IP address of a trusted server.
11. Under **SMMC Port Configuration**, in the **Remote SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the campus active server.
12. Under **SMMC Port Configuration**, in the **Local SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the RGN server.
13. Click **Save**.
14. On the **High Availability** dialog box, click **OK**.

    Do not reboot the server at this point.

Variable definitions

Name	Description
Campus CLAN	If you do not have HA at the campus site, type the IP address of the campus active server. If you have HA at the campus site, type the virtual Managed IP address that is used by the campus server pair. The RGN server monitors the Managed IP address of the campus site. If the active server on the campus site fails, the standby server assumes the managed IP address and continues processing. The RGN server continues shadowing from this IP address.
RGN CLAN	The IP address for the Remote Geographic Node server.
Trusted IP	The IP address of a trusted server that is not likely to fail, so that both active and RGN servers have a server to ping regularly to verify the network connection. Avaya recommends that you use an IP address from your IT infrastructure as the Trusted IP address.

Table continues…

Name	Description
Local SMMC Port	The Network Management port number for System Management and Monitoring Component (SMMC) on the RGN server. The default port number is 57012.
Remote SMMC Port	The Network Management port number for System Management and Monitoring Component (SMMC) on the campus active server. The port number entered here must match the port number set on the campus active server. The default port number is 57012.

Restoring the database on the Remote Geographic Node server

Before you begin

- Know the location of the backup database.
- Stop all Contact Center services using the SCMU utility, if services are running.
- Ensure the patch level on the Remote Geographic Node server is the same as the active server.

Important:

Not all CCT data is stored in the database. The following data must be configured on the Remote Geographic Node server: CCT SOA configuration (CCT Web Services), and CCT logging location.

Important:

You must restore all databases on the Voice Contact Server. Restoring only CCMS and not CCT, ADMIN, or CCMA can leave an inconsistent server, and HA cannot shadow data correctly.

Important:

Restoring the ADMIN database can change configuration of Backup locations on the Remote Geographic Node server if the active server and Remote Geographic Node server backup locations are different. Therefore, after you restore the ADMIN database, close and reopen the Database and Maintenance utility.

About this task

Restore the database from the active server to the Remote Geographic Node (RGN) server to ensure the databases are consistent. The Database Maintenance utility can restore all application databases at once. You must restore the CCMS, CCT, ADMIN, and CCMA database onto the RGN server.

Procedure

1. Log on to the RGN server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. In the **Database Maintenance** dialog box, in the left pane, click **Restore**.
4. In the right pane, under **Media Type**, select the media type on which the backup is restored.
5. If the backup file is on the network drive, in the **Backup Location** list, select the backup location.
6. Under **Application**, select CCMS, CCT, ADMIN, and CCMA.
7. Under **Restore contents**, select **Data**.

   Important:

   Do not select **Offline**.
8. Click **Restore**.
9. Use the **Information** field to monitor the progress of the restoration.
10. When the restore completes, click **OK**.
11. Click **Exit** to close the Database Maintenance utility.

Variable definitions

Name	Description
Application	The database and applications of Contact Center that you can back up.
Backup Location	The destination of the network disk. The values are configured in the Backup Locations.
Restore contents	The type of content that is stored in the database. Data is in the database. Schema is the data for the database structure, tables and procedures.
Media type	The type of media used for your backup file. You can use a network disk location or a tape drive. If you use a network disk location, you must configure a destination before you can back up the file.

Configuring server details on the Remote Geographic Node

About this task

Configure the Remote Geographic Node server with server details that do not replicate from the active server.

Important:

Changes to the SIP Local Subscriber data require an Avaya Aura® Contact Center restart.

Procedure

1. Log on to the Remote Geographic Node server.
2. From the **Start** menu, in the Avaya area, click **Server Configuration**.
3. In the **Server Configuration** dialog box, click the **Local Settings** tab.
4. Update the Remote Geographic Node server local settings.
5. On the **Restart Required** dialog, click **No**.
6. In the **Server Configuration** dialog box, click the **Licensing** tab.
7. Update the Remote Geographic Node server licensing details.
8. On the **Restart Required** dialog, click **No**.
9. In the **Server Configuration** dialog box, under **SIP**, click the **Network Settings** tab.
10. Update the Remote Geographic Node server **SIP Network Settings** details. Ensure the Avaya Aura® Contact Center RGN server is configured to use a local RGN Avaya Aura® Unified Communications platform.
11. On the **Restart Required** dialog, click **No**.
12. In the **Server Configuration** dialog box, under **SIP**, click the **Local Subscriber** tab.
13. Update the Remote Geographic Node server **SIP Local Subscriber** details.
14. Click **Apply All**.
15. On the **Restart Required** dialog, click **Yes**.
16. Click **Exit**.

Variable definitions

Name	Description
Avaya Server Subnet IP Address	The IP address of the subnet that connects the Contact Center servers (Contact Center Manager Server, Network Control Center, Contact Center Manager Administration, and Contact Center Multimedia).
Voice Proxy Server • IP Address • Port • Network Transport	Information about the server that provides support for inbound and outbound calls, such as routing a call to an agent telephone. If the contact center uses an Avaya Aura® Session Manager, enter the IP address for the primary Session Manager here. The server listening port. The default port is 5060.
CTI Proxy Server • IP Address • Port • Network Transport • Port • Network Transport	Information about the server that provides support for SIP Computer Telephony Integration (CTI) so that Agent Desktop can acquire and control agent telephones for TR87. Enter the IP address of the Avaya Aura® Application Enablement Services server. For an Application Enablement Services server the default SIP CTI Proxy Server port is 4723. The SIP Network Transport communication protocol. For an Application Enablement Services server, the default Network Transport communication protocol is TLS. The server listening port. The default port is 5060. The Backup Voice Proxy Server transport protocol.
IM Proxy Server • IP Address • Port • Network Transport	Information about the server that supports the deployment of Instant Message over SIP. The IP address of the SIP IM Proxy Server. The default SIP IM Proxy Server port is 5222. The IM SIP Proxy Server transport protocol.
IM Provider	Select your IM Provider, Aura Presence Services or Microsoft Lync (for Microsoft Skype for Business, select Microsoft Lync).
XMPP Domain	If using an Avaya Aura® Presence Services server, enter the domain name of the Extensible Messaging and Presence Protocol (XMPP) server.

Table continues…

Name	Description
Local SIP Subscriber • Contact Center Name • Domain Name	Information about the environment of the SIP-enabled contact center and how to identify the server within the network. The registration user name on the registration proxy. Use a suitable user name following the standards in your system. Associated domain name for the SIP- enabled contact center.
Web Service Ports	The Web Service Ports group box appears only if you select Avaya Aura® Presence Services as the IM Provider. Server Port default is 9100 Client Port default is 9120
SIP Server Type	Type of SIP proxy for the contact center integration. Depending on the switch type you select in the Application Selection window, the system automatically sets the specific SIP Server Type as the default.
MS Locale	Locale (including language and dialects) of the system environment.
Local Listening Ports	The SIP Communication protocol accepted by the system for incoming calls. TCP/UDP Port default is 5060 TLS Port default is 5061

Starting the active server

About this task

Start the active server using the System Management and Monitoring Component (SMMC) system tray. Starting the active server starts Contact Center services and system processes.

Procedure

1. Log on to the active server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Configuration**.
4. Under **Switchover And Network Timeout Configuration**, select **Enable Switchover**.
5. Click **Save**.

6. On the **Desktop** screen of the active server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start HA System**.
7. From the **Start** menu, in the Avaya area, click **System Control and Monitor Utility**.
8. Verify that the Contact Center services are running.

Starting shadowing on the standby server

About this task

Start shadowing on the standby server using the System Management and Monitoring Component (SMMC) system tray.

The Standby server shadows the active server, maintaining a near real-time local copy of the Contact Center applications and Administration databases. Therefore, the standby server is configured with the most recent data and it can take over from the active server if necessary.

Important:

You must backup the active server database, restore it onto the standby server, and enable shadowing within 24 hours. If the difference in time between the active and standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the active server database and restore it onto the standby server before re-enabling shadowing. Ensure that the system clock times on the active and standby servers are synchronized.

Procedure

1. Log on to the standby server.
2. On the **Desktop** screen of the standby server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start HA System**.
3. From the **Start** menu, in the Avaya area, click **System Control and Monitor Utility**.
4. Check that the Contact Center services are running.

   Note:

   The following services do not start on the standby server:

   - CCMS_MasterService
   - CCMA - IceRTDService
   - CCMM - EmailManager, MCMC, CCMMOAM, Campaign Scheduler Service

Starting shadowing on the Remote Geographic Node Server

About this task

Start shadowing on the Remote Geographic Node (RGN) server using the System Management and Monitoring Component (SMMC) system tray.

The RGN server shadows the campus active server, maintaining a near real-time local copy of the Contact Center applications and Administration databases. The Remote Geographic Node server is therefore configured with the most recent data.

Important:

You must backup the active server database, restore it onto the RGN server, and enable shadowing within 24 hours. If the difference in time between the active and standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the active server database and restore it onto the RGN server before re-enabling shadowing. Ensure that the system clock times on the active and standby servers are synchronized.

Procedure

1. Log on to the Remote Geographic Node server.
2. On the **Desktop** screen of the standby server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start HA System**.
3. From the **Start** menu, in the Avaya area, click **System Control and Monitor Utility**.
4. Verify that the Contact Center services are **Shut down**. On an RGN server, Contact Center services are shut down while the RGN database shadows the active database. You must manually start an RGN server if required, there is no automatic switchover if the campus site fails.

Verifying the Multimedia Contact Server RGN settings

About this task

If you have a Multimedia Contact Server, verify the Remote Geographic Node (RGN) settings. The RGN server must be available and manually enabled to take over if the campus site fails.

Procedure

1. Log on to the active server.
2. Log on to the CCMA Web client. If you have HA at the campus, use the managed name.
3. On the Launchpad, select **Configuration**.

4. Ensure the list of servers in the left hand pane includes only the campus CCMS, CCT and CCMM server details. Remove any Remote Geographic Node server listings from the left hand pane.
5. From the server list, select the CCMS server. If you have HA at the campus, use the managed name.
6. On the CCMS server, select **Refresh Server**.
7. Ensure the **Associated Reporting Server** section includes the associated Multimedia Contact Server. If you have HA at the campus, check that it is the managed name.
8. Ensure the **Remote Geographic Node** section displays the **RGN Server Name** and **RGN Server IP** of the Remote Geographic Node Voice Contact Server.
9. From the server list, select the CCMM server. If you have HA at the campus, use the managed name.
10. From the **Server** menu, choose **Edit Properties**.

    You can also right-click the server and select **Edit Properties**.
11. In the **Remote Geographic Node** section, in the **RGN Server Name** box, type the name of the RGN Multimedia Contact Server.
12. Press Enter.

    The **RGN Server IP** address box updates to display the IP address of the RGN Multimedia Contact Server.
13. Click **Submit**.

Verifying High Availability is running

About this task

Using the High Availability Utility, verify that the Remote Geographic Node (RGN) server is shadowing the active server . The System dialog box of the High Availability utility displays system information about the active and the Remote Geographic Node servers.

The dialog box displays the followings information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information
- Remote server connection status
- Remote server port information
- License information

- Databases shadowed
- Time of last record shadowed
- Database namespaces
- Local and remote information on system status, switchover, shadowing and network
- CC Application install information
- Database space and journaling information
- Database processes information

Procedure

1. Log on to the active server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. In the left pane, expand **Configuration**.
4. Select **System**.
5. Select **Get System Configuration**.

   The most recent system information appears.

Example

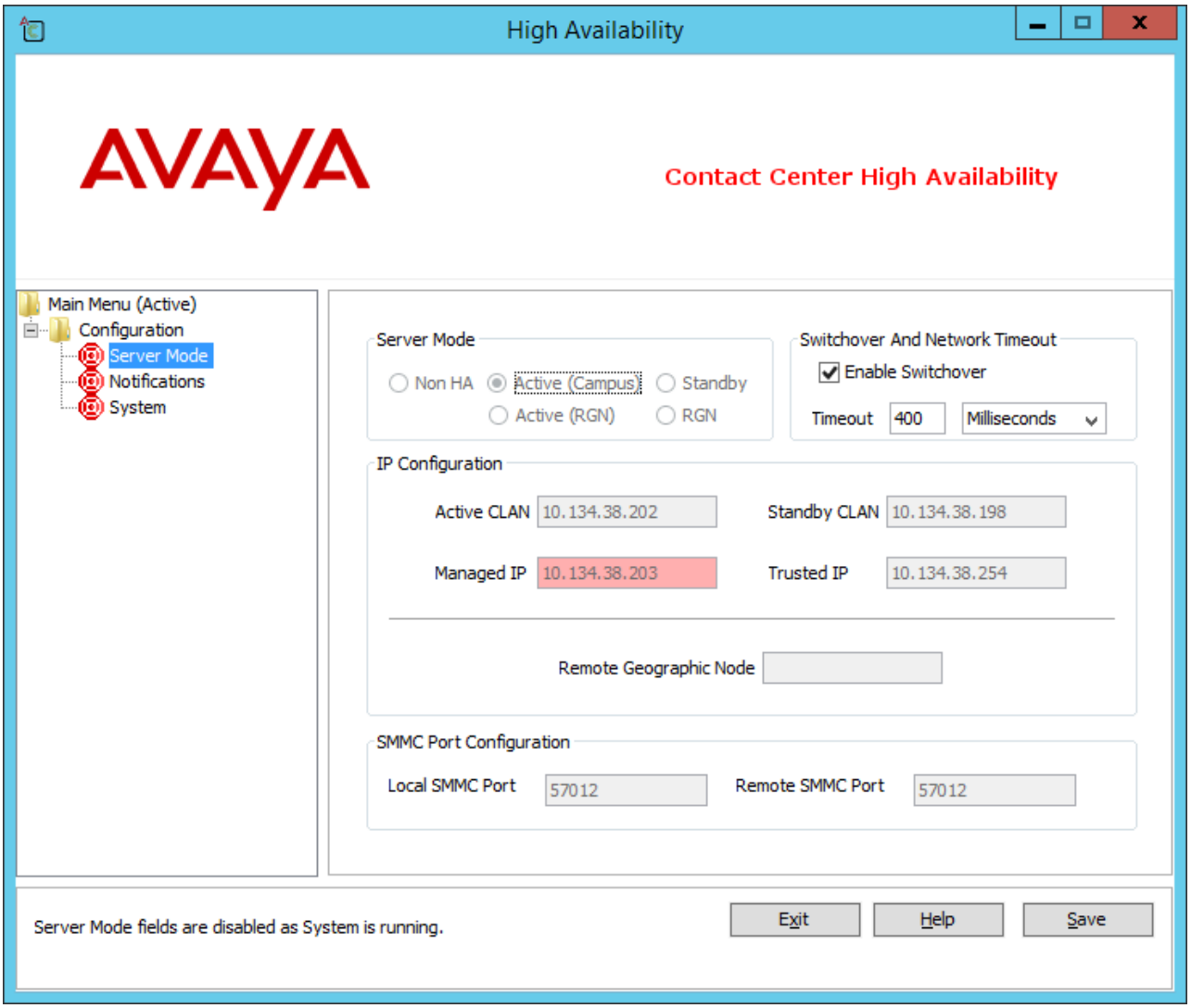


Figure 38: Example of an active server with the HA system running

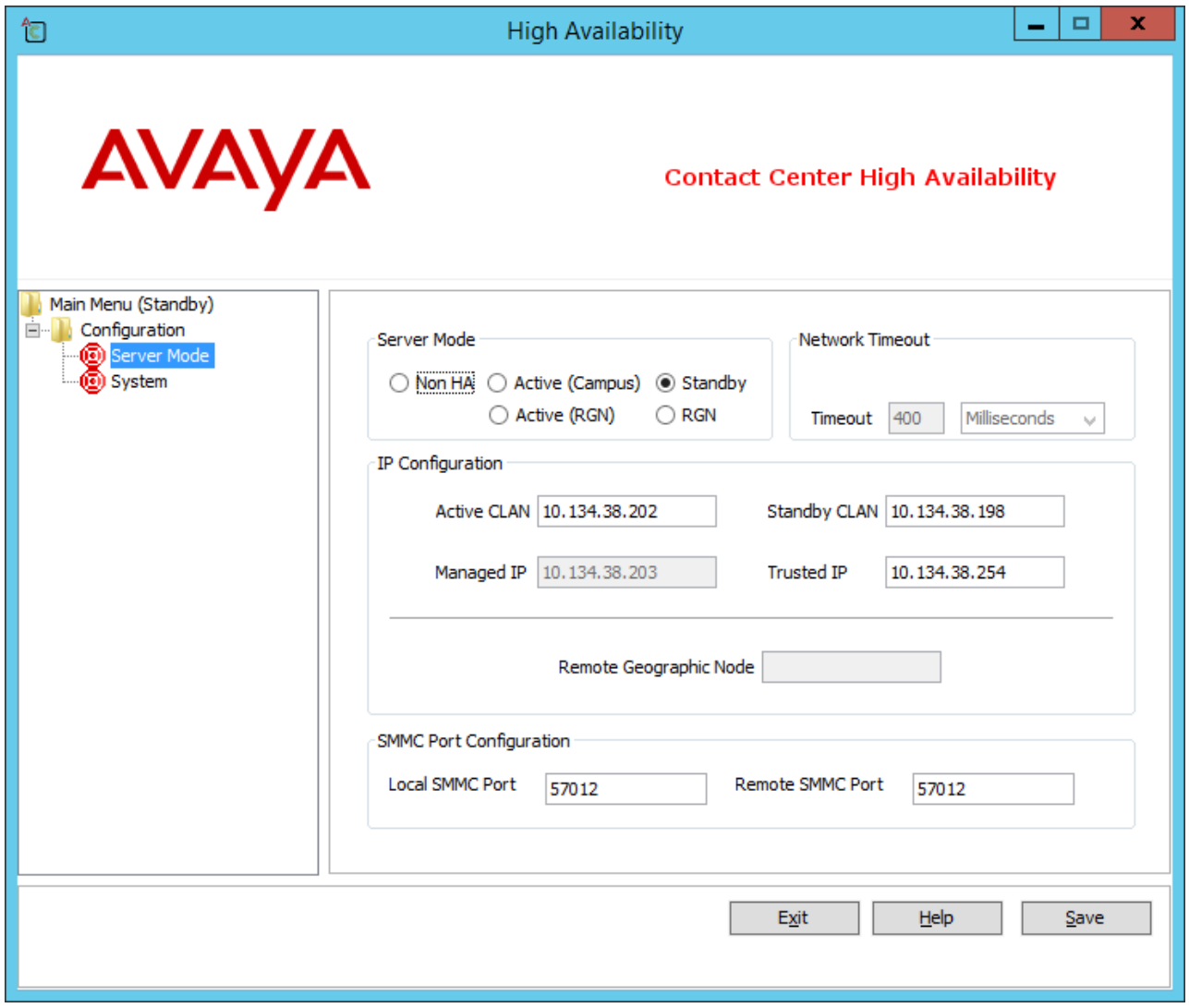


Figure 39: Example of an standby server with the HA system running

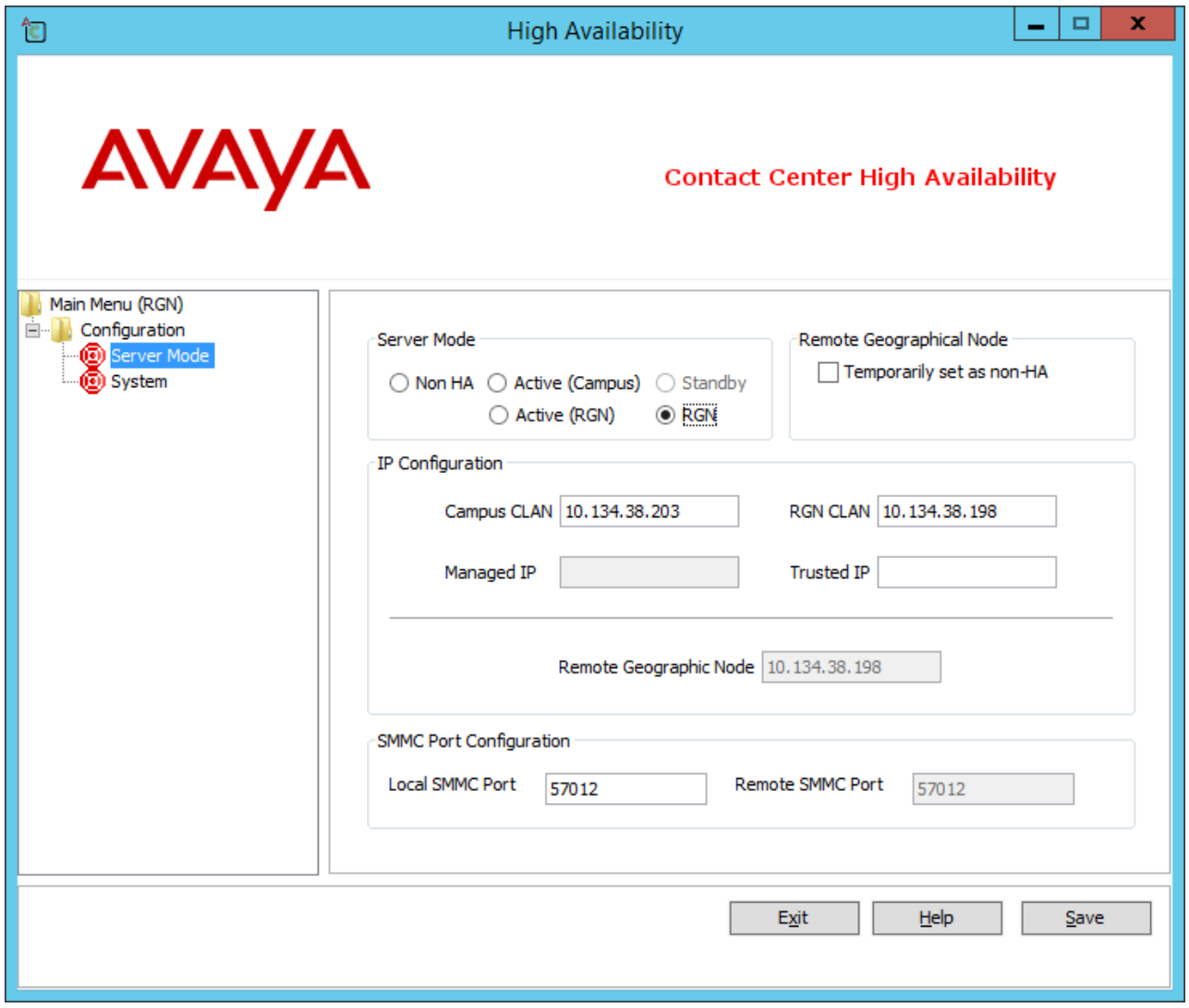


Figure 40: Example of an Remote Geographic Node server with the HA system running

Note the **Server Mode fields are disabled as HA System is running** notice on the HA user interface.

Chapter 26: High Availability Multimedia Contact Server commissioning

This section describes how to configure High Availability (HA) resiliency on a pair of Multimedia Contact Servers in a campus contact center solution.

You must complete all the procedures in this section in sequential order.

High Availability Multimedia Contact Server commissioning overview:

In a Multimedia Contact Server HA configuration, one Multimedia Contact Server is the active server and one is the standby server. The active Multimedia Contact Server actively processes contacts. The standby server shadows the active server. The standby server copies all configuration changes made on the active server and monitors the active server status. If the active Multimedia Contact Server fails, the standby Multimedia Contact Server, running in standby mode, recognizes the failure and starts processing contacts. The active and standby Multimedia Contact Servers are part of the same contact center and they must be in the same subnet IP address range for campus High Availability resiliency to work.

You must configure the standby Multimedia Contact Server the same as the active server. The standby and active servers must have the same patch level and the same hard disk drive partitions. Configuration changes made to the active Multimedia Contact Server during normal operation are automatically copied to the standby server so that the standby server can take over processing from the active server when necessary.

In a campus solution, a CCMM hardware, network, or database failure can initiate a switchover but only if:

- The switchover check box on both CCMM servers is selected
- The standby CCMM server is shadowing the active server
- A valid license file containing standby server license information for CCMM exists to allow switchover

Managed IP Address:

A Managed IP (MIP) address is a virtual IP address that is attached to a network adapter on the active server. Each Avaya Aura® Contact Center application server is assigned a static IP address. After the active server in each replication pair is determined, the active server attaches a Managed IP address to its network interface. The managed IP address is assigned only to the active server and it is used by all other Contact Center applications and clients to connect to that application. The standby server assumes this same managed IP address only if it takes over processing and

becomes the active application. The active server stops using the Managed IP when it stops being the active server.

High Availability Utility:

High Availability resiliency for Contact Center Multimedia is configured using the High Availability Utility in the Database Utilities. Use the High Availability Utility to configure which server is the active and which is the standby server. The HA utility also configures the Managed IP of the active server.

Prerequisites

- Ensure unused Network Interface Cards (NICs) are disabled.
- Install Contact Center Multimedia software on the active and standby servers.
- Install a Voice Contact Server to provide the core functionality for this Multimedia Contact Server.
- Commission Contact Center Multimedia. See Contact Center Multimedia server commissioning on page 192.
- Know how to configure the High Availability settings.
- CCMM stores license information in the registry. Configure CCMM licensing on the standby CCMM server, after restoring the database from the active server. See Contact Center Multimedia server commissioning on page 192.

High Availability commissioning checklist

The following is a list of key configuration items required for High Availability commissioning in a SIP-enabled contact center environment.

Item	Your value	Description
Ensure that Contact Center is licensed for High Availability		High Availability is a licensed feature and is enabled when you purchase a standby server license.
Active server host name		The name of your AACC active server.
Active server IP address		The IP address of your AACC active server.
Standby server host name		If you have HA at the campus site, the name of your AACC standby server.
Standby server IP address		If you have HA at the campus site, the IP address of your AACC standby server.

Table continues…

Item	Your value	Description
Managed name		If you have HA at the campus site, the managed name of your AACC campus HA pair.
Managed IP address		If you have HA at the campus site, the managed IP address of your AACC campus HA pair.
Using Hosts file or DNS?		If you are using the Hosts files to resolve Managed names to Managed IP addresses, ensure that you add the Managed names and Managed IP addresses to the Hosts file.
Trusted IP address		Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.
RGN server host name		If you have HA geographic redundancy, the name of your AACC RGN server.
RGN server IP address		If you have HA geographic redundancy, the IP address of your AACC RGN server.
Using email notification?		You can enable automatic email switchover notifications to alert the Contact Center administrator. When enabled, the specified email address receives an automatic email which provides switchover information to the recipient.
SMTP server name		The name of your SMTP server for email notification after an automatic switchover occurs.
Email Username		The log on name of an email user configured on the email server.
Email Password		The password of an email user configured on the email server.
Email address to send notifications from		The email address that the email notification is sent from.
Email address to send notifications to		The email address that the email notification is sent to.
Database backup location		The location of the shared folder where you store database backups. This folder must not be on the active or standby servers.

Resolving the Managed name to the Managed IP address

About this task

Complete the following procedure to resolve the Managed server name to the Managed IP address. If the server has two network interfaces, apply these settings to the CLAN network interface. Each Contact Center server in a domain requires a DNS static entry.

Important:

Avaya Aura® Contact Center High Availability solutions do not support Dynamic DNS.

Ask your System Administrator to add a Domain Name System (DNS) static entry for the active and standby servers and one additional DNS static entry for the each Managed name and associated Managed IP address.

In High Availability solutions, the managed IP address must be lower than the active and standby server IP addresses. For example, if the active server IP address is 1.2.3.4 and the standby server IP address is 1.2.3.5, the managed IP address is 1.2.3.3.

A typical High Availability campus solution with a pair of HA servers requires 3 DNS static entries; one DNS static entry for the active server, one DNS static entry for the standby server, and one DNS static entry for the Managed name and associated IP address.

If your solution is going to have a Remote Geographic Node (RGN) server, ask your System Administrator to add a Domain Name System (DNS) static entry for the RGN server.

Perform this procedure on the active server. Perform this procedure on the standby server if you have one. Perform this procedure on the RGN server if you have one.

Procedure

1. Log on to the active server.
2. Open Windows Explorer.
3. Go to the folder C:\Windows\system32\drivers\etc.
4. Double-click on the **hosts** file, select **Open**, and select **Notepad**.

   The hosts file opens in Notepad.
5. Add the Managed IP address and the Managed server name to the hosts file.

   Important:

   The Managed server name can be a full name or netbios server name.
6. If you have a standby server, repeat the above steps on the Standby server.
7. If you have an RGN server, repeat the above steps on the RGN server.

Installing a third-party utility to support High Availability

About this task

Install a third-party utility required by the Avaya Aura® Contact Center High Availability feature.

Perform this procedure on the Active and Standby servers.

Procedure

1. Log on to the Active Server.
2. Retrieve the WinPcap installer from a server with CCMS.

   The WinPcap installer is located at: `<installation drive>:\Avaya\Contact Center\Manager Server\CCSMMC\thirdparty\winpcap`.
3. Save it on the CCMM server you are commissioning.
4. On the CCMM server, using Windows Explorer, navigate to the location you had saved the `WinPcap_4_1_3.exe` file in step 3.
5. Double-click **WinPcap_4_1_3.exe**.
6. On the WinPcap installer dialog, click **Next**.
7. On the WinPcap installer Setup Wizard dialog, click **Next**.
8. On the WinPcap installer License Agreement dialog, click **I Agree**.
9. On the WinPcap installer Installation options dialog, click **Install**.
10. On the WinPcap installer dialog, click **Finish**.
11. Repeat this procedure on the Standby Server.

Configuring CCMM General Administration

About this task

In a multimedia-enabled solution, Avaya Agent Desktop client software is typically downloaded from Contact Center Multimedia (CCMM). Agent Desktop then communicates with CCMM to handle email-based contacts. Agent Desktop communicates with Communication Control Toolkit (CCT) to handle voice contacts.

In a multimedia-enabled High Availability solution, use the CCMM Administration tool to configure standby CCMM and CCT details. Avaya Agent Desktop client software downloads these standby CCMM and CCT details and communicates with them if it cannot communicate with the active CCMM and CCT.

Important:

Before changes to the CCMM server settings take effect, you might need to restart the CCMM server.

Procedure

1. On the active Multimedia Contact Server, log in to the Contact Center Manager Administration application and click **Multimedia**.
2. In the left column, select **General Administration**.
3. Click **Server Settings**.
4. Configure the **Contact Center Manager Server** entry with the managed IP address of the Voice and Multimedia Contact Server High Availability pair.
5. Configure the **Contact Center License Server** entry with the managed IP address or managed name of the Voice Contact Server High Availability pair.
6. Configure the **Contact Center Manager Administration** entry with the managed name of the Voice Contact Server High Availability pair.
7. Configure the **Contact Center Multimedia Server** entry with the managed IP address or managed name of the Multimedia Contact Server High Availability pair.
8. If your solution has a Remote Geographic Node Multimedia Contact Server, enter its name or IP address in the **Geographic Standby CCMM Server** field.
9. Configure the **Communication Control Toolkit Server** entry with the IP address of your primary Voice Contact Server.
10. Configure the **Standby CCT Server** entry with the IP address of your standby Voice Contact Server.
11. If you are using a Remote Geographic Node server, configure the **Geographic Standby CCT Server** entry.

    Alternatively, if the Geographic Standby CCT Server does not exist, click **New** to create one.
12. Configure the **CC Web Stats** entry.

    If the Contact Center Web Statistics Server details do not exist and your solution uses Web Statistics, click **New**. Use the managed IP address of the optional Web Statistics server. The default port number is 9086.
13. In the left column, select **Email**.
14. Click **General Settings**.
15. Ensure that the Inbound URL is of the form `http://<ManagedIPAddress>/inboundattachment`.
16. Ensure that the Outbound URL is of the form `http://<ManagedIPAddress>/outboundattachment`.

Variable definitions

Name	Description
Contact Center Manager Server	Enter the Managed IP address or managed name of the CCMS High Availability server pair.
Contact Center Multimedia Server	Enter the Managed IP address or managed name of the CCMM High Availability server pair.
Geographic Standby CCMM Server	Enter the IP address or name of the Remote Geographic Node CCMM server, if your solution has one.
Communication Control Toolkit Server	Enter the name or IP address of your primary CCT server in the Communication Control Toolkit Server box.
Standby CCT Server	Enter the name or IP address of your standby CCT server in the Communication Control Toolkit Server box.
Geographic Standby CCT Server	Enter the name or IP address of the Remote Geographic Node CCT server.
CC Web Stats	The Managed IP address or managed name of the optional Web Statistic server that agents and supervisors use to view real-time statistics for call handling, skillset data, and the state information on the Agent Desktop. This is typically the Managed IP address or managed name of the CCMS server.

Configuring the Active Server

About this task

The Active Server is configured using the High Availability utility. This utility saves IP information for the Active Server to the database.

Procedure

1. From the **Start** menu, in the Avaya area, click **High Availability**.
2. Expand **Configuration**.
3. Double-click **Server Mode**.
4. Under **Server Mode**, select **Active**.
5. Under **Server Mode Configuration**, in the text box, type the maximum length of time the network connectivity tests can continue to fail consecutively before corrective action is considered.
6. Under **Server Mode Configuration**, from the drop down list, select the unit of time for the network connectivity tests.
7. Under **IP Configuration**, type the **Managed IP**, **CLAN** IP address.
8. Under **IP Configuration**, type the **Active Server details**, **CLAN** IP address.

9. Under **IP Configuration**, type the **Standby Server details**, **CLAN** IP address.
10. In the **Trusted IP** box, type the IP **Address** of the trusted server.
11. In the **Address** box, type the IP address of the optional **Remote Geographic Node**.
12. Click **Save**.

    A system message box appears. You must stop the system before you save any information.
13. Click **Yes** to stop the system.
14. Click **OK** to save the data.

Variable definitions

Name	Description
Server Mode Configuration - Network Timeout	The High Availability—Network Timeout value sets the maximum length of time the network connectivity test can continue to fail consecutively, before corrective action is considered. The default value is 60 seconds. Avaya recommends that you set Network Timeout high enough to be tolerant of normal network latency, but low enough to be responsive if a failure occurs.
Managed IP	The Managed IP (MIP) address that is used for both the Active and Standby servers for campus resiliency. The Active Server is always assigned the MIP. If a switchover occurs, the MIP is assigned to the new Active Server. Agents and other applications are not aware that a switchover occurred because the IP address does not change. A MIP is used only when the Active and Standby servers are in the same subnet.
Active Server details	The IP address for the server initially configured in Active mode.
Standby Server details	The IP address for the server initially configured in Standby mode.

Table continues…

Name	Description
Trusted Address	The Active and Standby servers use the Trusted IP address to verify network connectivity. If the Active server cannot communicate with the Standby server it attempts to communicate with the Trusted IP address. If the Active Server cannot connect to the Trusted IP address on startup then no Contact Center services start on that server. If the Active server cannot communicate with the Trusted IP address, and if shadowing and switchover are enabled, then the Active server stops processing contacts and shuts down. The Standby server starts processing contacts if it cannot communicate with the Active server but can communicate with the Trusted IP address. Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.
Remote Geographic Node	The IP address of the optional Remote Geographic Node.

Backing up the Active Server database

About this task

Use the Database Maintenance utility on to back up the Active Multimedia Contact Server database. The backup of the database is restored to the Standby Server.

Important:

Do not use a folder on the Active or Standby servers as the backup location.

Procedure

1. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
2. Click **Backup Locations**.
3. Click **Create**.
4. From the **Drive Letter** list, select the network drive on which you want to store the CCMM database.
5. In the **UNC Path** box, type the location to store the backup, in the format `\\Computer Name\Backup Location`.

Important:

Do not use the same backup folder for your Voice Contact Server and Multimedia Contact Server databases, because databases stored in the same backup location overwrite each other.

This location must be a shared folder with correct permissions.

6. In the **User Name** box, type the user name used to log on to the computer specified in the UNC Path box.

   The user name is in the format `Computer Name\Account Name`.

7. In the **Password** box, type the domain password.
8. In the left pane, click **Immediate Backup**.
9. In the **Media Type** section, select **Network Location**.
10. In the **Application** section, select **Offline**.
11. From the **Backup Location** list, select the network drive on which to store the backup.
12. Click **Backup**.

Restoring the database on the Standby Server

Before you begin

- When CCMM is installed, the license type is NODAL. If you have a Corporate (CORP) license this must be set on the standby server, before the active server backup is restored on to the standby machine.

Important:

Restoring the ADMIN database can change configuration of Backup locations on the Standby Server, if the Active Server and Standby Server backup locations are different. After you restore the ADMIN database, close and reopen the Database and Maintenance utility.

About this task

Restore the database from the Active Server to the Standby Server to ensure the databases are consistent. The Database Maintenance utility can restore all application databases at once.

You must restore the CCMM and ADMIN databases to the Standby Server.

Procedure

1. Log on to the Standby Server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. In the **Database Maintenance** dialog box, in the left pane, click **Restore**.

4. In the right pane, under **Media Type**, select the media type on which the backup is restored.
5. If the backup file is on the network drive, in the **Backup Location** list, select the backup location.
6. Under **Application**, select **CCMM** and **ADMIN**.
7. Under **Restore contents**, select **Data** and **Offline**.
8. Click **Restore**.
9. Use the **Information** field to monitor the progress of the restoration.
10. Click **Exit** to close the Database Maintenance utility.

Configuring the Standby Server

Before you begin

- The database from the Active server has been restored to the Standby Server.

About this task

Configure the Standby Multimedia Contact Server. The Standby Multimedia Contact Server must be shadowing the Active Multimedia Contact Server for switchover to occur, if the Active server fails. While the Standby server is shadowing the Active server, it maintains a near real-time local copy of the CCMM and Administration databases. Therefore, the Standby Server is configured with the most recent data and it can take over from the Active Server if necessary.

Procedure

1. Log on to the Standby Server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. In the left pane, click **Server Mode**.
4. In the **Server Mode Configuration** section, select **Standby**.
5. Under **IP Configuration**, type the **Active Server details**, **CLAN** IP address.
6. Under **IP Configuration**, type the **Standby Server details**, **CLAN** IP address.
7. Under **IP Configuration**, under **Trusted IP**, type the Trusted IP address.
8. Click **Save**.

   A system message box appears. You must stop the system before you save any information.
9. Click **OK**.

Starting the Active Server

About this task

Start the Active Server using the CC Applications tab in the High Availability utility. Starting the Active Server starts the system processes.

Procedure

1. Log on to the Active Server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Configuration**.
4. Under **Server Mode Configuration**, select **Switchover**.
5. Expand **Tasks**.
6. Double-click **CC Applications**.
7. In the first box under **CC Applications**, select the system.
8. Click **Start**.
9. Click **OK**.

Starting shadowing on the Standby Server

About this task

Use the High Availability utility to start shadowing on the Standby Server.

Important:

You must backup the Active server database, restore it onto the Standby server, and enable shadowing within 24 hours. If the difference in time between the Active and Standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the Active server database and restore it onto the Standby server before re-enabling shadowing. Ensure that the system clock time on the Active and Standby servers are synchronized.

Procedure

1. Log on to the Contact Center Multimedia standby server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Configuration**.
4. In **Server Mode Configuration**, select **Switchover**.
5. Under **Tasks**, click **System Control**.
6. Beside **Control**, select **Shadowing**.

7. Click **Start**.

Verifying shadowing is running on the Active Server

About this task

The system information tab of the High Availability utility displays system information regarding the Active and the Standby servers. The dialog box displays the following information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information
- Remote server connection status
- Remote server port information
- License information
- Databases shadowed
- Time of last record shadowed
- Database namespaces
- Local and remote information on system status, switchover, shadowing, and network.
- CC Application install information
- Database space and journaling information
- Database processes information
- Standby Server WebChat State, if you have Enterprise Web Chat licensed

Use this procedure to verify the settings.

Procedure

1. Log on to the Active Server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Configuration**.
4. Select **System**.
5. Select **Get System Configuration**.

   The most recent system information appears.
6. Under the **Shadowing** section, view the time of the most recent shadowed record.

   Ensure it has an up-to-date time, which corresponds with when shadowing was started.

Testing a switchover

About this task

When the Multimedia Contact Server commissioning is complete, you can test the CCMM switchover to ensure that it works.

Procedure

1. Log on to the Active Multimedia Contact Server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. On the Active Server, select **System Control**.
4. Under **Control**, select **Switchover** to initiate a manual switchover.
5. Send a test email to one of the CCMM configured mailboxes.

   After the email is received on the new Active Server, the test is successfully completed.

Next steps

Avaya recommends that you analyze your network performance after running HA for a number of days. Use the Network Analyzer utility to analyze the SMMC logs and verify whether your Network Timeout value is set correctly for your network performance. For more information about using the Network Analyzer utility to optimize the High Availability configuration settings on network, see *Troubleshooting Avaya Aura® Contact Center*.

Chapter 27: Geographic High Availability Multimedia Contact Server commissioning

This section describes how to configure geographic High Availability for Multimedia Contact Servers in a geographic Wide Area Network solution.

You must complete all the procedures in this section in sequential order.

In geographic Wide Area Network solutions the standby server on the remote geographic site is called a Remote Geographic Node (RGN) server. The active Multimedia Contact Server and the Remote Geographic Node Multimedia Contact Server are part of the same Avaya Aura® Contact Center solution but they are typically in different geographic locations and subnets.

If you have High Availability (HA) at the campus, there is also a standby Multimedia Contact Server in the same campus location. The standby Multimedia Contact Server shadows the active Multimedia Contact Server. If the active Multimedia Contact Server fails the standby Multimedia Contact Server takes over call processing on the local site.

The RGN Multimedia Contact Server on the remote site shadows the active server on the campus site. If the active server fails, the standby server assumes the shared Managed IP address and starts processing calls. The Remote Geographic Node server monitors the campus Managed IP address so it continues shadowing.

Geographic High Availability Multimedia Contact Server commissioning overview:

In a geographic High Availability server configuration, one Multimedia Contact Server is the active server and one server is the RGN. The active Multimedia Contact Server actively processes contacts. The RGN server shadows the active server. If the active Multimedia Contact Server fails, the RGN Multimedia Contact Server does not start processing contacts. You must start the RGN server manually.

The RGN and active servers must have the same patch level and the same hard disk drive partitions.

Prerequisites

- Ensure unused Network Interface Cards (NICs) are disabled.

- Install Contact Center Multimedia software on the active and Remote Geographic Node servers.
- Install a Voice Contact Server High Availability pair to provide the core functionality for this Multimedia Contact Server.
- Commission Contact Center Multimedia. See Contact Center Multimedia server commissioning on page 192.
- Know how to configure the High Availability settings.
- CCMM stores license information in the registry. Configure CCMM licensing on the Remote Geographic Node CCMM server, after restoring the database from the active server. See Contact Center Multimedia server commissioning on page 192.
- Ensure the Remote Geographic Node server IP addresses are configured in CCMM General Administration on the active server. For more information, see Configuring CCMM General Administration on page 355.

High Availability commissioning checklist

The following is a list of key configuration items required for High Availability commissioning in a SIP-enabled contact center environment.

Item	Your value	Description
Ensure that Contact Center is licensed for High Availability		High Availability is a licensed feature and is enabled when you purchase a standby server license.
Active server host name		The name of your AACC active server.
Active server IP address		The IP address of your AACC active server.
Standby server host name		If you have HA at the campus site, the name of your AACC standby server.
Standby server IP address		If you have HA at the campus site, the IP address of your AACC standby server.
Managed name		If you have HA at the campus site, the managed name of your AACC campus HA pair.
Managed IP address		If you have HA at the campus site, the managed IP address of your AACC campus HA pair.

Table continues…

Item	Your value	Description
Using Hosts file or DNS?		If you are using the Hosts files to resolve Managed names to Managed IP addresses, ensure that you add the Managed names and Managed IP addresses to the Hosts file.
Trusted IP address		Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.
RGN server host name		If you have HA geographic redundancy, the name of your AACC RGN server.
RGN server IP address		If you have HA geographic redundancy, the IP address of your AACC RGN server.
Using email notification?		You can enable automatic email switchover notifications to alert the Contact Center administrator. When enabled, the specified email address receives an automatic email which provides switchover information to the recipient.
SMTP server name		The name of your SMTP server for email notification after an automatic switchover occurs.
Email Username		The log on name of an email user configured on the email server.
Email Password		The password of an email user configured on the email server.
Email address to send notifications from		The email address that the email notification is sent from.
Email address to send notifications to		The email address that the email notification is sent to.
Database backup location		The location of the shared folder where you store database backups. This folder must not be on the active or standby servers.

Resolving the Managed name to the Managed IP address

About this task

Complete the following procedure to resolve the Managed server name to the Managed IP address. If the server has two network interfaces, apply these settings to the CLAN network interface. Each Contact Center server in a domain requires a DNS static entry.

Important:

Avaya Aura® Contact Center High Availability solutions do not support Dynamic DNS.

Ask your System Administrator to add a Domain Name System (DNS) static entry for the active and standby servers and one additional DNS static entry for the each Managed name and associated Managed IP address.

In High Availability solutions, the managed IP address must be lower than the active and standby server IP addresses. For example, if the active server IP address is 1.2.3.4 and the standby server IP address is 1.2.3.5, the managed IP address is 1.2.3.3.

A typical High Availability campus solution with a pair of HA servers requires 3 DNS static entries; one DNS static entry for the active server, one DNS static entry for the standby server, and one DNS static entry for the Managed name and associated IP address.

If your solution is going to have a Remote Geographic Node (RGN) server, ask your System Administrator to add a Domain Name System (DNS) static entry for the RGN server.

Perform this procedure on the active server. Perform this procedure on the standby server if you have one. Perform this procedure on the RGN server if you have one.

Procedure

1. Log on to the active server.
2. Open Windows Explorer.
3. Go to the folder C:\Windows\system32\drivers\etc.
4. Double-click on the **hosts** file, select **Open**, and select **Notepad**.

   The hosts file opens in Notepad.
5. Add the Managed IP address and the Managed server name to the hosts file.

   Important:

   The Managed server name can be a full name or netbios server name.
6. If you have a standby server, repeat the above steps on the Standby server.
7. If you have an RGN server, repeat the above steps on the RGN server.

Installing a third-party utility to support High Availability

About this task

Install a third-party utility required by the Avaya Aura® Contact Center High Availability feature.

Procedure

1. Log on to the Remote Geographic Node Server.
2. Retrieve the WinPcap installer from a CCMS server.

The WinPcap installer is located at: `<installation drive>:\Avaya\Contact Center\Manager Server\CCSMMC\thirdparty\winpcap`.

3. Save it on the CCMM server you are commissioning.
4. On the CCMM server, using Windows Explorer, navigate to the location you had saved the `WinPcap_4_1_3.exe` file in step 3.
5. Double-click **WinPcap_4_1_3.exe**.
6. On the WinPcap installer dialog, click **Next**.
7. On the WinPcap installer Setup Wizard dialog, click **Next**.
8. On the WinPcap installer License Agreement dialog, click **I Agree**.
9. On the WinPcap installer Installation options dialog, click **Install**.
10. On the WinPcap installer dialog, click **Finish**.

Configuring the active server

About this task

Configure the active server using the High Availability utility. This utility saves IP information for the active server to the database.

Procedure

1. From the **Start** menu, in the Avaya area, click **High Availability**.
2. Expand **Configuration**.
3. Double-click **Server Mode**.
4. Under **Remote Geographic Node**, in the **Address** box, type the IP address of the Remote Geographic Node server.
5. Click **Save**.

   A system message box appears. You must stop the system before you save any information.
6. Click **Yes** to stop the system.

Variable definitions

Name	Description
Server Mode Configuration - Network Timeout	The High Availability—Network Timeout value sets the maximum length of time the network connectivity test can continue to fail consecutively, before corrective action is considered. The default value is 60 seconds. Avaya recommends that you set Network Timeout high enough to be tolerant of normal network latency, but low enough to be responsive if a failure occurs.
Managed IP	The Managed IP (MIP) address that is used for both the active and standby servers for campus resiliency. The active server is always hosts the MIP. If a switchover occurs, the new active server hosts the MIP. Agents and other applications are not aware that a switchover occurred because the IP address does not change. A MIP is used only when the active and standby servers are in the same subnet.
Active Server details	The IP address for the server initially configured in Active mode.
Standby Server details	The IP address for the server initially configured in Standby mode.
Trusted IP address	Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.
Remote Geographic Node	The IP address of the optional Remote Geographic Node.

Backing up the active server database

About this task

Use the Database Maintenance utility to back up the active Multimedia Contact Server database. The backup of the database is restored to the Remote Geographic Node server.

Important:

Do not use a folder on the active or standby servers as the backup location.

Procedure

1. Log on to the active Multimedia Contact Server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. Click **Backup Locations**.
4. Click **Create**.
5. From the **Drive Letter** list, select the network drive on which you want to store the CCMM database.
6. In the **UNC Path** box, type the location to store the backup, in the format `\\Computer Name\Backup Location`.

   This location must be a shared folder with correct permissions.

   Important:

   Do not use the same backup folder for your Voice Contact Server and Multimedia Contact Server databases, because databases stored in the same backup location overwrite each other.
7. In the **User Name** box, type the user name used to log on to the computer specified in the UNC Path box.

   The user name is in the format `Computer Name\Account Name`.
8. In the **Password** box, type the domain password.
9. In the left pane, click **Immediate Backup**.
10. In the **Media Type** section, select **Network Location**.
11. In the **Application** section, select **Offline**.
12. From the **Backup Location** list, select the network drive on which to store the backup.
13. Click **Backup**.

Configuring RGN CCMM General Administration

About this task

Configure the Remote Geographic Node CCMM to use local telephony and multimedia resources.

Important:

Changes to the RGN CCMM settings might require an RGN server restart before they take effect.

Procedure

1. In Contact Center Manager Administration, from **Launchpad**, select **Configuration** .

2. Add the RGN Contact Center Multimedia as a CCMM server.
3. From **Launchpad**, select **Multimedia**.
4. In the left column, click the RGN Multimedia server.
5. Click **Launch Multimedia Client**.
6. In the left column, select **General Administration**.
7. Click **Server Settings**.
8. Change the **Contact Center Manager Server** entry to the IP address or name of the Remote Geographic Node Voice Contact Server.
9. Change the **Contact Center License Server** entry to the IP address or name of the Remote Geographic Node Voice Contact Server.
10. Change the **Contact Center Manager Administration** entry to the IP address or name of the Remote Geographic Node Voice Contact Server.
11. Change the **Contact Center Multimedia Server** entry to the IP address or name of the Remote Geographic Node Multimedia Contact Server.
12. Change the **Geographic Standby CCMM Server** entry to not configured.
13. Change the **Communication Control Toolkit Server** entry to the IP address or name of the Remote Geographic Node Voice Contact Server.
14. Change the **Standby CCT Server** entry to not configured.
15. Change the **Geographic Standby CCT Server** entry to not configured.
16. Configure the **CC Web Stats** entry.

    If the Contact Center Web Statistics Server details do not exist and your solution uses Web Statistics, click **New**. The default port number is 9086.
17. In the left column, select **Email**.
18. Click **General Settings**.
19. Ensure that the Inbound URL is of the form `http://<RGNIPAddress>/inboundattachment`, where *RGNIPAddress* is the IP address of the Remote Geographic Node Voice and Multimedia Contact Server.
20. Ensure that the Outbound URL is of the form `http://<RGNIPAddress>/outboundattachment`, where *RGNIPAddress* is the IP address of the Remote Geographic Node Voice and Multimedia Contact Server.
21. In Contact Center Manager Administration, from **Launchpad**, select **Configuration** .
22. Delete the RGN CCMM server.

Variable definitions

Name	Description
Contact Center Manager Server	Enter the IP address or name of the RGN CCMS server.
Contact Center Multimedia Server	Enter the IP address or name of the RGN CCMM server.
Contact Center License Server	Enter the IP address or name of the RGN License Manager (LM) server.
Contact Center Multimedia Standby Server	Not Configured.
Communication Control Toolkit Server	Enter the IP address or name of your RGN CCT server.
Standby CCT Server	Not Configured.
Geographic Standby CCT Server	Not Configured.
CC Web Stats	The name of the optional Web Statistics server that agents and supervisors use to view real-time statistics for call handling, skillset data, and the state information on the Agent Desktop. This is typically the CCMS server.

Configuring the Remote Geographic Node server

About this task

Configure the Remote Geographic Node (RGN) Multimedia Contact Server.

Procedure

1. Log on to the RGN server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. In the left pane, click **Server Mode**.
4. In the **Server Mode Configuration** section, select **RGN**.
5. If you do not have HA at the campus site, in the **Campus details** section, in the **CLAN** box, type the IP address of the active server.
6. If you have HA at the campus site, in the **Campus details** section, in the **CLAN** box, type the Managed IP address for the campus server pair.
7. In the **Remote Geographic Node details** section, in the **CLAN** box, type the CLAN IP address of the RGN server.
8. In the **Trusted IP** section, in the **Address** box, type the trusted IP address.
9. Click **Save**.

   A system message box appears. You must stop the system before you save any information.

10. Click **OK**.

Restoring the database on the Remote Geographic Node server

Before you begin

- When CCMM is installed, the license type is NODAL. If you have a Corporate (CORP) license, this must be set on the Remote Geographic Node (RGN) server, before the active server backup is restored on to the RGN server.

About this task

Restore the database from the active server to the RGN server to ensure the databases are consistent. The Database Maintenance utility can restore all application databases at once.

You must restore the CCMM and ADMIN databases to the RGN server.

Important:

Restoring the ADMIN database can change configuration of backup locations on the RGN Server, if the Active server and RGN server backup locations are different. After you restore the ADMIN database, close and reopen the Database Maintenance utility.

Procedure

1. Log on to the RGN server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. In the **Database Maintenance** dialog box, in the left pane, click **Restore**.
4. In the right pane, under **Media Type**, select the media type on which the backup is restored.
5. If the backup file is on the network drive, in the **Backup Location** list, select the backup location.
6. Under **Application**, select **CCMM** and **ADMIN**.
7. Under **Restore contents**, select **Data** and **Offline**.
8. Click **Restore**.
9. Use the **Information** field to monitor the progress of the restoration.
10. Click **Exit** to close the Database Maintenance utility.

Starting the active server

About this task

Start the active server using the CC Applications tab in the High Availability utility. Starting the active server starts the system processes.

Procedure

1. Log on to the active server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Tasks**.
4. Double-click **CC Applications**.
5. In the first box under **CC Applications**, select the system.
6. Click **Start**.
7. Click **Save**.

Starting shadowing on the Remote Geographic Node server

About this task

Use the High Availability utility to start shadowing on the Remote Geographic Node (RGN) server.

Important:

You must backup the active server database, restore it onto the RGN server, and enable shadowing within 24 hours. If the difference in time between the active and RGN server database content is greater than 24 hours, then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the active server database and restore it onto the RGN server before re-enabling shadowing. Ensure that the system clock times on the active and RGN servers are synchronized.

Procedure

1. Log on to the Contact Center Multimedia RGN server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Configuration**.
4. Beside **Control**, select **Shadowing**.
5. Click **Start**.

Verifying shadowing is running on the active server

About this task

The system information tab of the High Availability utility displays system information regarding the active and the Remote Geographic Node (RGN) servers. The dialog box displays the following information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information
- Remote server connection status
- Remote server port information
- License information
- Databases shadowed
- Time of last record shadowed
- Database namespaces
- Local and remote information on system status, switchover, shadowing, and network.
- CC Application install information
- Database space and journaling information
- Database processes information

Use this procedure to verify the settings.

Procedure

1. Log on to the active Multimedia Contact Server.
2. From the **Start** menu, in the Avaya area, click **High Availability**.
3. Expand **Configuration**.
4. Select **System**.
5. Select **Get System Configuration**.

   The most recent system information appears.
6. Under the **Shadowing** section, view the time of the most recent shadowed record.

   Ensure it has an up-to-date time, which corresponds with when shadowing was started.

Chapter 28: High Availability Network Control Center commissioning

Configure High Availability (HA) resiliency for a pair of Network Control Center (NCC) servers to improve solution resiliency. Network Control Center High Availability ensures access to uninterrupted and consolidated reports across multiple nodes in your contact center. Network Control Center supports the Hot-standby level of High Availability only; Mission Critical High Availability is not supported.

High Availability Network Control Center commissioning overview

Network Control Center High Availability is configured using the High Availability Utility. In an Avaya Aura® Contact Center solution containing a pair of Network Control Center servers, one NCC server is the active server and one is the standby server. The standby server shadows the active server. If the active server fails, the standby server, running in standby mode, recognizes the failure and becomes the active server.

The standby server must be configured the same as the active server. The standby and active servers must have the same patch level and the same hard disk drive partitions.

In a Network Control Center High Availability solution, a hardware, network or database failure can initiate a swithover, but only in the following situations:

- The switchover check box on both servers is selected.
- The standby server is shadowing the active server.
- A valid license file containing standby server license information for NCC exists to allow a switchover.

Administrator experience during a switchover

If a switchover occurs during the addition of a Network Control Center site, synchronization of the sites can fail. If the flag status of the sites you add during a switchover do not update, add the sites to the Network Control Center again. See Configuring the sites on page 57.

Managed IP Address

A Managed IP address is a virtual IP address that is attached to a network adapter on the active server. Each High Availability application server is assigned a static IP address. After the active server in each replication pair is determined, the active server attaches a Managed IP address to the network interface. The managed IP address is only assigned to the active server and it is used by all other contact center applications and clients to connect to that application. The standby server assumes this same managed IP address if it takes over processing and becomes the active server. The active server stops using the Managed IP when it stops being the active server.

High Availability Utility

Configure High Availability resiliency for NCC using the High Availability Utility in the Database Utilities. The High Availability Utility is used to configure which server is the active and which is the standby server. The HA utility also configures the Managed IP of the active server.

The High Availability Utility on an Active server allows you to:

- Configure the managed IP address
- Configure the IP address for the Active and Standby servers
- Configure the IP address for the Trusted server
- Identify if the server is Active or Standby
- Enable automatic switchover
- Configure the switchover time-out. This is the wait time if a network outage occurs before an automatic switchover occurs
- Configure an email server for email notifications
- Configure where and how often to send email notifications
- Configure the email character set
- Verify that shadowing is running
- Start or stop the system
- Enable or disable CC applications
- Display system information

Configuring High Availability on an existing standalone NCC solution

If you have a standalone NCC server and you want to configure HA, in addition to the procedures in this chapter, you must also perform the following steps:

- Obtain a new NCC HA license before you configure HA, and use License Manager to update the license file.
- When you configure HA on the active server, use the IP address of the existing standalone NCC server as the new managed IP address. You must run the Server Configuration utility after performing this step on the active server.

  Important:

  If you change the IP address of the existing NCC HA server, you must re-configure your NCC solution. For more information about configuring NCC, see *Avaya Aura® Contact Center Server Administration*.
- After completing HA configuration, on the active and standby servers validate the connection to the nodal servers using the Nbconfig utility.

Prerequisites for High Availability Network Control Center commissioning

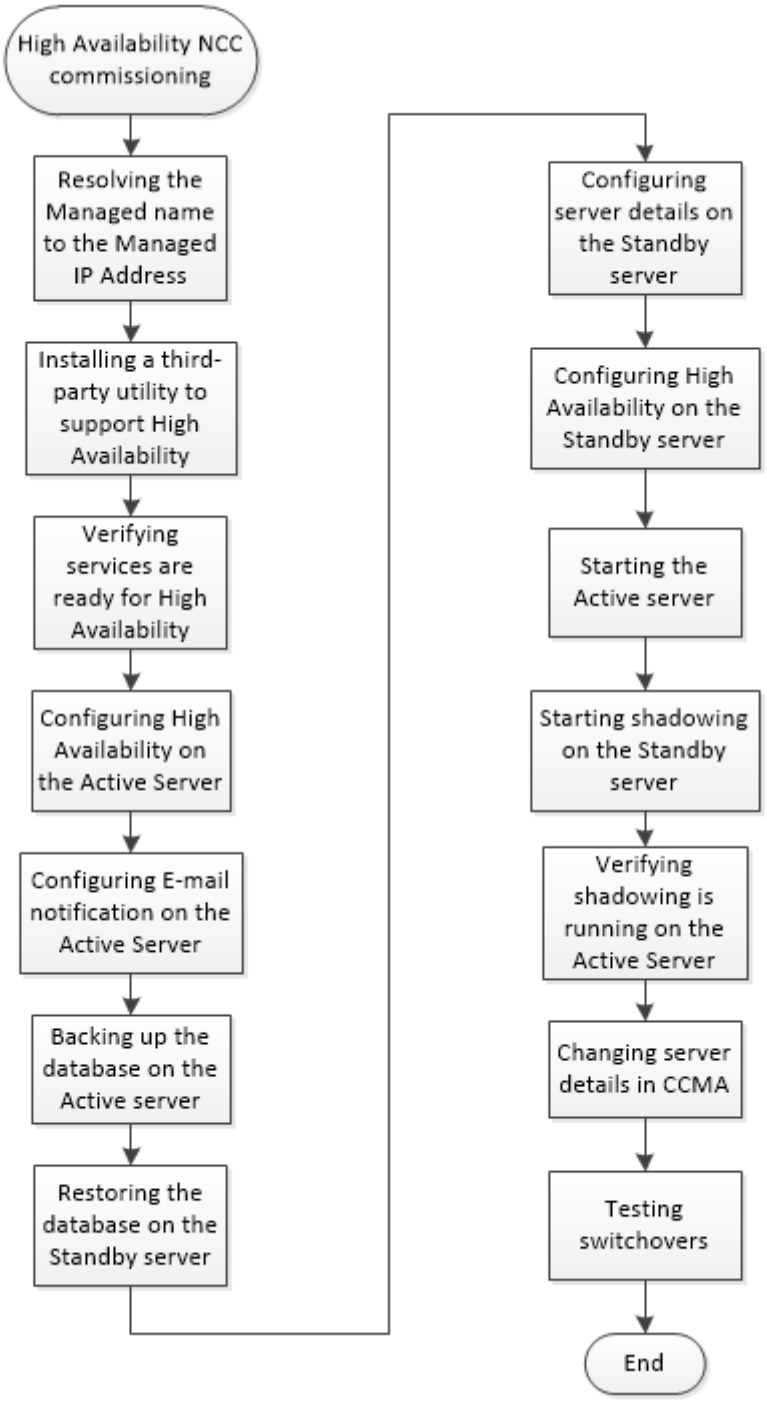
- The active and standby servers must meet the planning and engineering specifications. For more information, see *Avaya Aura® Contact Center Overview and Specification*.
- Ensure unused Network Interface Cards (NICs) are disabled.
- Install NCC on the Active and Standby servers using the same drive specification on each server.
- Configure NCC on the Active and Standby servers. For more information, see Network Control Center commissioning on page 57.
- Patch the active and standby servers. The active and standby servers must be patched to the same patch level. For more information, see *Upgrading and Patching Avaya Aura® Contact Center*.

High Availability Network Control Center commissioning procedures

About this task

This task flow shows you the sequence of procedures you perform to commission Network Control Center for High Availability.

Figure 41: High Availability Network Control Center commissioning procedures


High Availability NCC commissioning
Resolving the Managed name to the Managed IP Address
Installing a third-party utility to support High Availability
Verifying services are ready for High Availability
Configuring High Availability on the Active Server
Configuring E-mail notification on the Active Server
Backing up the database on the Active server
Restoring the database on the Standby server
Configuring server details on the Standby server
Configuring High Availability on the Standby server
Starting the Active server
Starting shadowing on the Standby server
Verifying shadowing is running on the Active Server
Changing server details in CCMA
Testing switchovers
End

Resolving the Managed name to the Managed IP Address

About this task

Complete the following procedure on the Active and Standby servers to resolve the Managed server name to the Managed IP address using the Windows hosts file. Each Contact Center server in a domain requires a DNS static entry.

Important:

Avaya Aura® Contact Center High Availability solutions do not support Dynamic DNS.

Ask your System Administrator to add a Domain Name System (DNS) static entry for the Active and Standby servers and one additional DNS static entry for the each Managed name and associated Managed IP address.

In High Availability solutions, the managed IP address must be lower than the active and standby server IP addresses. For example, if the active server IP address is 1.2.3.4 and the standby server IP address is 1.2.3.5, the managed IP address is 1.2.3.3.

A typical High Availability campus solution with a pair of NCC servers requires three DNS static entries; one DNS static entry for the active server, one DNS static entry for the standby server, and one DNS static entry for the Managed name and associated IP address.

Perform this procedure on the Active and Standby servers.

Procedure

1. Open Windows Explorer.
2. Go to the folder C:\Windows\system32\drivers\etc.
3. Double-click on the **hosts** file, click **Open**, and select **Notepad**.

   The hosts file opens in Notepad.
4. Add the Managed IP address and the Managed server name to the hosts file.

   Important:

   The Managed Server name can be a full name or netbios server name.

Installing a third-party utility to support High Availability

About this task

Install a third-party utility required by the Avaya Aura® Contact Center High Availability feature.

Important:

Perform this procedure on the Active and Standby servers.

Procedure

1. Log on to the Active server.

2. Using Windows Explorer, navigate to `<installation drive>:\Avaya\Contact Center \Manager Server\CCSMMC\thirdparty\winpcap`.
3. Double-click **WinPcap_4_1_2.exe**.
4. On the WinPcap installer dialog, click **Next**.
5. On the WinPcap installer **Setup Wizard** dialog, click **Next**.
6. On the WinPcap installer **License Agreement** dialog, click **I Agree**.
7. On the WinPcap installer **Installation options** dialog, click **Install**.
8. On the WinPcap installer dialog, click **Finish**.
9. Repeat this procedure on the Standby server.

Verifying services are ready for High Availability

About this task

Verify that all NCC services stop before you configure High Availability.

Perform this procedure on the Active and Standby servers.

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **System Control and Monitor Utility**.
3. On the **CCMS** tab, check that all services are stopped.
4. If any service is running, click **Stop CCMS**.
5. Repeat this procedure on the Standby server.

Configuring High Availability on the Active Server

About this task

Configure High Availability resiliency on the Active Server using the High Availability utility.

Procedure

1. Select one Network Control Center server to be the active server and log on.
2. Click **Start** > **All Programs** > **Avaya** > **High Availability**.
3. Expand **Configuration**.
4. Double-click **Server Mode**.

5. Under **Server Mode Configuration**, select **Active**.
6. Under **Server Mode Configuration**, select the **Switchover** check box.
7. Under **Server Mode Configuration**, in the text box, type the maximum length of time the network connectivity tests can continue to fail consecutively before corrective action is considered.
8. Under **Server Mode Configuration**, from the drop down list, select the unit of time for the network connectivity tests.
9. Under **IP Configuration**, type the **Managed IP** and **CLAN** IP address. Leave the **ELAN** IP address box blank.
10. Under **IP Configuration**, type the **Active Server details CLAN** IP address. Leave the **ELAN** IP address box blank.
11. Under **IP Configuration**, type the **Standby Server details**, **CLAN** IP address. Leave the **ELAN** IP address box blank.
12. In the **Address** box, type the IP address of the **Trusted IP** server.
13. Click **OK**.

    A system message box appears. You must stop the system before you save any information.
14. Click **Yes** to stop the system.

Variable definitions

Name	Description
Network Timeout	The High Availability feature tests network connectivity between HA components by default every 100 milliseconds (100ms). The High Availability—Network Timeout value sets the maximum length of time these network connectivity tests can continue to fail consecutively before corrective action is considered. For example, if Network Timeout is set to 1s, HA requires 10 consecutive failed network connectivity tests before the remote system is marked as unreachable. In this case, if switchovers are enabled, an attempt to switch over is made. Avaya recommends that you set Network Timeout high enough to be tolerant of normal network latency, but low enough to be responsive if a failure occurs.
Active CLAN	The IP address for the server initially configured in Active mode.

Table continues…

Name	Description
Standby CLAN	The IP address for the server initially configured in Standby mode.
Managed IP	The virtual Managed IP (MIP) address that is used by the Active Server for campus resiliency. A MIP is used only when the Active and Standby servers are in the same subnet.
Trusted IP	The Active and Standby servers use the Trusted IP address to verify network connectivity. If the Active server cannot communicate with the Standby server it attempts to communicate with the Trusted IP address. If the Active server cannot communicate with the Trusted IP address, if shadowing and switchover are enabled, then the Active server stops processing contacts and shuts down. The Standby server starts processing contacts if it cannot communicate with the Active server but can communicate with the Trusted IP address. Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.
Remote Geographic Node	The IP address of the optional Remote Geographic Node.

Configuring email notification on the Active Server

Before you begin

- If anonymous users are allowed, a user name and password might not be required. Check with the Administrator of the email server for setup configuration.

About this task

If an automatic switchover occurs, the High Availability utility can send email messages to configured users at a defined interval.

The default email notification character set is US_ASCII. The following character sets are also supported:

- ISO-8859-1
- UTF-16BE
- UTF-8
- UTF-16LE
- UTF-16

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **High Availability**.
3. Expand **Configuration**.
4. Double-click **Notification**.
5. Select the **Email** check box.
6. Type the **SMTP Server** name.
7. Type the **Username**.
8. Type the **Password**.
9. Type the **From Address**.
10. Type the **To Address** or **Addresses**.
11. Click **OK** to save the data.

Variable definitions

Name	Description
Email	Enables or disables email notifications.
SMTP Server	The SMTP Server name, which is automatically verified when saving the data.
Username	Email User log on name.
Password	Email User log on password.
Charset	Email character set to use.
From Address	Email address to send notifications from.
To Address	Email address to send notifications to.

Backing up the database on the Active server

About this task

The Active server is configured for High Availability. Now the Standby server must be prepared for High Availability resiliency. Back up the Active server to create a snapshot of the database which is then restored to the Standby server. On the active Network Control Center server all databases must be backed-up.

Important:

Do not use a folder on the Active or Standby servers as the backup location.

Procedure

1. Log on to the Active server.
2. Click **Start** > **All Programs** > **Avaya** > **Database Maintenance**.
3. Click **Backup Locations**.
4. Click **Create**.
5. From the **Driver Letter** list, select the network drive on which you want to store the Network Control Center and ADMIN databases.
6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Backup Location. This location must be a shared folder with correct permissions.

   Important:

   Do not use the same backup folder for your NCC and any other ADMIN database in your contact center, as ADMIN databases stored in the same backup location overwrite each other.
7. In the **User Name** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the Windows password.
9. Click **OK**.
10. In the left pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. From the **Backup Location** list, select the network drive on which to store the backup.
13. Click **Backup**.

Restoring the database on the Standby server

Before you begin

- Know the location of the backup database.
- Stop shadowing if shadowing is running on the Standby server.
- Stop all Contact Center services using the SCMU utility, if services are running.
- Ensure the patch level on the Standby server is the same as the Active server.

Important:

You must restore all databases on an NCC server. Restoring only CCMS and not ADMIN can leave an inconsistent server and HA cannot shadow data correctly.

Important:

Restoring the ADMIN database can change configuration of Backup locations on the Standby server if the Active server and Standby server backup locations are different. Therefore, after you restore the ADMIN database, close and reopen the Database and Maintenance utility.

Important:

Run the Server Configuration utility after performing a database restore and check that the data is correct.

About this task

Restore the database from the Active server to the Standby server to ensure the databases are consistent.

Procedure

1. Log on to the Standby server.
2. Click **Start** > **All Programs** > **Avaya** > **Database Maintenance**.
3. In the **Database Maintenance** dialog box, in the left pane, click **Restore**.
4. In the right pane, under **Media Type**, select the media type on which the backup is restored.
5. If the backup file is on the network drive, in the **Backup Location** list, select the backup location.
6. Under **Application**, select **CCMS**, **ADMIN**, and **CCMA**.
7. Under **Restore contents**, select Data.
8. Click **Restore**.
9. Use the **Progress information** field to monitor the progress of the restoration.
10. When the restore completes, click **Exit** to close the Database Maintenance utility.

Configuring server details on the Standby server

Before you begin

- The Active server databases are restored on to the Standby server.

About this task

After you restore the Active server database on to the Standby server, the Standby server database contains the same agent and statistical data as the Active server. However the Standby server details are now also configured exactly the same as the Active server, therefore you must reconfigure the Standby server with its own server details.

Procedure

1. Log on to the Standby Server.
2. Click **Start** > **All Programs** > **Avaya** > **Server Configuration**.
3. In the **Server Configuration** dialog box, click the **Local Settings** tab.
4. Click **Apply All**.
5. In the **Server Configuration** dialog box, click the **Licensing** tab.
6. In the **License Server IP** box, update the license server IP address.

   Note:

   If you use Corporate licensing and License Manager is installed co-resident with your Network Control Center, in the **License Server IP** box type the physical IP address of your standby NCC server.

   If you use Nodal licensing and License Manager is installed on your Contact Center Manager Server (CCMS), in the **License Server IP** box type the physical IP address of your CCMS server.
7. Click **Apply All**.
8. Click **OK**.

Configuring High Availability on the Standby server

Before you begin

- The Active server databases are restored on to the Standby server.

About this task

Configure High Availability resiliency on the Standby server using the High Availability utility. The NCC Standby server shadows the Active server and takes over processing if the Active server fails.

Procedure

1. Log on to the Standby server.
2. Click **Start** > **All Programs** > **Avaya** > **High Availability**.
3. In the left pane of the **High Availability** dialog box, click **Server Mode**.
4. In the **Server Mode Configuration** section, select **Standby**.
5. Under **Server Mode Configuration**, in the text box, type the maximum length of time the network connectivity tests can continue to fail consecutively before corrective action is considered.

6. Under **Server Mode Configuration**, from the drop down list, select the unit of time for the network connectivity tests.
7. Under **IP Configuration**, type the **Active Server details CLAN** IP address. Leave the **ELAN** IP address box blank.
8. Under **IP Configuration**, type the **Standby Server details**, **CLAN** IP address. Leave the **ELAN** IP address box blank.
9. Under **IP Configuration**, in the **Address** box, type the IP address of the **Trusted IP** server.
10. Click **Save**.

    A system message box appears. You must stop the system before you save any information.
11. Click **Yes**.

Starting the Active server

About this task

Start the Active server using the High Availability utility.

Procedure

1. Log on to the Active server.
2. Click **Start** > **All Programs** > **Avaya** > **High Availability**.
3. Expand **Tasks**.
4. Double-click **CC Applications**.
5. In the first box under **CC Applications**, select the system.
6. Click **Start**.

   A delay occurs before services start.
7. Click **Yes**.
8. Verify that the Contact Center services are running using the SCMU, select **Avaya** > **System Control and Monitor Utility**.

Procedure job aid

After the system starts, check that the Managed IP (MIP) address is assigned to the network adapter of the Active Server by opening a command window and entering:

```
IPCONFIG /all
```

The IP and the MIP of the Active Server appears.

Starting shadowing on the Standby server

Before you begin

Important:

Enabling the shadowing functionality is available only on the system control dialog box of the High Availability utility on the Standby server.

Important:

On the Standby server, Avaya recommends not to stop and start shadowing but to use the pause and resume functionality.

About this task

Start shadowing on the Standby server using the High Availability utility. The Standby NCC server must be shadowing the Active NCC server for a switchover to occur if the Active Server fails. While the Standby server is shadowing the Active server, it maintains a near real-time local copy of the CCMS and Administration databases. Therefore, the Standby server is configured with the most recent data and it can take over from the Active server if necessary.

Important:

You must back up the Active server database, restore it onto the Standby server, and enable shadowing within 24 hours. If the difference in time between the Active and Standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the Active server database and restore it onto the Standby server before re-enabling shadowing. Ensure that the system clock time on the Active and Standby servers are synchronized.

Procedure

1. Log on to the Standby Server.
2. Click **Start** > **All Programs** > **Avaya** > **High Availability**.
3. Expand **Tasks**.
4. Double-click **System Control**.
5. In the **Control** box, select **Shadowing**.
6. Click **Start**.
7. Click **OK**.
8. To verify that services are stopped using the SCMU, select **Avaya** > **System Control and Monitor Utility**. Ensure services are stopped.

Verifying shadowing is running on the Active Server

About this task

Verify that the Standby NCC server is shadowing the Active server using the High Availability Utility. The System dialog box of the High Availability utility displays system information about the Active and the Standby servers.

The dialog box displays the followings information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information
- Remote server connection status
- Remote server port information
- License information
- Databases shadowed
- Time of last record shadowed
- Database namespaces
- Local and remote information on system status, switchover, shadowing and network.
- CC Application install information
- Database space and journaling information
- Database processes information

Procedure

1. Log on to the Active server.
2. Click **Start** > **All Programs** > **Avaya** > **High Availability**.
3. In the left pane, expand **Configuration**.
4. Select **System**.
5. Select **Get System Configuration**.

   The most recent system information appears.

Changing server details in Contact Center Manager Administration

About this task

In Contact Center Manager Administration, change the Network Control Center server details to use the High Availability Managed IP address and Managed name details.

The High Availability Managed IP address and Managed name details entered here must match those configured in Resolving the Managed name to the Managed IP Address on page 381.

Procedure

1. Log on to the Contact Center Manager Administration application with administrative privileges.
2. On the **Launchpad**, click **Configuration**.
3. From the list of servers in the system tree, right-click on the active NCC server, and select **Edit Properties**.
4. In the **Server Name** box, type the High Availability Managed name of the Network Control Center server.
5. In the **IP Address** box, type the High Availability Managed IP address of the Network Control Center server.
6. In the **Display Name** box, type the name of the Network Control Center server HA pair as you want it to appear in the system tree of Contact Center Manager Administration.
7. Click **Submit**.

Testing switchovers

Before you begin

Configure High Availability on the Active and Standby servers and ensure that the Standby server is shadowing.

About this task

Test the High Availability feature and infrastructure by making a manual switchover from the Active server to the Standby server.

Procedure

1. Log on to the current Standby Server.
2. Click **Start** > **All Programs** > **Avaya** > **High Availability**.
3. In the left pane of the **High Availability** window, expand **Tasks**.
4. Under **Tasks**, double-click **System Control**.
5. In the **Control** box, select **Switchover**.
6. Select the **System** tab.
7. Select **Switchover**.
8. Click **Start**.

To verify whether the switchover was successful, log on to CCMA configuration using the Managed name. Select the NCC server and verify that the configured sites appear in the Network Sites table.

Reinstating High Availability after a switchover

Before you begin

Ensure the active and standby NCC servers can communicate with each other and with the Trusted IP address.

About this task

If the Active server fails, the Standby server becomes active. The initially Active server is now stopped, and the High Availability - Enable switchover option is disabled. The Standby server becomes the Active server. The High Availability SMTP feature sends an email to the Contact Center Administrator informing them about the switchover. The Active server has no corresponding Standby server at this point, and the solution is no longer resilient.

When the root cause of the failure has been addressed the Contact Center Administrator can reinstate High Availability resiliency using the following procedure.

Procedure

1. Back up the current active Network Control Center server and Administration databases.
2. Restore these databases to the new standby server. Restore the Administration database last.

   Note:

   If shadowing is started on the standby server, it must be stopped before you can restore the databases.
3. On the new active server, click **Start** > **All Programs** > **Avaya** > **High Availability**.
4. Expand Configuration and click **Server Mode**. Ensure the **Switchover** check box is selected.
5. On the new standby server, configure a standby server using the High Availability utility.
6. On the standby server, click **Start** > **All Programs** > **Avaya** > **High Availability**.
7. Expand Configuration and click **Server Mode**.
8. Under **Server Mode Configuration**, select **Switchover**.
9. Under **Tasks**, click **System Control**.
10. Beside **Control**, select **Shadowing**.
11. Click **Start**.

    The standby server is now shadowing the active server and High Availability resiliency is restored.

Chapter 29: Contact Center Manager Server web service configuration

A series of SOAP-based open interfaces are provided to third-party software structures so you can enable communications for your applications based on the Service-Oriented Architecture (SOA) model. The Open Queue Open Interface provides existing OpenQ functions to third-party applications using a web service. In a controlled fashion, third-party applications can add and remove contacts of a specific type in Avaya Aura® Contact Center.

The Open Networking Open Interface enables a third-party application to transfer a call between nodes in a network. The third-party applications can reserve a Landing Pad on the target node to enable the call to be transferred with associated data attached. The web services also provide the option to cancel the reservation of a Landing Pad to free it for other calls transferred across the network.

The open interface applications are optional. For more details, see the SDK documentation.

High Availability considerations

Mission Critical High Availability campus solutions support CCMS web services.

Hot standby campus solutions do not preserve web service sessions during a switchover. You must program clients developed using the Open Queue or Open Networking web services to detect and respond to HA switchovers. For information about programming web services to handle HA switchovers, see the SDK documentation.

In all remote geographic solutions, clients developed using web services must be programmed to connect to the RGN IP address if the RGN is brought online when the campus site is unavailable.

Supported TLS versions

Contact Center defaults to using TLS 1.2 for secured services and connections. For backward compatibility, Contact Center supports changing the minimum TLS version that Contact Center can negotiate with other systems. This is to interoperate with legacy systems that do not support TLS 1.2.

When the Contact Center configuration is for a TLS version lower than 1.2, Contact Center still attempts to negotiate the highest (and most secure) version first, before stepping down to a lower (and less secure) version. Avaya recommends that you maintain the TLS version settings at the highest possible TLS version, and that you change these settings only when it is certain that parts of your overall contact center solution do not work with the higher TLS version.

Contact Center Manager Server Web service commissioning checklist

The following is a list of key configuration items required for Contact Center Manager Server Web service commissioning.

Item	Your value	Description
Ensure that Contact Center is licensed for Open Queue		Open Queue is a licensed feature that you must enable in Contact Center Manager Server-Server Configuration.
Ensure that Contact Center is licensed for Open Networking		Open Networking is a licensed feature that you must enable in Contact Center Manager Server-Server Configuration.
Certificate Authority (CA) details		The details of the Certificate Authority (CA) you are using.

Generating a Certificate Signing Request for a non-HA server

Before you begin

Use this procedure if your contact center does not use the High Availability feature.

About this task

Generate a Certificate Signing Request (CSR) for a non HA server, to configure certificates and enable the Web services over the Transport Layer Security.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Server Configuration**.
3. In the left pane of the Server Configuration console, click **WS Open Interfaces**.
4. Select the **SOA ENABLED** check box.
5. Select the **TLS Encryption** check box.
6. From the **TLS Level** drop-down list, select the minimum supported TLS level.
7. Ensure the **Host** box contains the host name of the server.
8. In the **Password** box, type a password that contains at least six characters.
9. Click **Apply All**.

The CSR appears in the CSR File box. Use the CSR file to apply to a Certificate Authority (CA) to buy a certificate and import the certificate to the service using the configuration application.

10. If CCMS displays the **Restart Required** dialog, click **Yes**.

Variable definitions

Name	Description
TLS (Transport Layer Security)	Protocol that allows secure communication between applications across a network.

Procedure job aid

Certificate Authorities (CA) include the following components:

- Verisign
- Thawte
- Create your own

Generating a Certificate Signing Request for a High Availability CCMS server pair

Before you begin

Use this procedure only if your contact center uses the High Availability feature.

About this task

Generate a Certificate Signing Request (CSR) to configure certificates and enable the Web services over the Transport Layer Security.

Procedure

1. Log on to the active Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Server Configuration**.
3. In the left pane of the Server Configuration console, click **WS Open Interfaces**.
4. Select the **SOA ENABLED** check box.
5. Select the **TLS Encryption** check box.
6. From the **TLS Level** drop-down list, select the minimum supported TLS level.
7. Ensure the **Host** box contains the managed name of the pair of campus servers.
8. In the **Password** box, type a password that contains at least six characters.

The Password on both the active and standby servers must be identical, including the case of letters.

9. Click **Apply All**.

   The CSR appears in the CSR File box. Use the CSR file to apply to a Certificate Authority (CA) to buy a certificate and import the certificate to the service using the configuration application.

10. Click **Exit**.
11. Repeat steps 1 to 9 on the standby Contact Center server.

Importing the CSR-Related Certificates

Before you begin

- Ensure you generate a CSR certificate. For more information, see Generating a Certificate Signing Request on page 395.
- Ensure you apply to a Certificate Authority (CA) for a certificate.

About this task

Import the CSR-Related Certificates to the SOA configuration after you receive the certificates to enable services over the Transport Layer Security.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Server Configuration**.
3. In the left pane of the Server Configuration console, click **WS Open Interfaces**.
4. In the **Generate Certificate Signing Request Password** box, type a password.
5. In the **Alias** box, type an alias to identify the CA certificate, for example SomeCAPublicCert1.
6. In the **Trusted Certificate Authority CA Cert** box, click **Browse**, and then select the CA public certificate.
7. In the **CSR Response Certificate CSR Cert** box, click **Browse**, and then select the certificate.
8. Click **Apply All**.
9. Click **Exit**.

Configuring SOA OpenQueue and OpenNetworking Web Services

Before you begin

- You must restart the server to complete this procedure.
- Install and commission Contact Center Manager Server.
- Ensure that Contact Center License Manager is licensed to provide SOA OpenQueue and OpenNetworking Web Services.
- Ensure OpenQ and OpenNetworking Web Services and the CCT Web Services do not use the same port on the server. Change the OpenQ and OpenNetworking services port value from 9080 to 9070 in the Web services section of server configuration.

About this task

Configure and enable the SOA OpenQueue and OpenNetworking Web Services to configure other applications that can add contacts to the open queue for routing, remove contacts from the open queue, and move contacts between nodes in a network.

This procedure enables the Web services without Transport Layer Security (TLS). If you want to enable TLS, when you finish this procedure complete the procedures in this chapter to generate and import security certificates.

Procedure

1. Log on to the Contact Center Manager Server.
2. From the **Start** menu, in the Avaya area, click **Server Configuration**.
3. In the left pane of the Server Configuration console, click **WS Open Interfaces**.
4. Select the **SOA ENABLED** check box.
5. Ensure the **Host** box contains the host name of the server.
6. In the **Ports** box, type an available port number for which the services are available for access.
7. In the **User Password** box, type the new password for the OpenWsUser account.
8. In the **Session Timeout** box, select the value of the timeout duration in minutes.
9. Clear the **TLS Encryption** check box.
10. Click **Apply All**.
11. If CCMS displays the **Restart Required** dialog, click **Yes**.

Variable definitions

Name	Description
Host	The host name of the server, not the IP address.

Table continues…

Name	Description
Ports	The port number on which the OpenQueue and OpenNetwork Interfaces are published. This port and the following three consecutive port numbers are used to access the Web services from the external applications. All four port numbers must be available.
Session Timeout	The time in minutes that a session is valid after a user logs on. The session times out if it is inactive for the specified duration. The default is 120 minutes.
TLS Encryption	To publish services under TLS (HTTPS), select the TLS Encryption check box. To publish services under HTTP, clear the TLS Encryption check box.

Removing Certificate Configuration

Before you begin

- Clear the TLS Security check box.
- Ensure the certificates are configured. For more information, see Generating a Certificate Signing Request on page 395.

About this task

Remove certificate configuration to delete all imported certificates and any outstanding CSR files.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Server Configuration**.
3. In the left pane of the Server Configuration console, click **WS Open Interfaces**.
4. Select the **SOA Enabled** check box.
5. Select the **Remove Certificates** check box.
6. Click **Apply All**.
7. In the **Restart Required** dialog, click **Yes**.
8. Click **Exit**.

Chapter 30: Communication Control Toolkit web service configuration

A series of SOAP-based open interfaces are provided to third-party software structures so you can enable communications for your applications based on the SOA model. The CCT open interface environment offers functionality similar to the CCT SDK but with the flexibility to choose your own development environment.

You can use these CCT services to recreate Agent tools in your own applications or to access call control functionality for Avaya Aura® Contact Center from any business process. The open interface applications are optional. For more details, see the SDK documentation.

High Availability considerations

Mission Critical High Availability campus solutions support CCT web services.

Hot standby campus solutions do not preserve web service sessions during a switchover. You must program clients developed using the Open Queue or Open Networking web services to detect and respond to HA switchovers. For information about programming web services to handle HA switchovers, see the SDK documentation.

In remote geographic solutions, clients developed using web services must be programmed to connect to the RGN IP address if the RGN is brought online when the campus site is unavailable.

Important:

In a High Availability solution, CCT web services configuration information does not replicate to standby or remote geographic servers. Configure web services identically for the active CCT, standby CCT, and RGN CCT servers.

Supported TLS versions

Contact Center defaults to using TLS 1.2 for secured services and connections. For backward compatibility, an administrator can change the TLS version that Contact Center can negotiate with other systems. This is to interoperate with legacy systems that do not support TLS 1.2.

In CCT, TLS works as follows:

- If you select TLS 1.0 in CCT web services, it accepts connections from other applications with TLS 1.0 only.
- If you select TLS 1.1 in CCT web services, it accepts connections from other applications with TLS 1.1 only.
- If you select TLS 1.2 in CCT web services, it accepts connections from other applications with TLS 1.2 only.

Communication Control Toolkit Web service commissioning checklist

The following is a list of key configuration items required for Communication Control Toolkit Web service commissioning.

Item	Your value	Description
Ensure that Contact Center is licensed for Open Queue		Open Queue is a licensed feature that you must enable in Contact Center Manager Server-Server Configuration.
Ensure that Contact Center is licensed for Open Networking		Open Networking is a licensed feature that you must enable in Contact Center Manager Server-Server Configuration.
Certificate Authority (CA) details		The details of the Certificate Authority (CA) you are using.

Configuring SIP Call Recording

Before you begin

Configure SOA CCT Web services. For more information, see Configuring SOA CCT Web services on page 406.

About this task

Configure the SIP Call Recording user account. This SIP Call Recording user account is a special user that is used only by the Call Recording server to connect to Communication Control Toolkit, and only using the OI interface.

Avaya recommends that the SIP Call Recording user account is a Windows domain user account, although no restriction is in place to prevent the selection of a local Windows Security Account Manager (SAM) account.

Important:

You must not map a Contact Center agent to the SIP Call Recording user account.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **CCT Console**.
3. In the left pane of the CCT console, expand **Communication Control Toolkit**.
4. Expand **Server Configuration**.
5. Select **CCT Web Services**.
6. Under **SOA Configuration**, select the **Enable SIP Call Recording** check box.

7. Click **Browse Users**.
8. On the **Browse Users** dialog, in the **Location** list, select the location of the Windows account you plan to use as the SIP Call Recording user account.
9. In the **Search Type** list, select **All Users**.
10. Click **Search**.
11. From the list of users, select the user that you plan to use as the SIP Call Recording user account.
12. In the **Actions** pane, click **Apply changes**, and then click **OK**.
13. If your contact center uses the High Availability feature, repeat steps 1 to 12 on the standby server.
14. If your contact center uses the Geographic High Availability feature, repeat steps 1 to 12 on the RGN server.

Generating a Certificate Signing Request

Before you begin

- Use this procedure if you want to enable TLS for your CCT Web services, and only if your contact center does not use the High Availability feature.
- Configure SOA CCT Web services. For more information, see Configuring SOA CCT Web services on page 406.

About this task

Generate a Certificate Signing Request (CSR) to configure certificates and enable services over Transport Security Layer (TLS).

An application can use a CSR to apply to a Certificate Authority (CA) for a certificate. The host name and password is used to generate the CSR. The password is saved in an encrypted format.

After you generate the CSR file, present it to your CA to obtain a corresponding certificate.

When you have received the certificate from the CA, import it to complete the TLS configuration. For more information on importing the certificate, see Importing CSR-related Certificates on page 405.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **CCT Console**.
3. In the left pane of the CCT console, expand **Communication Control Toolkit**.
4. Expand **Server Configuration**.
5. Select **CCT Web Services**.

6. Select the **TLS Security** check box.
7. From the **Min TLS Level** drop-down list, select the minimum supported TLS level.
8. Ensure the **Host Name** box contains the host name of the server.
9. Click **Generate CSR**.
10. In the **Location** box, type the location of the company.
11. In the **Company Name** box, type the name of your company.
12. In the **Password** box, type a password that contains at least six characters.
13. If required, change the encryption settings.

    The default encryption setting is SHA256 with a key size of 2048. For backward compatibility, you can choose SHA1 or a key size 1024. However, neither SHA1 nor 1024 provide the industry-recommended level of encryption.
14. Click **Generate**.

    The CSR file path and name appear in the CSR box. Use the CSR file to apply to a Certificate Authority (CA) to buy a certificate and import the certificate to the service using the configuration application.
15. Click **Apply Changes**, and then click **OK**.

Variable definitions

Name	Description
TLS (Transport Layer Security)	Protocol for secure communication between applications across a network.

Generating a Certificate Signing Request for a High Availability CCT server pair

Before you begin

- Use this procedure if you want to enable TLS for your CCT Web services, and only if your contact center uses the High Availability feature.
- Configure SOA CCT Web services. For more information, see Configuring SOA CCT Web services on page 406.
- Ensure that the **WS Open Interfaces** section of CCMS **Server Configuration** contains the managed name of the campus pair.

About this task

Generate a Certificate Signing Request (CSR) to configure certificates and enable the Web services over Transport Layer Security.

An application can use a CSR to apply to a Certificate Authority (CA) for a certificate. The host name and password is used to generate the CSR. The password is saved in an encrypted format.

After you generate the CSR file, present it to your CA to obtain a corresponding certificate.

When you have received the certificate from the CA, import it to complete the TLS configuration. For more information on importing the certificate, see Importing CSR-related Certificates on page 405.

Procedure

1. Log on to the active Contact Center server.
2. From the **Start** menu, in the Avaya area, click **CCT Console**.
3. In the left pane of the CCT console, expand **Communication Control Toolkit**.
4. Expand **Server Configuration**.
5. Select **CCT Web Services**.
6. If Contact Center displays the **Host Name Mismatch** dialog, click **No**.
7. Select the **TLS Security** check box.
8. From the **Min TLS Level** drop-down list, select the minimum supported TLS level.
9. Ensure the **Host Name** box contains the managed name of the pair of campus servers.
10. Click **Generate CSR**.
11. In the **Location** box, type the location of the company.

    The location on both the active and standby servers must be identical. It is case-sensitive.
12. In the **Company Name** box, type the name of your company.

    The company name on both the active and standby servers must be identical. It is case-sensitive.
13. In the **Password** box, type a password that contains at least six characters.

    The password on both the active and standby servers must be identical. It is case-sensitive.
14. If required, change the encryption settings.

    The default encryption setting is SHA256 with a key size of 2048. For backward compatibility, you can choose SHA1 or a key size 1024. However, neither SHA1 nor 1024 provide the industry-recommended level of encryption.
15. Click **Generate**.

    The CSR file path and name appear in the CSR box. Use the CSR file to apply to a Certificate Authority (CA) to buy a certificate and import the certificate to the service using the configuration application.
16. Click **Apply Changes**, and then click **OK**.

Importing CSR-related Certificates

Before you begin

- Complete this procedure only if you want to enable TLS for your CCT Web services.
- Ensure you generate a CSR certificate. For more information, see Generating a Certificate Signing Request on page 402 or Generating a Certificate Signing Request for a HA CCT server pair on page 403.
- Ensure you apply to a Certificate Authority (CA) for a certificate.

About this task

After you receive the certificate, import the CSR-related certificates to the SOA configuration to enable services over TLS.

Procedure

1. Log on to the Communication Control Toolkit server.
2. From the **Start** menu, in the Avaya area, click **CCT Console**.
3. In the left pane of the CCT console, expand **Communication Control Toolkit**.
4. Expand **Server Configuration**.
5. Select **CCT Web Services.**
6. In the **CA Alias** box, type an alias to identify the CA certificate, such as SomeCAPublicCert1.
7. Click **Import Trusted CA Certificate** to select the CA public certificate.
8. Click **Import Certificate** to select the certificate.
9. Click **Apply Changes**, and then click **OK**.

Next steps

If your contact center uses the High Availability feature, complete the steps in Importing CSR-related Certificates on Standby and RGN servers on page 405

Importing CSR-related Certificates on Standby and RGN servers

Before you begin

- Complete this procedure only if you enabled TLS for your CCT Web services on the High Availability Active server.
- Generate and import a certificate on the Active server.

About this task

Complete this procedure to import the CSR-related certificate to the Standby server and, optionally, to the RGN server.

Procedure

1. Log on to the active Contact Center server.
2. Copy all the files from the directory `D:\Avaya\Contact Center\Common Components\CMF\security`.
3. Log on to the standby Contact Center server.
4. Paste the files that you copied from the Active server into the directory `D:\Avaya\Contact Center\Common Components\CMF\security`, but do not overwrite the existing `SecureServer.cxf` or `gs-directory.fsm` files.
5. From the **Start** menu, in the Avaya area, click **CCT Console**.
6. In the left pane of the CCT console, expand **Communication Control Toolkit**.
7. Expand **Server Configuration**.
8. Select **CCT Web Services.**
9. In the **CA Alias** box, type an alias to identify the CA certificate, such as SomeCAPublicCert1.
10. Click **Import Trusted CA Certificate** to select the CA public certificate.
11. Click **Import Certificate** to select the certificate.
12. Click **Apply Changes**, and then click **OK**.
13. If your contact center uses the Geographic High Availability feature, repeat steps 3 to 12 on the RGN server.

Configuring SOA CCT Web services

Before you begin

- Understand the network requirements for your installation of Communication Control Toolkit.
- Know how to stop and restart the core Communication Control Toolkit services.
- Install and commission Contact Center Manager Server.
- Ensure that a valid SOA Web Services (Open Queue and Open Networking) license is available.
- Applications connected to the CCT SOA interface consume the same per seat licenses as agents using Agent Desktop. Ensure you have sufficient additional Maximum Contact Center devices (license identifier of VALUE_CCTR_CTIDT_CC or LM_VOD, depending on your license file type) for the clients that connect to the CCT SOA interface.

About this task

Configure and enable the SOA CCT Web Services without Transport Layer Security (TLS). If you want to enable TLS, when you finish this procedure, complete the procedures in this chapter to generate and import security certificates.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **CCT Console**.
3. In the left pane of the CCT console, expand **Communication Control Toolkit**.
4. Expand **Server Configuration**.
5. Select **CCT Web Services**.
6. Select the **Enable CCT Web Services** check box.
7. Ensure the **Host Name** box contains the host name of the server.
8. In the **Ports** box, type an available port number where the services are available for access.
9. In the **Session Timeout** box, select the value of the timeout duration in minutes.
10. Clear the **TLS Security** check box.
11. In the **Actions** pane, click **Apply changes**, and then click **OK**.
12. Stop and restart the core Communication Control Toolkit services.
13. Verify that the services are available by viewing the following on the host: http://localhost:9090.
14. If your contact center uses the High Availability feature, repeat steps 1 to 14 on the standby server.
15. If your contact center uses the Geographic High Availability feature, repeat steps 1 to 14 on the RGN server.

Variable definitions

Name	Description
Host Name	The host name of the server; do not enter the IP address.
Ports	The port number on which the SOA CCT Interfaces are published. External applications use this port, along with the following three consecutive port numbers, to access the Web services. All four port numbers must be available.
Session Timeout	The amount of time in minutes that a session is valid after a user logs on. The session times out if it is inactive for the specified duration. The default is 120 minutes.

Table continues…

Name	Description
TLS Security	Clear the TLS Security check box. If you want to publish services under TLS (HTTPS), you must create and import security certificates: follow the procedures in this chapter relating to certificate creation and import.

Removing Certificate Configuration

Before you begin

- Clear the TLS Security check box.
- Ensure you generated a CSR certificate. For more information, see Generating a Certificate Signing Request on page 402 or Generating a Certificate Signing Request for a HA CCT server pair on page 403.

About this task

Remove certificate configuration to delete all imported certificates and any outstanding CSR files.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **CCT Console**.
3. In the left pane of the CCT console, expand **Communication Control Toolkit**.
4. Expand **Server Configuration**.
5. Select **CCT Web Services**.
6. Click **Reset TLS Encryption Configuration**.
7. In the confirmation dialog box, click **Yes**, and then click **Confirm**.
8. In the **Actions** pane, click **Apply changes**, and then click **OK**.
9. If your contact center uses the High Availability feature, repeat steps 1 to 8 on the standby server.
10. If your contact center uses the Geographic High Availability feature, repeat steps 1 to 8 on the RGN server.

Index

A

about mission critical high availability 251
accessing CCMA
    Edge in IE mode 115
active server 369
Active Server 357
active server campus high availability 259, 308
active server database backups 262, 285, 312, 335
active server database CCMM 359
active server email 261, 311
active server high availability 283, 333
active server start 270, 294, 320, 343, 362, 375
active server verifying high availability 271, 297, 321, 346
active server verifying shadowing 363, 376
Active X controls 182
ActiveX controls 181
add administrator email address
    CCMM Dashboard 208
adding CCT to CCMA 184
adding multimedia servers to CCMA 194
administration for CCMM 257, 307, 355
agent adding 185
agent desktop display parameters 110
Agent Desktop voice contacts LDAP 198
Agent Greeting
    checklist 221
    configuring for SSO 166
apply
    license file 51
applying ActiveX controls 182
assigning certificates 157
attachment file locations 202
availability of servers critical 251
Avaya Aura MS
    root certificate 44, 147
Avaya Aura MS High Availability configuration and status
    reviewing 79
Avaya Aura MS security
    configuration 151
Avaya support website 18
Avaya WebLM 52

B

backing up CCMM active server database 359, 370
backup System Manager communication 165

C

call recording for SIP 401
campus high availability on active server 259, 308
CCMA adding CCT server 184
CCMA adding multimedia servers 194
CCMA Administration shared folder 109
CCMA Administration user password 112
CCMA agent desktop display parameters 110
CCMA and System Manager communication 162
CCMA client ActiveX controls 181
CCMA client display settings 178
CCMA client internet options configuration 179
CCMA client shared folders 107
CCMA commissioning 100
CCMA historical reporting 106
CCMA historical reporting folders 106
CCMA logging in 127
CCMA managed name 275, 325
CCMA real-time reporting 104
CCMA starting client 164
CCMA user permissions folders 108
CCMA users mapping System Manager users 163
CCMA web service verification 113
CCMM active server database backup 359, 370
CCMM administration 257, 307, 355
CCMM Dashboard
    add administrator email address 208
CCMM general administration 285, 371
CCMM server database restore 374
CCMS changing server details 274, 324
CCMS commissioning tasks 49
CCMS configuring multiple sites 57
CCMS disk defragmentation 53
CCMS global settings 129
CCMS multicast for statistics 54
CCMS multiplicity 52
CCMS successful installation verification 51
CCMS Web service
    checklist 395
CCMS web services 394
CCT adding to CCMA 184
CCT certification removal 408
CCT confirming services 183
CCT CSR certificates 405
CCT SOA Web services 406
CCT Web service
    checklist 401
CCT web services 400
certificate removal 399
certificate signing request 402
certificate signing requests 395
certificates for CCT CSR 405
certificates importing 397
changes in this release 19
changing server details in CCMA
    NCC HA 391
changing server details in CCMS 274, 324

checklist
Agent Greeting ... 221
CCMS Web service ... 395
CCT Web service ... 401
HA ... 255, 281, 304, 331, 352, 366
Microsoft instant messaging server ... 234
client commissioning
CCMA ... 178
client installation Orchestration Designer ... 134
client starting CCMA ... 164
clients shared folder ... 107
commissioning
single sign-on ... 160
commissioning CCMA ... 100
commissioning CCMS ... 49
commissioning SIP-enabled Contact Center server ... 24
common commissioning checklist
Media Server ... 92
Communication Control Toolkit ... 400
compatibility list view ... 125
compatibility view configuration ... 119
completing
HA pair configuration ... 76
configuration
Avaya Aura MS security ... 151
configure RGN ... 285, 371
configuring active server ... 369
configuring Active Server ... 357
configuring campus high availability on active server 259, 308
configuring CCMA and System Manager communication . 162
configuring CCMM general administration ... 257, 307, 355
configuring certificate signing request ... 395
configuring communication between CCMA and System Manager
geographic server ... 174
primary server ... 171
standby server ... 172
configuring communication to backup System Manager ... 165
configuring database backups on active server .262, 312, 335
NCC HA ... 385
configuring desktop display parameters ... 110
configuring display settings ... 178
configuring email notification
NCC HA ... 384
configuring email on active server ... 261, 311
configuring email recipient addresses ... 200
configuring High Availability
Network Control Center ... 382
configuring high availability on active server ... 283, 333
configuring high availability on remote geographic server ... 288, 337
configuring high availability on standby server ... 265, 315
NCC HA ... 388
configuring internet options ... 179
single sign-on HA ... 176
configuring internet options on the CCMA server ... 113
configuring LDAP for voice contacts ... 198
configuring MIME types ... 206
configuring multimedia server settings ... 196
configuring multimedia users ... 192
configuring real-time reporting ... 104
configuring shared folders for client ... 107
configuring shared folders to export historical reports ... 106
configuring shared folders to read from users ... 108
configuring SIP call recording ... 401
configuring sites ... 57
configuring skillsets ... 203
configuring SOA CCT Web services ... 406
configuring SOA Web service ... 398
configuring SRTP
Media Server ... 158
confirming services ... 183
Contact Center commissioning ... 24
Contact Center Manager Server
web service ... 394
Creating a configuration file for Internet Explorer mode ... 121
critical high availability ... 251
CSR certificates ... 397
customizing
master script flow ... 214
Media_Server_Selection ... 215

D

database backups on active server ... 262, 285, 312, 335
database restore ... 374
database restore on standby server ... 263, 313, 360
deleting CCT certificates ... 408
deleting certificate ... 399
desktop display parameter configuration ... 110
disabling
IE mode ... 127
disk defragmentation ... 53
display settings in CCMA client ... 178
domain server ... 119

E

Edge integration with Internet Explorer ... 116
Element Manager ... 60, 71, 93
email on active server ... 261, 311
email recipient addresses ... 200
enabling
Media Server zoning ... 212
enabling multiplicity ... 52
Enterprise Mode Site List ... 117
exceptions list for internet firewall ... 181
exporting ... 43, 145

F

fax mailbox
add ... 208

firewall exceptions 181

G

generating certificate signing request 402
generating CSR with multiple SANs 155
geographic remote server shadowing 296, 345
geographic server
configuring communication between CCMA and System Manager 174
global settings
Contact Center Manager Server 129

H

HA
checklist 255, 281, 304, 331, 352, 366
HA checklist
Media Server 69
HA pair configuration
completing 76
HA prerequisites
Avaya Aura Media Server 67
High Availability
installing third-party utility 381
mapping System Manager users to CCMA users 175
Network Control Center 377
single sign-on 168
High Availability CCMM 357
High Availability Network Control Center commissioning
prerequisites 379
high availability on active server 283, 333
high availability on standby server 265, 315
High Availability RGN CCMM 373
high availability switchover testing 276, 326
high availability third-party support 355, 368
high availability verification 283, 333
high availability verification on active server 271, 321
high availability verifying services 258, 308
historical reporting shared folder 106
HTTP proxy 95

I

IE mode 115
configure compatibility list view 125
configure on local computer 125
disable 127
domain server 119
enabling on domain server 123
installing administrative templates 120
IE Mode 116
importing 156
importing CCT CSR certificates 405
importing CSR certificates 397
installation CCMS verification 51
installing Orchestration Designer client 134
installing third-party utilities for HA 355, 368
instant messaging TCP port 240
integration with IE 116
Internet Explorer integration 116
Internet Explorer mode 115
domain server 119
internet options on CCMA client 179
IP addresses managed for high availability
..... 256, 282, 306, 332

L

LDAP server for Agent Desktop voice contacts 198
license file
apply 51
licensing administration
apply license file 51
remote Avaya WebLM 52
list builder
using 218
local multimedia users permissions 192
logging in to CCMA 127
logging in to CCMA securely 177
logging on privileges for multimedia 192
low volume of announcement
adjusting 97

M

managed IP addresses 256, 282, 306, 332, 354, 367
managed name for CCMA 275, 325
management adding agent 185
mapping System Manager users to CCMA 163
mapping System Manager users to CCMA users
High Availability 175
master script flow
zoning 214
Media Server
common commissioning checklist 92
configuring SRTP 158
HA checklist 69
list builder 218
non-HA checklist 60
verifying TLS 158
verifying TLS configuration 159
zoning 209
Media Server zoning
enabling 212
Media Server Zoning
commissioning procedures 210
Media_Server_Selection
customizing 215
Microsoft Edge 115, 116
Microsoft Edge administrative templates 116
Microsoft instant messaging server
checklist 234

Microsoft Lync Server 233
mission critical high availability
voice contact server 301
mission critical high availability about 251
multicast controller 54
multimedia email recipient addresses 200
multimedia LDAP server 198
multimedia MIME types 206
multimedia server settings 196
multimedia servers to CCMA adding 194
multimedia services start 193
multimedia skillsets 203
multimedia users configuring 192
multiplicity enabling 52

N

name managed for high availability 256, 282, 306, 332
NCC HA
changing server details in CCMA 391
configuring database backups on active server 385
configuring email notification 384
configuring high availability on standby server 388
reinstating High Availability 393
restoring the database on the Standby server 386
starting active server 389
starting shadowing on standby server 390
testing switchovers 392
verifying shadowing on active server 391
network 56
network addressing for statistics 54
Network Control Center
configuring High Availability 382
High Availability 377
Network Control Center HA
resolving the managed name to the managed IP address 381
networking configuring sites 57
non-HA checklist
Media Server 60

O

open interfaces 400
open networking
call transfer 394
open networking SOA Web service 398
OpenQ 394
optimizing performance 53
Orchestration Designer installation 134

P

prerequisites
High Availability Network Control Center commissioning 379
primary server
configuring communication between CCMA and System Manager 171

R

read permissions for clients in shared folder configuration 107
real-time data multicast 54
real-time reporting 104
recipient addresses 200
reinstating High Availability
NCC HA 393
related documentation 13
remote Avaya WebLM 52
remote geographic node server details 292, 341
remote geographic server database restore 290, 339
remote geographic server high availability 288, 337
remote geographic server shadowing 296, 345, 375
removing CCT certificate configuration 408
removing certificate 399
reporting historical shared folder configuration 106
reporting real-time data configuration 104
requests for signing certificates 395
resolving managed names 256, 282, 306, 332, 354, 367
resolving the managed name to the managed IP address
Network Control Center HA 381
restarting instant messaging 241
restoring database 374
restoring database on remote geographic server 290, 339
restoring database on standby server 313, 360
restoring the database on the Standby server
NCC HA 386
reviewing
Avaya Aura MS High Availability configuration and status 79
RGN settings 296, 345
root certificate 43, 145
Avaya Aura MS 44, 147

S

scheduled task 47, 48, 149, 150
scheduling disk defragmentation 53
scheduling historical reports 106
security certificates commissioning 29
security store
subject alternative name 38, 140
server details in CCMA 274, 324
server details on remote geographic node server 292, 341
server details on standby server 267, 317
server settings for multimedia 196
servers critical availability 251
services availability for high availability 258, 308
services for multimedia 193
services starting in CCT 183
shadowing on remote geographic server 296, 345
shadowing on standby server 270, 295, 320, 344, 362

shadowing verification on active server 363
shared folders for clients to read 107
shared folders for historical reporting 106
shared folders for user permissions 108
signing request 402
single sign-on
commissioning 160
High Availability 168
single sign-on HA
internet options 176
SIP adding agents 185
SIP call recording 401
SIP Contact Center server commissioning 24
site configuration 57
skillsets 203
SMGR 155
SMTP server 46, 148
SOA 394, 400
SOA CCT Web services 406
SOAP interfaces 394, 400
standby server
configuring communication between CCMA and System Manager 172
standby server database restore 263, 313, 360
standby server high availability 265, 315
standby server server details 267, 317
standby server shadowing 270, 295, 320, 344, 362
starting active server 270, 294, 320, 343, 362, 375
NCC HA 389
starting CCMA client 164
starting shadowing on remote geographic node server 296, 345, 375
starting shadowing on standby server 270, 295, 320, 344, 362
NCC HA 390
static route 238
subject alternative name
security store 38, 140
support 18
switchover testing 276, 326
System Manager and CCMA communication 162
System Manager mapping to CCMA users 163

T

testing switchovers 276, 326
NCC HA 392
third call appearance button 55
third line appearance 55
third-party support for high availability 355, 368
third-party utility
High Availability 381
TLS version 42, 144
trusted application 235, 236
Trusted Application Pool 234
turning off web services security 35

U

updating CCMA Administration password 112
updating the master script 212
user mapping from System Manager to CCMA 163
user permissions shared folder 108
user permissions shared folder configuration 108
using CCMA managed name 275, 325

V

verifying CCMS installation 51
verifying high availability 283, 333
verifying high availability on active server ..271, 297, 321, 346
verifying multimedia services 193
verifying services for HA 258, 308
verifying shadowing on active server 363, 376
NCC HA 391
verifying TLS
Media Server 158
verifying TLS configuration
Media Server 159
verifying web services in CCMA 113
videos 17

W

Web browser ActiveX controls 181
web service configuration
CCT 400
Communication Control Toolkit 400
Contact Center Manager Server 394
Web service SOA Open Networking 398
web services security turning off 35