Deploying Avaya Aura® Conferencing

Release 7.2
Issue 1
August 2013

© 2013 Avaya Inc.

All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked 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 its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

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

Avaya grants you a license within the scope of the license types described below, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

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

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

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

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

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

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and

software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

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

Contents

Chapter 1: An Introduction to Avaya Aura® Conferencing 17
- About this document 17
- Related resources 17
  - Documentation 17
  - Training 18
  - Avaya Mentor videos 18
- Support 18
- Audience 19
- How to use this document 20
  - Preparing your data using the Avaya Aura® Conferencing 7.2 Intelligent Workbook 20
- Solution requirements 21
- License key 22
- Administrative user roles and preconfigured accounts 23
- Supported Web browsers 24
- Supported hardware 25

Chapter 2: Deployment options 27
- Deployment layouts 27
- Performance specifications 29
  - Servers 30
  - Deployment layouts and DMZ 32
  - Coresident deployment without the DMZ access and the Audio/Video in Collaboration Agent feature 33
  - Coresident deployment with the DMZ access and the Audio/Video in Collaboration Agent feature 34
  - Standalone simplex and standalone with redundancy deployment layouts 37
  - Media cascading 41
  - Flash Media Gateway 42
- Server components 43
- Co-resident with redundancy layout 51
  - System requirements for a co-resident with redundancy layout 52
- Co-resident with redundancy with DMZ layout 53
  - System requirements for a co-resident with redundancy with DMZ layout 54
- Co-resident simplex layout 55
  - System requirements for a co-resident simplex layout 56
- Co-resident simplex with DMZ layout 56
  - System requirements for a co-resident simplex with DMZ layout 57
- Standalone with redundancy layout 58
  - System requirements for a standalone with redundancy layout 60
- Standalone simplex layout 60
  - System requirements for a standalone simplex layout 61
- Enterprise DMZ deployment 62
- Event conferencing 64

Chapter 3: Network planning and design considerations 67
- Network considerations 67
- Conference usage patterns 67

Communities of interest ... 67
Avaya Media Server usage ... 68
QoS ... 68
Bandwidth capacity ... 69
Event conferencing considerations ... 70
Network impact on audio ... 71
Audio delays without media cascading ... 72
Audio delays with media cascading ... 73
Network impact on video ... 74
Service level agreements for audio queues ... 75
Virtual Private Network location and bandwidth management ... 76
Conference dial out ... 76
Adhoc conferences ... 76
Network location information ... 77
Voice activity detection and silence suppression ... 77
Cascading Avaya Media Server capacity ... 77
Blocking due to cascading bandwidth capacity ... 78
DTMF signaling by H.323 devices with Communication Manager ... 78
Direct media with Communication Manager ... 78
Robustness and reliability ... 78
Application server redundancy ... 79
Avaya Media Server redundancy ... 80
Web server redundancy ... 81
Avaya Media Server deployment for bandwidth optimization ... 82
Estimating WAN bandwidth usage ... 83
Hosting locations without media cascading ... 86
Locations without Avaya Media Server ... 87
Estimating bandwidth reductions due to media cascading ... 87
Conference size and media stream bandwidth ... 88
Non-hosting locations with media cascading ... 92
Hosting locations with media cascading ... 92
Multiple hosting locations with media cascading ... 93
Delay engineering guidelines ... 93
Minimizing overall delays with packet time selection ... 96
Shared bandwidth management ... 96
Monitoring bandwidth usage ... 96
Chapter 4: Before you begin ... 99
Before you begin checklist ... 99
Chapter 5: Installing hardware ... 105
Downloading HP documentation ... 105
HP DL360 document set ... 105
Front view of HP DL360 G7 Server ... 106
Back view of HP DL360 G7 Server ... 106
HP DL360 G7 Server environmental specifications ... 107
HP DL360 G7 Server physical specifications ... 108
Installing the server in the rack ... 108
Updating the HP DL360 G7 server power management settings ... 110

Chapter 6: Installing software 113
Introduction to software installation 113
Software installation procedure 113
Prerequisites for software installation 115
Installing the AAC Platform 116
Modifying the BIOS clock 119
Classifying the hardware environment 120
Configuring the system 121
Configuring the NTP clock 123
Configuring the Syslog Server 125
Viewing the user accounts and passwords 126
Creating the initial logon password 126
Applying server platform patches 127
Verifying the AAC Platform installation 129
Introduction to the Avaya Media Server (MS) 130
Reconfiguring the RAID 1 arrays using the HP SmartStart CD 131
Formatting and mounting the second RAID 132
Installing Avaya Media Server 134
Installing the components for Avaya Aura® Conferencing 135
IP address table for Avaya Aura® Conferencing deployment types 138
Populating tags 139
Checklist for verifying software versions 145
Accessing Element Manager Console using local login 147
Chapter 7: Installing the Avaya Aura® Conferencing license key 151
Installing the Avaya Aura® Conferencing license key on Avaya Aura® System Manager 151
Chapter 8: Configuring Transport Layer Security 153
Checklist for configuring Transport Layer Security 153
Introduction to Transport Layer Security 156
Guidelines for certificate configuration 156
Adding the System Manager CA certificate to the Administrator Internet Explorer browser 158
Adding the System Manager CA certificate to the administrator Firefox browser 159
Creating an administrator End Entity for identity certificates from System Manager 160
Installing an administrator identity certificate on the administrator Internet Explorer Web browser 161
Installing an administrator identity certificate on the administrator Firefox Web browser 162
Installing an administrator identity certificate on the Element Manager Console 163
Obtaining enrollment password from System Manager 165
Creating Network Element certificates signed by System Manager 165
Importing certificates from a third party CA 167
Importing CA certificates from a third party CA 168
Assigning a certificate to the Element Manager 169
Assigning a certificate to the Provisioning Manager 171
Assigning a certificate to the Personal Agent Manager 172
Assigning a certificate to the Application Server 173
Assigning certificates to the Avaya Media Servers 174
Assigning a certificate to the Web Conferencing Server 175
Assigning a certificate to the Web Conferencing Management Server 176
Chapter 9: Configuring Avaya Media Servers and clusters 177

Adding additional Avaya Media Server hosts ... 177
Adding an Avaya Media Server network element ... 178
Adding an additional Avaya Media Server to an existing media server cluster ... 179
Creating a new Media Server cluster ... 180
Chapter 10: Configuring Web Conferencing components ... 181
Configuration procedure for the Web conferencing server components ... 181
Configuring the meeting event processor for the Web conferencing management server ... 182
Configuring the default Web Conferencing Server group ... 182
Configuring Web Conferencing Management Server Rsync ... 183
Adding a Web Conferencing Management Server Rsync user account ... 184
Generating an SSH user key ... 185
Copying the SSH key ... 185
Migrating to and from a DMZ ... 186
Checklist for migrating to a DMZ ... 187
Migrating the Web Conference Server to the DMZ ... 188
Migrating the Web Conference Server from the DMZ ... 190
Chapter 11: Installing and configuring the Document Conversion Server ... 193
The Document Conversion Server and the Microsoft Office® operating system ... 193
Introduction to installing and configuring the Document Conversion Server ... 193
Disabling automatic installation of Microsoft Windows updates ... 195
Verifying the Java version ... 195
Configuring the Java bin folder through Windows ... 196
Configuring the SNMP service ... 197
Activating Microsoft Office 2013 license ... 198
Installing Microsoft Visual C++ 2008 Redistributable ... 199
Disabling macros in Microsoft Office ... 200
Installing the Document Conversion Server ... 200
Restricting access to the Document Conversion Server ... 201
Configuring SSL/TLS on the Document Conversion Server ... 202
Starting and stopping the Document Conversion Server ... 204
Configuring the Document Conversion Server to start automatically ... 205
Adding the Document Conversion Server on Element Manager ... 205
Configuring the Document Conversion Server on Element Manager ... 206
Optional: Disabling SSL/TLS on the Document Conversion Server ... 207
Chapter 12: Deploying and starting the remaining Network Elements ... 209
Starting Server Monitors ... 209
Starting Database Monitors ... 210
Deploying and starting secondary Element Manager Network Element ... 210
Deploying and starting an Accounting Manager Network Element ... 212
Deploying and starting a Provisioning Manager Network Element ... 213
Deploying and starting an Application Server Network Element ... 215
Enabling replication on the Avaya Media Server ... 216
Deploying and starting the Avaya Media Server Network Element ... 217
Deploying and starting the Web conferencing Network Elements ... 218
Deploying and starting the Web conferencing management Network Elements ... 219
Deploying and starting Personal Agent Network Elements ... 219
Verifying local/emergency access to the Provisioning Client ... 221

Verifying local access to Collaboration Agent ... 223
Verifying the status of all system components ... 224
Chapter 13: Configuring single sign-on for Element Manager Console and Provisioning Client ... 227
Introduction ... 227
Configuring time on System Manager and network elements ... 227
Configuring the application server network elements on System Manager ... 229
Launching Element Manager Console and Provisioning client from System Manager ... 231
Chapter 14: Configuring routing between System Manager and Avaya Aura® Conferencing ... 233
Configuring the route to Avaya Aura® Conferencing on System Manager ... 233
Configuring TLS route to Session Manager from the Element Manager ... 235
Chapter 15: Provisioning system settings and users for Avaya Aura® Conferencing 237
Adding MeetMe, Adhoc, and Event service URIs in Provisioning Client ... 237
Creating a user template ... 238
Creating a conference class of service user template ... 239
Creating a video class of service user template ... 240
Configuring display numbers in Provisioning Client ... 241
Deleting display numbers in Provisioning Client ... 242
Adding a location ... 242
Assigning media server clusters to locations ... 243
Assigning media server clusters to a physical location ... 244
Making Avaya Aura® Conferencing aware of System Manager domains ... 244
Enabling the automatic synchronization of domains ... 245
Adding System Manager domains in Provisioning Client ... 246
Assigning the conferencing profile to new System Manager users ... 246
Assigning the conferencing profile to existing System Manager users ... 248
Assigning the conferencing profile to a group of System Manager users ... 250
Verifying access to the MeetMe conference ... 253
Associating Web conferencing resources with a location in Provisioning Client ... 254
Configuring a Web conferencing host ... 255
Configuring an operator ... 256
Configuring the system operator ... 256
Configuring Event conferencing ... 257
Configuring Avaya Media Server cascading ... 258
Configuring the codecs for the cascading trunks ... 259
Configuring a regional cascading location ... 260
Media Cascading Locations tab field descriptions ... 261
Configuring bandwidth management ... 262
Chapter 16: Configuring Audio SRTP ... 265
Audio SRTP configuration tasks ... 265
Administering the Audio SRTP settings for Avaya Aura Conferencing ... 266
SRTP Settings dialog box field descriptions ... 267
Modifying Communication Manager settings for Audio SRTP ... 270
Chapter 17: Configuring the recording feature ... 273
Checklist for configuring recording in a dedicated recording server deployment ... 273
Checklist for configuring recording in a co-resident deployment ... 274

Dedicated recording server deployment only ... 275
Adding a media server dedicated for recording ... 275
Creating a certificate for the dedicated Recording server ... 278
Co-resident deployments only ... 279
Configuring recording for a media server cluster in a co-resident deployment ... 279
Both deployments ... 280
Assign a Recording media server cluster to locations ... 280
Configuring the Recording media server cluster for locations ... 281
Configuring the system-wide Recording setting ... 281
Configuring the recording feature for users ... 282
Configuring the Recording backup server ... 286
Chapter 18: Configuring a load balancer ... 289
Introduction to installing and configuring a load balancer ... 289
Configuring a load balancer ... 291
Chapter 19: Alarm and log forwarding to System Manager ... 295
Enabling alarm forwarding to System Manager ... 295
Disabling alarm forwarding to System Manager ... 296
Checklist for forwarding logs to System Manager ... 297
Generating enrollment password on System Manager ... 298
Configuring Element Manager log UDP client feed rule ... 298
Enabling log forwarding to System Manager ... 300
Disabling log forwarding to System Manager ... 301
Chapter 20: Secure Access Link Gateway ... 303
Secure Access Link Gateway overview ... 303
Enabling alarm forwarding to the SAL gateway ... 303
Disabling alarm forwarding to the SAL gateway ... 305
Chapter 21: Configuring Communication Manager system parameters ... 307
Checklist for Communication Manager parameter settings ... 307
Modifying Communication Manager system parameters ... 308
Modifying Signaling Groups ... 309
Optional: Modifying IP network region for private numbering ... 310
Modifying IP options system parameters ... 310
Modifying IP codec sets ... 311
Chapter 22: Integrating Avaya Aura® Conferencing with LDAP directory servers ... 313
Pre-deployment checklist for LDAP integration ... 313
LDAP integration tasks ... 314
Configuring the physical sites ... 316
Configuring the IP addresses and ports for the directory servers ... 317
Adding the directory domains ... 319
Configuring directory servers ... 319
Configuring the directory synchronization service ... 321
Configuring the directory authentication service ... 325
Configuring the directory access passcode settings ... 326
Passcodes encryption ... 327
Configuring multiple directory domains ... 328
Configuring LDAP directory-synchronized users on System Manager ... 328
Retrieving the CA certificate from the Active Directory server ... 330

Assigning the Directory Server Certificate for the network elements 331
Chapter 23: Deploying Audio/Video in Collaboration Agent 333
Pre-deployment checklist for Audio/Video in Collaboration Agent 333
Checklist for installing Audio/Video in Collaboration Agent 337
Configuring ports for Audio/Video in Collaboration Agent 339
Accessing and extracting the Audio/Video in Collaboration Agent installation files 342
Configuring Audio/Video in Collaboration Agent for a coresident deployment 343
Installing the Audio/Video in Collaboration Agent server software 344
Installing the Audio/Video in Collaboration Agent Management Portal software 347
Configuring the Flash Media Gateway 349
Adding a Flash Media Gateway cluster 351
Starting the Flash Media Gateway 353
Creating the client configuration file 353
Installing the Audio/Video in Collaboration Agent client software 355
Verifying integration of the multimedia client software with Collaboration Agent 356
Hardening Audio/Video in Collaboration Agent 357
Creating a System Manager- signed certificate for the Flash Media Gateway IP address 358
Creating a VeriSign-signed certificate for the Flash Media Gateway 359
Securing the JMX connection between the Flash Media Gateways and the RTMPS connection to the Flash Media Gateway Management server 360
Configuring a secure SIP TLS connection from the Flash Media Gateway to Avaya Aura® Session Manager 361
Configuring a secure RTMPS connection between the Flash Media Gateways and the Audio/Video in Collaboration Agent clients 362
Upgrading Audio/Video in Collaboration Agent 365
Chapter 24: Hardening Avaya Aura® Conferencing 367
Configuring the BIOS password 367
Configuring the BIOS boot order 367
Setting operating system inactive account auditing 368
Configuring the operating system warning banners 368
Configuring the pre-login warning banner 369
Configuring the post-login warning banner 369
Verifying the warning banners 370
Configuring operating system password and account policies 370
Resetting the GRUB password 371
Hardening the database 372
Configuring administrator accounts 372
Creating new user-specific accounts 372
Allowing administrator sudo access 374
Loading a new authentication file 375
Deleting pre-configured OS administrator accounts 375
Configuring the access control list (ACL) 376
Configuring internal ACL rules 377
Configuring external ACL rules 379
Configuring a file system baseline 388
Enabling Tomcat webserver access and error logs for the Element Manager 388
Enabling Tomcat webserver access logs and audit logging for the Provisioning Manager 389
Enabling Tomcat webserver access logs and audit logging for the Personal Agent Manager 390

Configuring local logon password policies for Element Manager Console and Provisioning Client 391
Configuring local logon account login rules for Element Manager Console and Provisioning Client 391
Changing the Element Manager SNMP community string 392
Removing the default staging certificates 393
Configuring Avaya Media Server DSCP 394
Fixing remote host SSH keys 394
Chapter 25: Configuring collaboration aware clients for Avaya Aura® Conferencing. 397
Configuring the settings for Avaya Flare® Experience for Windows 397
Configuring the settings for Avaya Flare® Experience for iPad Devices 398
Configuring the settings for Avaya 96x1 SIP telephones 400
Chapter 26: Deploying the Avaya Aura® Conference Manager Add-in for Microsoft Outlook® 401
Implementing a ClickOnce deployment 402
Implementing a centralized software deployment 403
Chapter 27: Upgrading to Release 7.2 407
Upgrading a co-resident deployment to Release 7.2 410
Before you begin checklist 410
Upgrade procedure for a co-resident deployment 412
Installing the 900 Gb hard drives into the HP DL360 G7 server 417
Reconfiguring the RAID 1 arrays using the HP SmartStart CD 418
Formatting and mounting the second RAID 419
Upgrading a standalone deployment to Release 7.2 421
Before you begin checklist 421
Upgrade procedure for a standalone deployment 423
Common administration procedures 443
Stopping a non-Avaya Media Server network element instance 443
Undeploying a network element instance 444
Locking and stopping an Avaya Media Server instance 445
Patching the Avaya Aura Conferencing Platform 446
Upgrading a network element instance 447
Upgrading an Avaya Media Server 448
Upgrading a Document Conversion Server 449
Verifying system operation for a location after an upgrade 451
Verifying system operation for a location 451
Upgrading memory for the HP DL360 G7 server 452
Chapter 28: Installing feature packs 455
Feature pack installation procedure 457
Chapter 29: Installing service packs and patches 463
Checklist for upgrading and patching Avaya Aura® Conferencing 466
Copying and extracting installation files to servers 467
Applying operating system patches to the system servers 470
Stopping a Network Element instance 472
Locking and stopping an Avaya Media Server instance 473
Stopping a database instance 474
Patching the operating system 474
Starting a database instance 476
Starting a Network Element instance 476

Starting and unlocking an Avaya Media Server instance ... 477
Deploying and starting the core Network Element instances on the Primary servers ... 478
Applying patches to the database software ... 479
Upgrading or patching the Avaya Aura® Conferencing software ... 480
Upgrading the MCP database and Element Manager ... 483
Patching the MCP database and Element Manager ... 484
Patching or upgrading a network element ... 485
Upgrading the Avaya Media Server software ... 486
Upgrading the Document Conversion Server ... 487
Upgrading Audio/Video in Collaboration Agent ... 488
Patching database software ... 492
Deploying a network element instance ... 493
Configuring a DNS client ... 494
Chapter 30: Backing up Avaya Aura® Conferencing ... 497
Backing up the database ... 499
Backing up the database manually ... 499
Scheduling automatic database backups ... 500
Removing scheduled automatic database backups ... 501
Backing up an Avaya Media Server ... 502
Backing up an Avaya Media Server manually ... 502
Scheduling automatic backups on an Avaya Media Server ... 503
Removing scheduled automatic database backups ... 504
Backing up an Avaya Aura® Conferencing server ... 505
Backing up an Avaya Aura® Conferencing server to a local folder ... 507
Backing up an Avaya Aura® Conferencing server to remote server ... 508
Backing up an Avaya Aura® Conferencing server to a USB drive ... 509
Configuring remote backup parameters ... 510
Enabling and configuring the remote backup configuration parameters ... 511
Disabling the remote backup configuration parameters ... 512
Configuring and verifying SSH keys ... 513
Cleaning up SSH keys ... 513
Setting the remote configuration backup parameters to the default values ... 514
Viewing the list of backup sets ... 515
Configuring individual remote backup parameters ... 515
Removing unneeded loads from the Element Manager servers ... 516
Removing unneeded installers of PostgreSQL from the Element Manager server ... 517
Backing up FSI data ... 518
Creating an FSI baseline ... 518
Backing up FSI baselines to a local drive ... 519
Backing up FSI baselines to a remote server ... 519
Backing up FSI baselines to a USB drive ... 520
Chapter 31: Restoring Avaya Aura® Conferencing ... 521
Restoring an Avaya Aura® Conferencing server ... 522
Restoring an Avaya Aura® Conferencing server from a local drive ... 523
Restoring an Avaya Aura® Conferencing server from a remote disk ... 524
Restoring an Avaya Aura® Conferencing server from a USB drive ... 525
Restoring the database ... 525

Restoring the primary database from a backup file ... 526
Restoring an Avaya Media Server ... 528
Restoring FSI data ... 529
Restoring FSI baselines from a local drive ... 529
Restoring FSI baselines from a remote server ... 530
Restoring FSI baselines from a USB drive ... 530
Chapter 32: Uninstalling software ... 533
Introduction to uninstalling software ... 533
Checklist for uninstalling Application Server software ... 533
Stopping and undeploying a network element instance ... 534
Stopping and undeploying Element Manager ... 534
Cleaning up the Application Server database ... 535
Uninstalling the database software ... 535
Checklist for uninstalling the Avaya Media Server software ... 536
Uninstalling the Avaya Media Server ... 536
Appendix A: Shutting down and starting the Avaya Aura® Conferencing system ... 539
Shutting down the Avaya Aura® Conferencing system ... 539
Starting the Avaya Aura® Conferencing system after a shutdown ... 540
Appendix B: Migrating existing data to Avaya Aura Conferencing 7.2 ... 541
Introduction to migrating your data ... 541
Installing the data migration tool ... 541
Exporting data from Meeting Exchange 5.2 or Avaya Aura® Conferencing 6.0 ... 542
Checking connection between Avaya Aura® Conferencing and System Manager ... 543
Importing data from Meeting Exchange 5.2 or Avaya Aura® Conferencing 6.0 ... 544
Appendix C: Re-IPing the Application Server ... 551
Introduction to re-IPing the Avaya Aura® Conferencing servers ... 551
Preparing your data for re-IP ... 551
Preparing server data ... 552
Preparing application data ... 553
Preparing role data ... 555
Checklist for reIPing an Avaya Aura® Conferencing system ... 556
Shutting down Avaya Aura® Conferencing core applications ... 557
Configuring Access Control List to system default ... 558
Updating IP addresses for the server ... 559
Updating the hostname and clock source ... 560
Updating Element Manager, database, and network element IP addresses ... 562
Updating hostnames, Element Manager, and network element certificates ... 563
Shutting down the application ... 565
Configuring ACL ... 565
Starting the application and the database ... 566
Appendix D: Using OpenSSL for Certificate Signing Requests ... 567
Introduction ... 567
Generating a private key ... 567
Generating a Certificate Signing Request ... 568
Creating a PKCS#12 file ... 568
Removing the passphrase key file ... 569
Appendix E: Downgrading a system ... 571

Introduction to downgrading your system ... 571
Prerequisites for performing a downgrade ... 571
Checklist for downgrading when a replicated database upgrade fails ... 574
Checklist for downgrading a system—co-resident with redundancy or standalone with redundancy layout 575
Stopping a Network Element instance ... 577
Dropping database replication ... 577
Verifying the database backup file on the secondary database ... 578
Restoring the database backup file to the secondary database ... 578
Downgrading the Avaya Media Server ... 579
Downgrading the Network Elements ... 580
Downgrading the Element Manager ... 581
Resyncing the database ... 581
Checklist for downgrading a system—co-resident simplex or standalone simplex layout ... 582
Restoring install scripts ... 583
Restoring the old database backup to the database ... 584
Downgrading the Avaya Media Server ... 585
Downgrading the Element Manager ... 585
Downgrading the Network Elements ... 586
Appendix F: DNS and Avaya Aura Conferencing ... 589
DNS and Avaya Aura® Conferencing ... 589
Updating the host table entries ... 589
Glossary ... 591
Index ... 595

Chapter 1: An Introduction to Avaya Aura® Conferencing

About this document

This document provides an overview of the components and services that comprise the Avaya Aura® Conferencing solution. This document also contains technical specifications and requirements, and a list of procedures required to install and configure this solution. This document describes the procedures to perform the initial installation and deployment of Avaya Aura® Conferencing Application Server software and Avaya Media Server software.

Related resources

Documentation

Obtain the following related documents and documents about other Avaya products mentioned in this guide from the Avaya Support website:http://www.avaya.com/support:

- *Avaya Aura® Conferencing 7.2 Overview and Specification*
- *Avaya Aura® Conferencing 7.2 Security*
- *Avaya Aura® Conferencing 7.2 Accounting Records Reference*
- *Avaya Aura® Conferencing 7.2 Alarms and Logs Reference*
- *Avaya Aura® Conferencing 7.2 Operational Measurements Reference*
- *Avaya Aura® Conferencing Collaboration Agent Quick Reference*
- *Deploying Avaya Aura® Conferencing 7.2*
- *Administering Avaya Aura® Conferencing 7.2*
- *Maintaining and Troubleshooting Avaya Aura® Conferencing 7.2*
- *Using Avaya Aura® Conferencing Collaboration Agent*

Training

The following courses are available on http://www.avaya-learning.com. In the **Search** field, type the course code, and click **Go** to search for the course.

Course code	Course title
5U00120V	Avaya Aura® Conferencing 7.0 Implementation, Maintenance, and Troubleshooting
3202	Avaya Aura® Conferencing Release 7.x Implementation and Maintenance
2U00032O	Selling Avaya Aura® Conferencing 7 - Level 1
2U00033O	Selling Avaya Aura® Conferencing 7 - Level 2
2U00325O	Avaya Aura® Conferencing 7 L1 Customer Scenario
3U00025O	Designing Avaya Aura® Conferencing 7.0 - Tech Sales L1

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Go to http://www.youtube.com/AvayaMentor and perform one of the following actions:

- Enter a key word or key words in the Search Channel to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Support

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

Audience

The intended audience for this document is:

- Tier 1 Avaya technical support
- Avaya Professional Services
- Authorized Business Partners

You must have the following core competencies:

- The ability to access servers using:
  - a locally attached keyboard and monitor or KVM (Keyboard, Video, Mouse) switch
  - the ssh remote access protocol
- Basic Linux operations:
  - navigating the file system (changing directories)
  - managing the implications of uninformed or careless use of system commands while logged in as the root user
- Basic server tasks:
  - powering servers up
  - powering servers down
  - resetting servers
  - inserting and removing CD-ROM and DVD-ROM disks
- Basic Microsoft knowledge:

  Windows:
  - editing text files
  - creating folders
  - Microsoft Excel:
    - transitioning between worksheets of a workbook
    - entering data into cells
    - copying/pasting between cells and commands, such as Control+c, Control+v, and Edit > Paste Special menu
- The ability to operate a supported Web browser (such as Firefox or Internet Explorer):
  - Interacting with pop-up windows

- Inspecting and accepting x.509 certificates and installing CA certificates that are presented by the browser
- Downloading and installing software through the browser

• Basic Public Key Infrastructure (PKI) tasks:

- Creating Certificate Signing Requests (CSR)
- Inspecting the details of a certificate
- Installing Certificate Authority certificates on Windows Certificate Store
- Installing Personal certificates on Windows Certificate Store
- Installing Certificate Authority certificates on Firefox Certificate Manager
- Installing Your Certificates on Firefox Certificate Manager

How to use this document

You must complete a given task successfully before beginning the next one. If you encounter issues while performing a step, contact the Avaya Support Web site at http://support.avaya.com to open a service request.

Use the Avaya Aura® Conferencing 7.2 Intelligent Workbook together with this document to guide you through the preparatory requirements and installation and configuration steps for Avaya Aura® Conferencing. The Intelligent Workbook can be found on the Avaya Web site at http://support.avaya.com/.

Related topics:

Preparing your data using the Avaya Aura Conferencing 7.2 Intelligent Workbook on page 20

Preparing your data using the Avaya Aura® Conferencing 7.2 Intelligent Workbook

The Avaya Aura® Conferencing 7.2 Intelligent Workbook has the following tabs to assist you through the installation process:

• Instructions

• 0-Configuration Data

• 1-OS Linux Install

• 2-OS Patches Install

• 3-ACC Apps Install

- 4-Licensing
- 5-Single sign-on
- 6-Config AAC Services
- 7-Config Avaya Aura
- 8-Provisioning
- 9-Web Conferencing: Enabling Web conferencing
- 10-DCS: Installing the Document Conversion Server
- A-Flare for Windows and iPad
- B-Update AAC
- C-Apply patches
- FAQ
- Troubleshooting
- Values

Solution requirements

Before installing and configuring Avaya Aura® Conferencing, make sure the following products are already installed, configured, and fully operational:

- Avaya Aura® Communication Manager Release 5.2.1, 6.0.1, or 6.2
- Avaya Aura® Session Manager Release 6.2
- Avaya Aura® System Manager Release 6.2 or 6.3

The following documents are required for setting up the Avaya Aura® solution.

Communication Manager

To install and configure Avaya Aura® Communication Manager, see:

- *Administering Network Connectivity on Aura® Communication Manager*
- *Administering Avaya Aura® Communication Manager*

Session Manager

To install and configure Avaya Aura® Session Manager, see:

- *Administering Network Connectivity on Avaya Aura® Session Manager*
- *Administering Avaya Aura® Session Manager*

- *Administrator Guide for Avaya Aura® Session Manager*
- *Installing Avaya Aura® Session Manager*

System Manager

To install and configure Avaya Aura® System Manager, see:

- *Administering Network Connectivity on Avaya Aura® System Manager*
- *Administering Avaya Aura® System Manager*
- *Installation Guide for Avaya Aura® System Manager*

License key

Licensing functionality operates in a different way, depending on your type of Avaya Aura® Conferencing deployment.

You can deploy Avaya Aura® Conferencing 8.0 with the Avaya Aura® platform. The Avaya Aura® platform consists of Avaya Aura® System Manager and Avaya Aura® System Platform. This type of deployment is called an Avaya Aura® deployment. Alternatively, you can deploy Avaya Aura® Conferencing 8.0 without the Avaya Aura® platform. This type of deployment is called a Universal deployment.

In an Avaya Aura® deployment, licensing is supported on the Application Server and the Media Server. The License key is installed on the Web License Manager (WebLM) server which is co-resident with System Manager. The license key must be obtained prior to starting the deployment.

WebLM is a client/server model where numerous clients can share the same WebLM server and the same license key. For more information, see Installing the license key on on page 151.

In a Universal deployment, licensing is also supported by WebLM. However, in a Universal deployment, the WebLM server is embedded with Avaya Aura® Conferencing. For more information, see Applying a license key.

For both solutions, a grace period of 30 days exists for upgrades and new installations. Additionally, new upgrades and installations include a number of default licenses. If the licensing limits are exceeded, Avaya Aura® Conferencing displays full explanatory error messages to users. Licenses must be periodically renewed. If they are not renewed, they expire.

The license monitors:

- Maximum number of audio web users
- Maximum number of video web users
- Maximum number of conference recording sessions

- Maximum number of media servers
- Maximum number of web conferencing servers

Administrative user roles and preconfigured accounts

Roles define operational boundaries (access permissions) for administrators. Administrators can have more than one role, depending on their duties. You assign roles to new administrators when you create their accounts. During server installation, the installation software creates the following user accounts:

Preconfigured /Admin accounts	Default password	Preassigned role	Description
ntsysadm	password	System Security Administrator (SSA) role.	The SSA can perform system configuration and specify security attributes such as: • Password configuration • User management • Certificate management • Access control • Antivirus • File System Integrity tools • Network configuration • System backup and restore
ntappadm	password	Application Administrator (AA) role	The AA can install the Avaya Aura® Conferencing application software and manage components related to the application. The AA is responsible for installing, maintaining, patching, and upgrading Avaya Aura® Conferencing software only.
ntsecadm	password	Security Auditor (SA) role	The SA can collect and view security audit logs and syslogs at the platform level. The SA can also transfer the security logs off the server.
ntbackup	password	Backup Administrator (BA) role	The BA can perform only system backups. A BA cannot perform:

Preconfigured /Admin accounts	Default password	Preassigned role	Description
			• any operation on the server except backups. • a system restore—only the SSA or root user can perform a system restore.
ntdbadm	password	Database Administrator (DBA) role	The DBA can manage the database schemas and database tools on servers where the database resides. The server must host the database for this role to be relevant.
ntossadm	password	Operational Support System Administrator (OSS) role	Downstream processors can use the ntossadm account with this role to connect to the server and collect OSS logs.
admin admin1 admin2 admin3 admin4 admin5	admin admin1 admin2 admin3 admin4 admin5	Unlimited privileges	For expert mode login to Avaya Aura® Conferencing, Element Manager, and Provisioning Manager.
init	Not applicable	System Security Administrator (SSA) role and Database Administrator (DBA) role	SSA and DBA account for Avaya Services access.
craft	Not applicable	Application Administrator (AA) role	AA account for Avaya Services access

Supported Web browsers

Avaya Aura® Conferencing supports the following browsers for Collaboration Agent users and Avaya Aura® Conferencing administrators. Administrators use the following applications to administer and maintain Avaya Aura® Conferencing:

- Element Manager Console
- Provisioning Client
- Avaya Conferencing Reports & Monitors

Browsers	Operating System	Collaboration Agent	Administration Applications
Microsoft Internet Explorer 7.0 and 8.0	Windows XP Windows 7	yes	yes
Microsoft Internet Explorer 9.0 and 10.0	Windows 7	yes	yes
Mozilla Firefox version 10 and later	Windows XP Windows 7	yes	yes

Possible limitations

When running the Audio/Video in Collaboration Agent feature, Google Chrome may demonstrate poor lip synchronization. When Collaboration Agent detects when a user wishes to use the Audio/Video in Collaboration Agent feature in Google Chrome, it displays an information message to inform them of this possible limitation.

In addition, users running Google Chrome for the Mac operating system may experience issues when sharing their desktop. Avaya recommends using Apple Safari or Mozilla Firefox for desktop sharing instead.

Supported hardware

HP ProLiant DL360 G7

Avaya Aura® Conferencing 7.2 supports the HP ProLiant DL360 G7 for all deployment configurations.

Note:

If you are upgrading from Avaya Aura® Conferencing 6.0 or Meeting Exchange 5.2, you can repurpose your Dell™ PowerEdge™ R610 or IBM S8800 as a Document Conversion Server for web conferencing. For Avaya Aura® Conferencing 7.2, you must install the Avaya Aura® Conferencing software on the HP ProLiant DL360 G7 server.

Chapter 2: Deployment options

Deployment layouts

Avaya Aura® Conferencing supports the following deployment layouts:

Table 1: Deployment layouts

Deployment layout	Description	Features	Scalable	Enterprise DMZ deployment
Co-resident with redundancy	For small scale deployments where redundancy is required. The Avaya Media Server is co-resident with the Application Server.	• Avaya Media Server with load sharing • Web Conferencing Management Server • Active/active redundancy for Document Conversion Server for Web Conferencing Server/ Collaboration Agent • Active/standby redundancy with an additional Application Server	Yes, scalable to a standalone deployment	Yes, add Web Conferencing Server components within your firewall demilitarized zone (DMZ) for added functionality. For more information about DMZ, see Enterprise DMZ deployment on page 62.
Co-resident simplex	For small scale deployments where all the Application Server components reside on a single server and redundancy is not required. The Avaya Media Server is co-resident with the	• Web Conferencing Server with Collaboration Agent • Web Conferencing Management Server	Yes, scalable to a standalone deployment	Yes, add Web Conferencing Server components within your firewall demilitarized zone (DMZ) for added functionality. For more information about DMZ, see Enterprise DMZ

Deployment layout	Description	Features	Scalable	Enterprise DMZ deployment
	Application Server.			deployment on page 62.
Co-resident with redundancy with DMZ	For small scale deployments where redundancy is required. The Avaya Media Server is co-resident with the Application Server. Web Conferencing Server components are deployed within your firewall DMZ.	• Avaya Media Server with load sharing • Web Conferencing Management Server • Active/active redundancy with Document Conversion Server for Web Conferencing Server/ Collaboration Agent • Active/standby redundancy with an additional Application Server	Yes, to a standalone deployment	Yes
Co-resident simplex with DMZ	For small scale deployments where all the Application Server components reside on a single server and redundancy is not required. The Avaya Media Server is co-resident with the Application Server. Web Conferencing Server components are deployed within your firewall DMZ.	• Avaya Media Server with load sharing • Web Conferencing Server with Collaboration Agent • Web Conferencing Management Server	Yes, to a standalone deployment	Yes

Deployment layout	Description	Features	Scalable	Enterprise DMZ deployment
Standalone with redundancy	For medium to large scale deployments. One pair of redundant Application Servers are dedicated for element management, database, application and service, and accounting functions. One server is dedicated to Avaya Media Server components.	• Avaya Media Server with load sharing • Web Conferencing Server with Collaboration Agent • Web Conferencing Management Server for web conferences with more than 1500 participants. • Active/active redundancy with Document Conversion Server for Web Conferencing Server with Collaboration Agent • Active/standby redundancy with an additional Application Server	Yes, scalable with additional servers, if required.	Yes, with additional Web Conferencing Server components in the enterprise Demilitarized Zone (DMZ) for added functionality. For more information about DMZ, see Enterprise DMZ deployment on page 62.
Standalone simplex	For medium to large scale deployments where all the Application Server components reside on separate servers to provide higher capacities and where redundancy is not required.	• Avaya Media Server with load sharing • Web Conferencing Server with Collaboration Agent • Document Conversion server • Web conferencing management server for Web conferences with more than 1500 participants.	Yes, with additional servers, if required.	Yes, with additional Web Conferencing Server components in the enterprise DMZ for added functionality. For more information about DMZ, see Enterprise DMZ deployment on page 62.

Performance specifications

The following sections provide the performance specifications for Avaya Aura® Conferencing.

Related topics:

Servers on page 30
Deployment layouts and DMZ on page 32
Coresident deployment without the DMZ access and the Audio/Video in Collaboration Agent feature on page 33
Coresident deployment with the DMZ access and the Audio/Video in Collaboration Agent feature on page 34
Standalone simplex and standalone with redundancy deployment layouts on page 37
Media cascading on page 41
Flash Media Gateway on page 42

Servers

The following table provides the specifications of the Avaya Aura® Conferencing servers.

Note:

- If your deployment contains more than one Web server, you must administer a third-party Web load balancer for Collaboration Agent.
- The IBM S8800 and Dell™ PowerEdge™ R610 servers can only be repurposed if you are migrating from Avaya Aura® Conferencing Release 6.0. You cannot deploy these servers as coresident servers in an Avaya Aura® Conferencing Release 7.2 deployment.

Table 2: Server specifications

Server	CPU	Memory (GB)	Hard disk drive (GB)	Applications
HP ProLiant DL360 G7 as an application server	Intel® Xeon® E5620 2xQuad core @ 2.4 GHz	6 x 2 = 12	2 x 300	An application server with the following network elements: • Application Server • Provisioning Manager • Element Manager • Database Manager • Accounting Manager • Web Conferencing Management Server

Server	CPU	Memory (GB)	Hard disk drive (GB)	Applications
HP DL360 G7 as one of the following servers: • Coresident server • Coresident server with the licensed Recording feature enabled • Standalone recording server	Intel® Xeon® X5670 2xHEX core @ 2.93 GHz	(6 x 2) + (6 x 4) = 36	2 x 300 or 2 x 900	A coresident server with the licensed Recording feature enabled and the following network elements: • Application Server • Provisioning Manager • Element Manager • Database Manager • Accounting Manager • Media Server • Collaboration Agent • Web Conferencing Server • Web Conferencing Management Server or A recording media server with the Media Server network element that has the licensed Recording feature enabled.
HP DL360 G7 as one of the following servers: • Standalone media server • Standalone Web server • Flash media gateway	Intel® Xeon® X5670 2xHEX core @ 2.93 GHz	6 x 2 = 12	2x300	Media Server that: • Manages local conferences. • Hosts cascaded conferences. • Manages cascading sessions at remote sites. or Media Server with the Event Conference Server network element. or A Web server with the following network elements: • Personal Agent Manager • Web Conferencing Server or Flash Media Gateway with the Audio/Video in Collaboration Agent network element

Server	CPU	Memory (GB)	Hard disk drive (GB)	Applications
HP DL360 G7 is a low cost server that is deployed as one of the following servers: • Web server. • Cascading media server. • Document conversion server.	Intel® Xeon® E5620 1xQuad core at 2.4 GHz	4 x 2 = 8	2x300	A low cost Web server with the Audio/ Video in Collaboration Agent network element for a coresident deployment or A Web server for a coresident deployment or A low cost Media Server for cascaded sites or A document conversion server for a standalone deployment
IBM S8800 repurposed as a Web server	Intel® Xeon® X5670 2xQuad core at 2.93 GHz	6 x 4 = 24	5x146	A repurposed server with the following network elements: • Web Server • Audio/Video in Collaboration Agent
Dell R610 repurposed as a Web server	Intel® Xeon® X5670 2x HEX core at 2.93 GHz	6 x 4 = 24	5x146	A repurposed server with the following network elements: • Web Server • Audio/Video in Collaboration Agent

Deployment layouts and DMZ

For the Audio/Video in Collaboration Agent feature, you must deploy:

- A separate Web server in the enterprise DMZ for Web conferencing and Collaboration Agent.
- An optional Flash Media Gateway in the enterprise DMZ for external users to join a conference using the Audio/Video in Collaboration Agent feature.

Note:

If you want external users to join a conference using the Audio/Video in Collaboration Agent feature, you must deploy Flash Media Gateway in the enterprise DMZ.

The following table lists the network elements that are deployed in the enterprise network and DMZ:

Table 3: Network elements

Network elements in the enterprise network	Network elements in the enterprise DMZ
• Application Server • Media Server • Web Conferencing Server • Web Conferencing Management Server • Collaboration Agent	• Web Conferencing Server • Collaboration Agent • (Optional) Flash Media Gateway

Coresident deployment without the DMZ access and the Audio/ Video in Collaboration Agent feature

The following table provides the performance specifications of a coresident server.

Table 4: Performance specifications of a coresident server deployment without the DMZ access and the Audio/Video in Collaboration Agent feature

Server	Codec			Pixels (p) x 30fps	Bandwidth usage (kbps)	Active sessions		
	Audio	Video				Audio	Web and Collaboration Agent	Video
A coresident server with the following network elements and the licensed Recording feature enabled: • Application Server • Media Server • Web Conferencing Server	Audio and Web	—	—	—	—	500 audio, 500 Web and Collaboration Agent, and 320 720p, SVC video sessions		
	G.711	—	—	—	83	500	—	—
	G.722	—	—	—	83	500	—	—
	G.729	—	—	—	30	300	—	—
	G.711	H.264	AVC	720	1264	500	500	400
				360	512	500	500	500
			SVC	720	1530	500	500	320
				360	512	500	500	500

Server	Codec			Pixels (p) x 30fps	Bandwidth usage (kbps)	Active sessions		
	Audio	Video				Audio	Web and Collaboration Agent	Video
• Web Conferencing Management Server • Collaboration Agent This deployment supports a maximum of: • 5000 users. • 250 sessions for each conference. **Note:** The bandwidth usage of sharing the library and desktop depends on the type of document and might vary.	G.722	H.264	AVC	720	1264	500	500	400
				360	512	500	500	500
			SVC	720	1530	500	500	320
				360	512	500	500	500
	G.729	H.264	AVC	720	1264	300	300	300
				360	512	300	300	300
			SVC	720	1530	300	300	300
				360	512	300	300	300
	Library sharing	—	—	—	32	—	—	—
	Desktop sharing	—	—	—	453	—	—	—
	Collaboration Agent	—	—	—	—	—	—	—
	Recording	—	—	—	—	80 simultaneous sessions		
	Playback	—	—	—	—	30 simultaneous sessions, which might be a combination of the streaming and downloading sessions		

Coresident deployment with the DMZ access and the Audio/Video in Collaboration Agent feature

These tables provide the performance specifications of the coresident server and a separate low-cost Web server that is deployed in the enterprise DMZ with Flash Media Gateway for the Audio/Video in Collaboration Agent feature.

The following table provides the performance specifications of a coresident server:

Table 5: Performance specifications of a coresident server

Server	Codec			Pixels (p) x 30fps	Bandwidth usage (kbps)	Active sessions		
	Audio	Video				Audio	Web and Collaboration Agent	Video
A coresident server with the following network elements and the licensed Recording feature enabled: • Application Server • Media Server • Web Conferencing Server • Web Conferencing Management Server • Collaboration Agent This deployment supports a maximum of: • 5000 users. • 250 sessions for each conference. **Note:** The bandwidth usage of sharing the library and desktop depends on	Audio and Web	—	—	—	—	500 audio, 500 Web and Collaboration Agent, and 320 720p, SVC video sessions		
	G.711	—	—	—	83	500	—	—
	G.722	—	—	—	83	500	—	—
	G.729	—	—	—	30	300	—	—
	G.711	H.264	AVC	720	1264	500	500	400
				360	512	500	500	500
			SVC	720	1530	500	500	320
				360	512	500	500	500
	G.722	H.264	AVC	720	1264	500	500	400
				360	512	500	500	500
			SVC	720	1530	500	500	320
				360	512	500	500	500
	G.729	H.264	AVC	720	1264	300	300	300
				360	512	300	300	300
			SVC	720	1530	300	300	300
				360	512	300	300	300
	Library sharing	—	—	—	32	—	—	—
	Desktop sharing	—	—	—	453	—	—	—
	Collaboration Agent	—	—	—	—	—	—	—
	Recording	—	—	—	—	80 simultaneous sessions		
	Playback	—	—	—	—	30 simultaneous sessions, which might be		

Server	Codec			Pixels (p) x 30fps	Bandwidth usage (kbps)	Active sessions		
	Audio	Video				Audio	Web and Collaboration Agent	Video
the type of document and might vary.						a combination of the streaming and downloading sessions		

The following table provides the performance specifications of the low-cost Web server with Collaboration Agent and the Audio/Video in Collaboration Agent feature that is deployed in the enterprise DMZ:

Table 6: Performance specifications of a low cost server used as a Web server for the DMZ access and Flash Media gateway

Server	Protocol	Pixels (p) x 30 fps	Maximum Audio/Video in Collaboration Agent sessions	
			Audio and Video	Web
Web server and Flash Media Gateway on one of the following: • An HP DL360 G7 low cost server • A repurposed IBM S8800 server • A repurposed Dell R610 server Each of these servers supports a maximum of 500 Web sessions. **Note:** You must administer RTMPS for Flash Media Gateway.	RTMP	720	200	200
		360	300	300
		180	300	300
	RTMPT	720	150	200
		360	225	300
		180	225	300
	RTMPS	720	120	200
		360	180	300
		180	180	300

Standalone simplex and standalone with redundancy deployment layouts

The standalone deployment provides higher capacities than a coresident deployment with dedicated servers for the following network elements:

- Media Server
- Web Server
- Web Conferencing Management Server
- Document Conversion Server
- Event Conference Server

The following table provides the performance specifications of the standalone simplex and standalone with redundancy deployment layouts:

Table 7: Performance specifications of standalone simplex and standalone with redundancy deployment layouts

Note:

Assuming that 50% sessions for desktop sharing and 50% sessions for library sharing, for more than 3000 Web sessions, you must have a dedicated Web Conferencing Management Server.

Session type	Active sessions
Provisioned users	150000
Audio and video	15000
Web	7500
Collaboration Agent	7500
Audio, video, Web, and Collaboration Agent	7500 audio and video + 7500 Web + 7500 Collaboration Agent
Audio/Video in Collaboration Agent audio and video using RTMPS at a 360p x 30fps resolution	1600 with the maximum supported four Flash Media Gateways
Recording	375 simultaneous recordings
Playback	500 simultaneous sessions, which might be a combination of the streaming and downloading sessions

Related topics:

Standalone Media Server on page 38
Standalone Web Server on page 39

Standalone Web Conferencing Management Server on page 39
Standalone Document Conversion Server on page 40
Event Conference Server on page 40

Standalone Media Server

The following table provides the performance specifications of a standalone Media Server that is deployed in a standalone deployment layout:

Table 8: Performance specifications of a standalone Media Server

Server	Codec			Pixels (p) x 30fps	Bandwidth used (kbps)	Active sessions
	Audio	Video				
Standalone Media Server using TCP/RTP or TLS/SRTP **Note:** • The standalone Media Server can also be administered as a media cascading server. • As a cascading server, the final capacity of Media Server depends on the number of media cascading sites and the number of users in each conference and might be lower than the capacities provided in this table.	G.711	—	—	—	—	3000
	G.722	—	—	—	—	2500
	G.729	—	—	—	—	2000
	G.711	H.264	AVC	720	1264	600
				360	512	1500
			SVC	720	1530	480
				360	512	1200
	G.722	H.264	AVC	720	1264	575
				360	512	1360
			SVC	720	1530	460
				360	512	1200
	G.729	H.264	AVC	720	1264	540
				360	512	1200
			SVC	720	1530	440
				360	512	1080

Standalone Web Server

The following table provides the performance specifications of a standalone Web Server that is deployed in a standalone deployment layout:

Table 9: Performance specifications of a standalone Web Server

Server	Session type	Active sessions
Standalone Web Server with the following network elements: • Collaboration Agent Manager • Web Conferencing Server	Total simultaneous sessions	1500 Web conferencing + 1500 Collaboration Agent
	Web conferencing sessions only	1500
	Collaboration Agent sessions only	1500

Standalone Web Conferencing Management Server

The following table provides the performance specifications of a standalone Web Conferencing Management Server that is deployed in a standalone deployment layout:

Table 10: Performance specifications of a standalone Web Conferencing Management Server

Server	Deployment	Active sessions
Web Conferencing Management Server **Note:** • You must change the Maxclient/Server limit from 72 to 200 for a standalone Web Conferencing Management Server • The maximum active sessions are based on the assumption that 50% sessions are for desktop sharing and 50% sessions are for library sharing.	Standalone Web Conferencing Management Server	7500
	Web Conferencing Management Server coresident with Application Server	3000

Standalone Document Conversion Server

The following table provides the performance specifications of a standalone Document Conversion Server that is deployed in a standalone deployment layout:

Table 11: Performance specifications of Document Conversion Server

Server	Session type	Active sessions
Standalone Document Conversion Server	Simultaneous document upload sessions	200
	Simultaneous Web sessions	3000

Event Conference Server

The following table provides the performance specifications of Event Conference Server that is deployed in a standalone deployment layout:

Table 12: Performance specifications of Event Conference Server

Server	Codec			Pixels (p) x 30fps	Bandwidth used (kbps)	Active sessions		
	Audio	Video				Audio	Video	Web
Standalone Media Server and a standalone Web Server using TCP/RTP or TLS/SRTP	Any combination of G.711, G.722, or G.729	—	—	—	—	2000	—	1500
	All codecs	H.264	AVC	720	1200	2000	500	1500
				360	420	2000	1500	1500
			SVC	720	1500	2000	400	1500
				360	515	2000	1200	1500

Table 13: Performance specifications of an Event Conference Server with the Audio/ Video in Collaboration Agent feature

Server	Codec			Pixels (p) x 30fps	Bandwidth used (kbps)	Active sessions		
	Audio	Video				Audio	Audio/ Video in Collaboration Agent	Web
Standalone Media Server and standalone Web Server with Flash Media Gateway **Note:** The performance specifications of the Audio/ Video in Collaboration Agent sessions are based on RTMPS at a 360p x 30fps resolution.	All codecs	H.264	AVC	720	1200	2000	400	1500
				360	420	2000	400	1500
			SVC	720	1500	2000	400	1500
				360	515	2000	400	1500

Media cascading

You can use the standalone Media Server or the low cost server as a cascading media server.

The following table provides the performance specifications of a low cost server that is used as a media cascading server:

Table 14: Performance specifications of a low cost server used as a media cascading server

Server	Codec			Pixels (p) x 30fps	Bandwidth usage (kbps)	Active sessions
	Audio	Video				
Low cost server used as a media cascading server for audio and video streams **Note:** The final capacity of the low cost server for media cascading depends on the number of media cascading sites and the number of users in each conference and might be lower than the capacities provided in this table.	G.711	—	—	—	—	850
	G.722	—	—	—	—	700
	G.729	—	—	—	—	475
	G.711	H.264	AVC	720	1200	350
				360	420	450
			SVC	720	1500	350
				360	515	450
	G.722	H.264	AVC	720	1200	300
				360	420	400
			SVC	720	1500	300
				360	515	400
	G.729	H.264	AVC	720	1200	200
				360	420	275
			SVC	720	1500	200
				360	515	275

For the performance specifications of a standalone Media Server that is deployed as a cascading media server, click *Standalone Media Server in the Related topics section.*

Related topics:

Standalone Media Server on page 38

Flash Media Gateway

The following table provides the performance specifications of a standalone Flash Media Gateway.

Table 15: Performance specifications of a standalone Flash Media Gateway

Server	Protocol	Pixels (p) x 30 fps	Maximum Audio/ Video in Collaboration Agent sessions
Standalone Flash Media Gateway • Flash Media Gateway supports a maximum of 250 Audio/Video in Collaboration Agent sessions for each conference. • Avaya Aura® Conferencing supports a maximum of four Flash Media Gateways. **Note:** • For the best user experience of the Audio/ Video in Collaboration Agent feature, administer a maximum of four Flash Media Gateways using the RTMPS protocol at a 360p x 30fps resolution. With this configuration, you can have a total of 1600 active sessions simultaneously. • If you want external users to join a conference using the Audio/Video in Collaboration Agent feature, you must deploy Flash Media Gateway in the enterprise DMZ. • You can use the Audio/Video in Collaboration Agent feature in the audio-only mode. The performance specifications of the audio-only mode are the same as the specifications for the audio and video at 180p x 30fps resolution mode.	RTMP	720	300
		360	700
		180	850
	RTMPT	720	225
		360	525
		180	625
	RTMPS	720	180
		360	400
		180	500

Server components

The following tables list the software components that are resident on each of the servers according to deployment type.

Table 16: Co-resident with redundancy and co-resident simplex

Deployment type	Server	Description
Co-resident with redundancy For more information, see figure Figure 1: Co-resident with redundancy layout on page 52.	Element Manager Server 1 (EMServer1)	**Avaya Aura® Conferencing software:** • primary database Network Element • EM_0: Element Manager is responsible for Application Server configuration and Network Element tasks • PROV1: Provisioning Manager Network Element is responsible for provisioning conference service and subscriber data • AM1_0: Accounting Manager Network Element • AS1_0: Application Server Network Element • WCMS1: Web Conferencing Management Server Network Element • WCS1: Web Conferencing Server Network Element **Avaya Media Server software:** • Avaya Media Server platform - MS1: A Media Server Network Element that is deployed on the Avaya Media Server platform
	Element Manager Server 2 (EMServer2)	**Avaya Aura® Conferencing software:** • secondary database Network Element • EM_1: Element Manager is responsible for Application Server configuration and Network Element tasks

Comments? infodev@avaya.com

Deployment type	Server	Description
		• PROV2: Provisioning Manager Network Element is responsible for provisioning conference service and subscriber data • AM1_1: Accounting Manager Network Element • AS1_1: Application Server Network Element • WCMS2: Web Conferencing Management Server Network Element • WCS2: Web Conferencing Server Network Element **Avaya Media Server software:** • Avaya Media Server platform - MS2: A Media Server Network Element that is deployed on the Avaya Media Server platform
Co-resident simplex For more information, see figure Figure 3: Co-resident simplex layout on page 55.	Element Manager Server 1 (EMServer1)	**Avaya Aura® Conferencing software:** • primary database Network Element • EM_0: Element Manager is responsible for Application Server configuration and Network Element tasks • PROV1: Provisioning Manager Network Element is responsible for provisioning conference service and subscriber data • AM1_0: Accounting Manager Network Element • AS1_0: Application Server Network Element

Deployment type	Server	Description
		• WCMS1: Web Conferencing Management Server Network Element • WCS1: Web Conferencing Server Network Element **Avaya Media Server software:** • Avaya Media Server - MS1: A Media Server Network Element that is deployed on the Avaya Media Server platform

Table 17: Standalone with redundancy and standalone simplex

Deployment type	Server	Description
Standalone with redundancy For more information, see figure Figure 5: Standalone with redundancy layout on page 59.	Element Manager Server 1 (EMServer1)	**Avaya Aura® Conferencing software:** • primary database Network Element • EM_0: Element Manager is responsible for Application Server configuration and Network Element tasks • PROV1: Provisioning Manager Network Element is responsible for provisioning conference service and subscriber data • AM1_0: Accounting Manager Network Element • AS1_0: Application Server Network Element
	Element Manager Server 2 (EMServer2)	**Avaya Aura® Conferencing software:** • secondary database Network Element • EM_1: Element Manager is responsible for Application

Deployment type	Server	Description
		Server configuration and Network Element tasks • PROV2: Provisioning Manager Network Element is responsible for provisioning conference service and subscriber data • AM1_1: Accounting Manager Network Element • AS1_1: Application Server Network Element
	Web Conferencing Server 1 (WCServer1)	**Avaya Aura® Conferencing software:** • PA1: Personal Agent Network Element • WCMS1: Web Conferencing Management Server Network Element • WCS1: Web Conferencing Server Network Element
	Web Conferencing Server 2 (WCServer2)	**Avaya Aura® Conferencing software:** • PA2: Personal Agent Network Element • WCMS2: Web Conferencing Management Server Network Element • WCS2: Web Conferencing Server Network Element
	Avaya Media Server (MS1)	**Avaya Media Server platform:** • MS1: A Media Server Network Element that is deployed on the Avaya Media Server platform
Standalone simplex For more information, see figure Figure 6: Standalone	Element Manager Server 1 (EMServer1)	**Avaya Aura® Conferencing software:**

Deployment type	Server	Description
simplex layout on page 61.		• primary database Network Element • EM_0: Element Manager is responsible for Application Server configuration and Network Element tasks • PROV1: Provisioning Manager Network Element is responsible for provisioning conference service and subscriber data • AM1_0: Accounting Manager Network Element • AS1_0: Application Server Network Element
	Web Conferencing Server 1 (WCServer1)	**Avaya Aura® Conferencing software:** • PA1: Personal Agent Network Element • WCMS1: Web Conferencing Management Server Network Element • WCS1: Web Conferencing Server Network Element
	Avaya Media Server (MS1)	**Avaya Media Server platform:** • MS1: A Media Server Network Element that is deployed on the Avaya Media Server platform

Table 18: Co-resident with redundancy with DMZ and co-resident simplex with DMZ

Deployment type	Server	Description
Co-resident with redundancy For more information, see figure .	Element Manager Server 1 (EMServer1)	**Avaya Aura® Conferencing software:** • primary database Network Element • EM_0: Element Manager is responsible for Application

Deployment type	Server	Description
		Server configuration and Network Element tasks • PROV1: Provisioning Manager Network Element is responsible for provisioning conference service and subscriber data • AM1_0: Accounting Manager Network Element • AS1_0: Application Server Network Element • WCMS1: Web Conferencing Management Server Network Element **Avaya Media Server platform:** • MS1: A Media Server Network Element that is deployed on the Avaya Media Server platform
	Web Conferencing Server 1 (WCServer1)	**Avaya Aura® Conferencing software:** • PA1: Personal Agent Network Element • WCS1: Web Conferencing Server Network Element
	Element Manager Server 2 (EMServer2)	**Avaya Aura® Conferencing software:** • secondary database Network Element • EM_1: Element Manager is responsible for Application Server configuration and Network Element tasks • PROV2: Provisioning Manager Network Element is responsible for provisioning conference service and subscriber data

Deployment type	Server	Description
		• AM1_1: Accounting Manager Network Element • AS1_1: Application Server Network Element • WCMS2: Web Conferencing Management Server Network Element **Avaya Media Server software:** • Avaya Media Server platform • MS2: A Media Server Network Element that is deployed on the Avaya Media Server platform
	Web Conferencing Server 2 (WCServer2)	**Avaya Aura® Conferencing software:** • PA2: Personal Agent Network Element • WCS2: Web Conferencing Server Network Element
Co-resident simplex For more information, see figure Figure 6: Standalone simplex layout on page 61.	Element Manager Server 1 (EMServer1)	**Avaya Aura® Conferencing software:** • primary database Network Element • EM_0: Element Manager is responsible for Application Server configuration and Network Element tasks • PROV1: Provisioning Manager Network Element is responsible for provisioning conference service and subscriber data • AM1_0: Accounting Manager Network Element • AS1_0: Application Server Network Element • WCMS1: Web Conferencing

Deployment type	Server	Description
		Management Server Network Element **Avaya Media Server software:** • Avaya Media Server platform • MS1: A Media Server Network Element that is deployed on the Avaya Media Server platform
	Web Conferencing Server 1 (WCServer1)	**Avaya Aura® Conferencing software:** • PA1: Personal Agent Network Element • WCS1: Web Conferencing Server Network Element

Note:

The Personal Agent Network Element includes the Personal Agent Manager. The Personal Agent Manager also includes the Collaboration Agent application in addition to other applications. Use the Avaya Aura® Conferencing Collaboration Agent to join a conference by clicking the provided Collaboration Agent URL and entering authentication credentials. Collaboration Agent connects with the Collaboration Agent application which connects to the Personal Agent Manager and therefore connects to the Personal Agent Network Element through a single connection.

Co-resident with redundancy layout

The co-resident with redundancy layout is required for small scale deployments where redundancy is required.

The following figure shows the hosted components by server type:

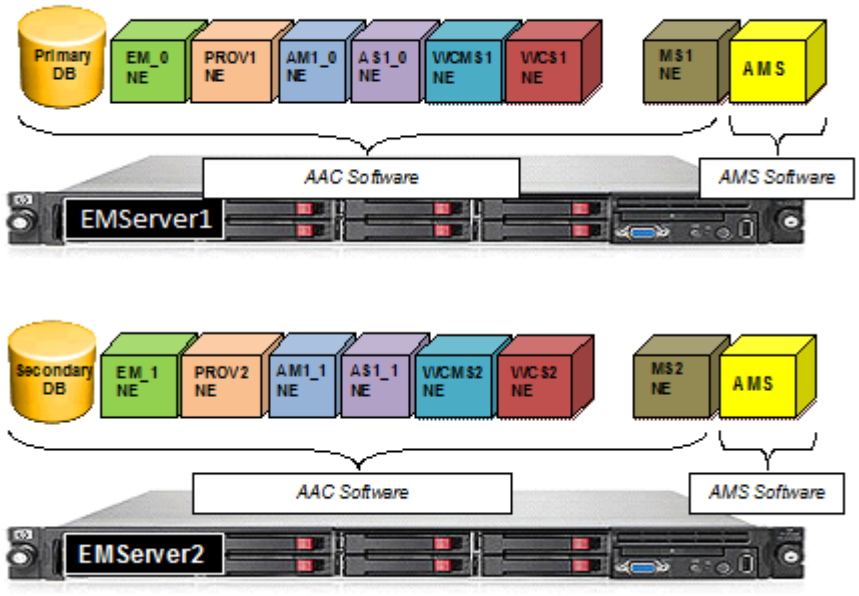


Figure 1: Co-resident with redundancy layout

Related topics:

System requirements for a co-resident with redundancy layout on page 52

System requirements for a co-resident with redundancy layout

Avaya Aura® Conferencing supports the HP DL360 G7 server.

The following table provides the system requirements for a co-resident with redundancy layout:

Table 19: System requirements for a co-resident with redundancy layout

Avaya Aura® Conferencing Application Server co-resident with Avaya Media Server, Web Conferencing Server, Web Conferencing Management Server, Collaboration Agent	Document Conversion Server for Web Conferencing
HP DL360 G7: • 1U chassis • 2.93 GHz dual Hex processor • 36 GB RAM	HP DL360 G7: • 1U chassis • 2.4 GHz dual quad processor • 6 GB RAM • 2 x 300 GB Hard Disk RAID 1 • Windows server 2003/2008 • Microsoft Office 2010/2013

Avaya Aura® Conferencing Application Server co-resident with Avaya Media Server, Web Conferencing Server, Web Conferencing Management Server, Collaboration Agent	Document Conversion Server for Web Conferencing
• 2 x 300 GB Hard Disk RAID 1 • 2 x 900 GB Hard Disk RAID 1	For repurposing only: Dell PowerEdge R610 • 1U chassis • 2.93 GHz dual Hex processor • 24 GB RAM • 2 x 146 GB Hard Disk RAID 5 • Windows server 2003/2008 • Microsoft Office 2010/2013 For repurposing only: IBM S8800: • 1U chassis • 2.93 GHz dual quad core processor • 24 GB RAM • 5 x 146 GB Hard Disk RAID 1 • Windows server 2003/2008 • Microsoft Office 2010/2013

Co-resident with redundancy with DMZ layout

The co-resident with redundancy with DMZ layout is required for small scale deployments where redundancy is required.

The following figure shows the hosted components by server type:

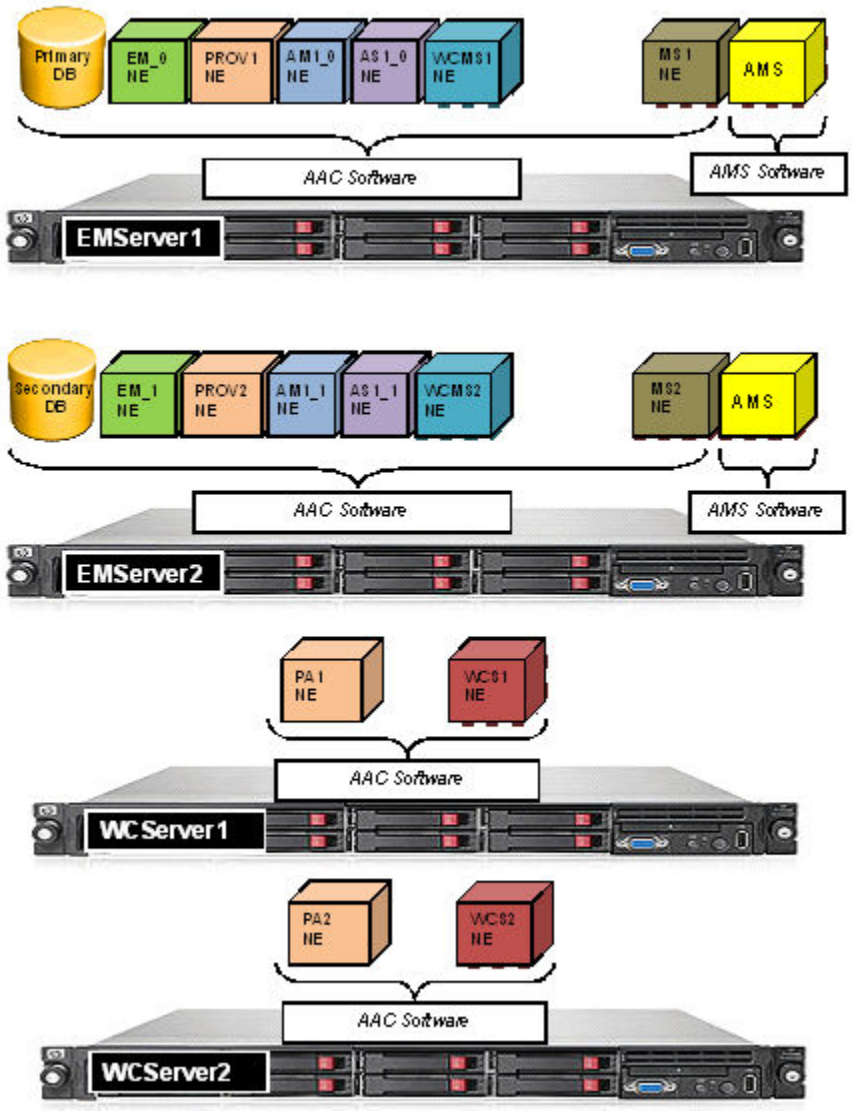


Figure 2: Co-resident with redundancy with DMZ layout

Related topics:

System requirements for a co-resident with redundancy with DMZ layout on page 54

System requirements for a co-resident with redundancy with DMZ layout

Avaya Aura® Conferencing supports the HP DL360 G7 server.

The following table provides the system requirements for a co-resident with redundancy with DMZ layout:

Table 20: System requirements for a co-resident with redundancy with DMZ layout

Avaya Aura® Conferencing Application Server co-resident with Avaya Media Server, Web Conferencing Management Server	Web Conferencing Server, Collaboration Agent	Document Conversion Server for Web Conferencing
HP DL360 G7: • 1U chassis • 2.93 GHz dual Hex processor • 36 GB RAM • 3 x 300 GB Hard Disk RAID 5	HP DL360 G7: • 1U chassis • 2.4 GHz dual quad processor • 6 GB RAM • 2 x 300 GB Hard Disk RAID 1	HP DL360 G7: • 1U chassis • 2.4 GHz dual quad processor • 6 GB RAM • 2 x 300 GB Hard Disk RAID 1 • Windows server 2003/2008 • Microsoft Office 2010/2013

Co-resident simplex layout

The co-resident simplex layout is required for small scale deployments where all application server components are located on a single server and redundancy is not required.

The following figure shows the hosted components by server type:

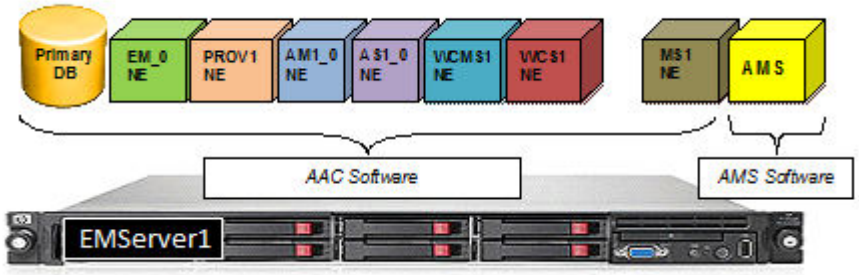


Figure 3: Co-resident simplex layout

Related topics:

System requirements for a co-resident simplex layout on page 56

System requirements for a co-resident simplex layout

Avaya Aura® Conferencing supports the HP DL360 G7 server for new installations and the Dell™ PowerEdge™ R610 or IBM S8800 for repurposing systems from Avaya Aura® Conferencing 6.0 or Meeting Exchange 5.2.

The following table provides the system requirements for a co-resident simplex layout:

Table 21: System requirements for a co-resident simplex layout

Avaya Aura® Conferencing co-resident Application Server, Avaya Media Server, Web Conferencing Server for Web Conferencing/Collaboration Agent	Document Conversion Server for Web Conferencing
HP DL360 G7: • 1U chassis • 2.93 GHz dual Hex processor • 36 GB RAM • 3 x 300 GB Hard Disk RAID 5 Dell™ PowerEdge™ R610: • 1U chassis • 2.93 GHz dual Hex processor • 24 GB RAM • 5 x 146 GB Hard Disk RAID 5 IBM S8800: • 1U chassis • 2.93 GHz dual quad core • 24 GB RAM • 5 x 146 GB Hard Disk	HP DL360 G7: • 1U chassis • 2.4 GHz dual quad processor • 6 GB RAM • 2 x 300 GB Hard Disk RAID 1 • Windows server 2003/2008 • Microsoft Office 2010

Co-resident simplex with DMZ layout

The co-resident simplex with DMZ layout is required for small scale deployments where all application server components are located on a single server and redundancy is not required.

The following figure shows the hosted components by server type:

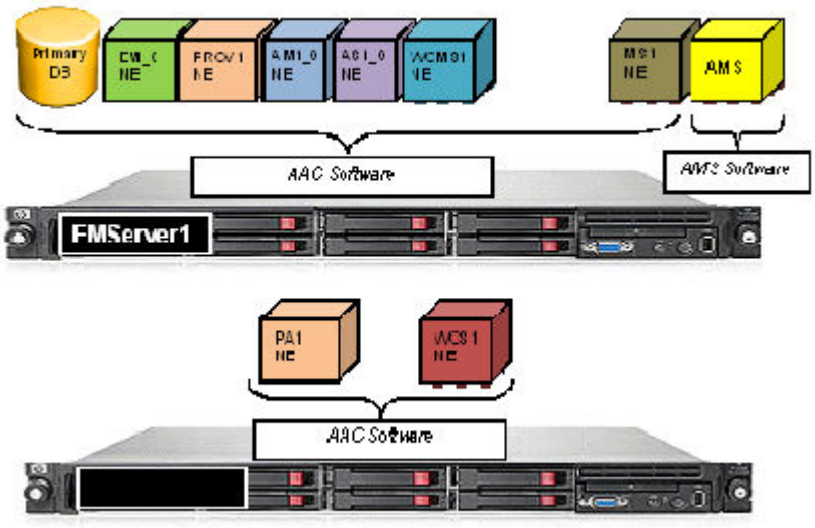


Figure 4: Co-resident simplex with DMZ layout

This figure shows the hosted components by server type for a co-resident simplex with DMZ layout configuration.

Related topics:

System requirements for a co-resident simplex with DMZ layout on page 57

System requirements for a co-resident simplex with DMZ layout

Avaya Aura® Conferencing supports the HP DL360 G7 server for new installations and the Dell™ PowerEdge™ R610 or IBM S8800 for repurposing systems from Avaya Aura® Conferencing 6.0 or Meeting Exchange 5.2.

The following table provides the system requirements for a co-resident simplex with DMZ layout:

Table 22: System requirements for a co-resident simplex with DMZ layout

Avaya Aura® Conferencing co-resident Application Server, Avaya Media Server, Web Conferencing Management Server	Web Conferencing Server, Collaboration Agent	Document Conversion Server for Web Conferencing
HP DL360 G7:	HP DL360 G7:	HP DL360 G7:

Avaya Aura® Conferencing co-resident Application Server, Avaya Media Server, Web Conferencing Management Server	Web Conferencing Server, Collaboration Agent	Document Conversion Server for Web Conferencing
• 1U chassis • 2.93 GHz dual Hex processor • 36 GB RAM • 3 x 300 GB Hard Disk RAID 5 Dell™ PowerEdge™ R610: • 1U chassis • 2.93 GHz dual Hex processor • 24 GB RAM • 5 x 146 GB Hard Disk RAID 5 IBM S8800: • 1U chassis • 2.93 GHz dual quad core • 24 GB RAM • 5 x 146 GB Hard Disk	• 1U chassis • 2.4 GHz dual quad processor • 6 GB RAM • 2 x 300 GB Hard Disk RAID 1	• 1U chassis • 2.4 GHz dual quad processor • 6 GB RAM • 2 x 300 GB Hard Disk RAID 1 • Windows server 2003/2008 • Microsoft Office 2010/2013

Standalone with redundancy layout

The standalone with redundancy layout configuration is required for medium to large scale deployments. Avaya Aura® Conferencing Standalone with redundancy layout is a configuration where a single pair of redundant Application Servers are dedicated for element management, database, application/service, and accounting functions. One server is dedicated to Avaya Media Server components. You can add more Avaya Media Servers and Web Conferencing Servers, if required. This layout configuration allows for system expansion beyond the basic layout.

The following figure shows the hosted components by server type:

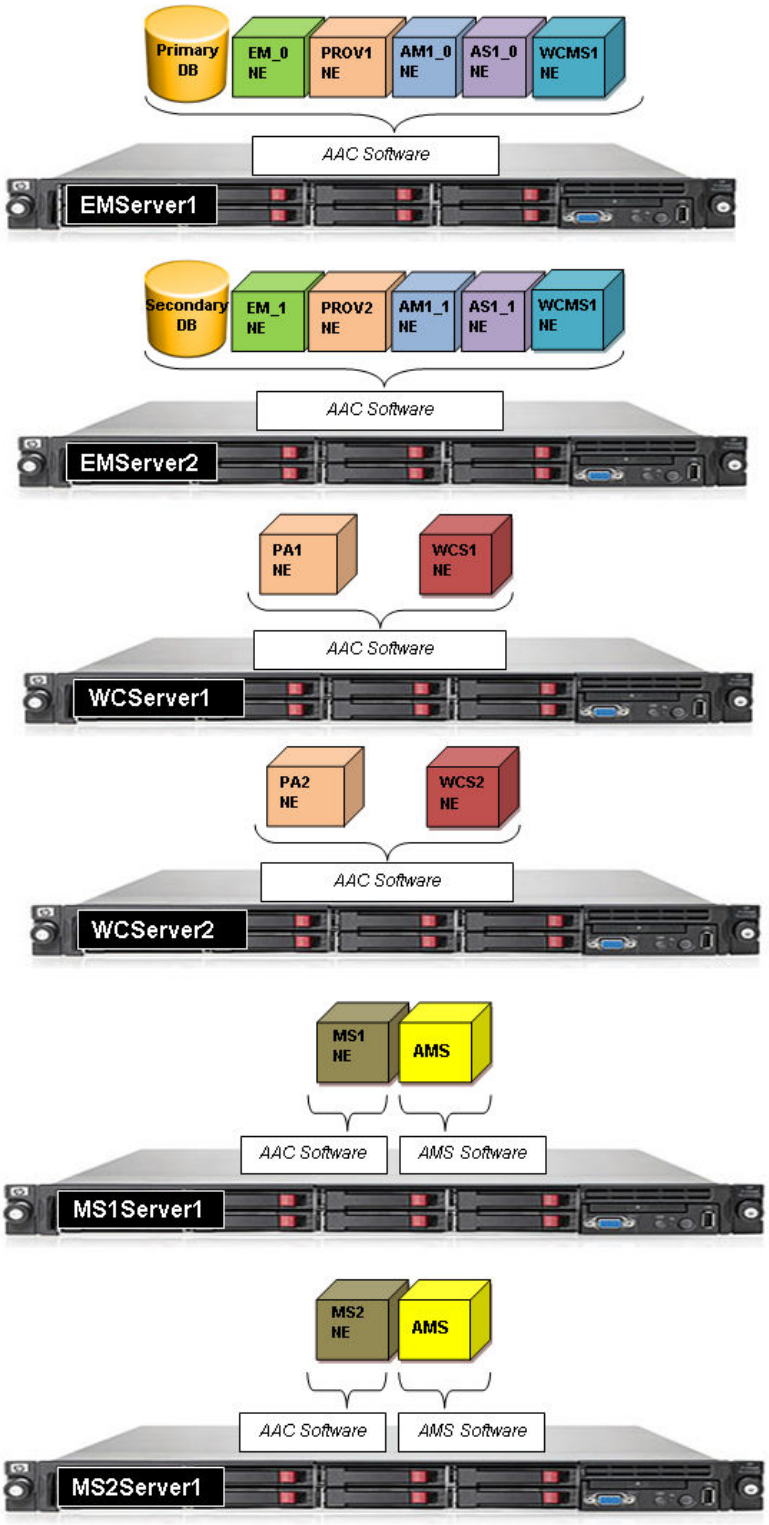


Figure 5: Standalone with redundancy layout

Related topics:

System requirements for a standalone with redundancy layout on page 60

System requirements for a standalone with redundancy layout

Avaya Aura® Conferencing supports the HP DL360 G7 server for new installations.

The following table provides the system requirements for a standalone with redundancy layout:

Table 23: System requirements for a standalone with redundancy layout

Avaya Aura® Conferencing Application Server – Redundant pair	Avaya Media Server	Web Conferencing Server for Web Conferencing/ Collaboration Agent	Document Conversion Server for Web Conferencing
HP DL360 G7: • 1U chassis • 2.4 GHz dual quad processor • 12 GB RAM • 2 x 300 GB Hard Disk RAID 1	HP DL360 G7: • 1U chassis • 2.93 GHz dual Hex processor • 12 GB RAM • 2 x 300 GB Hard Disk RAID 1 **Note:** Additional servers can be added for scaling/redundancy purposes.	HP DL360 G7: • 1U chassis • 2.93 GHz dual Hex processor • 12 GB RAM • 2 x 300 GB Hard Disk RAID 1 **Note:** Additional servers can be added for scaling/redundancy purposes.	HP DL360 G7: • 1U chassis • 2.4 GHz dual quad processor • 6 GB RAM • 2 x 300 GB Hard Disk RAID 1 • Windows server 2003/2008 • Microsoft Office 2010

Standalone simplex layout

The standalone simplex layout is required for medium to large scale deployments where all Application Server components are on a separate server to provide higher capacities and where redundancy is not required.

The following figure shows the hosted components by server type:

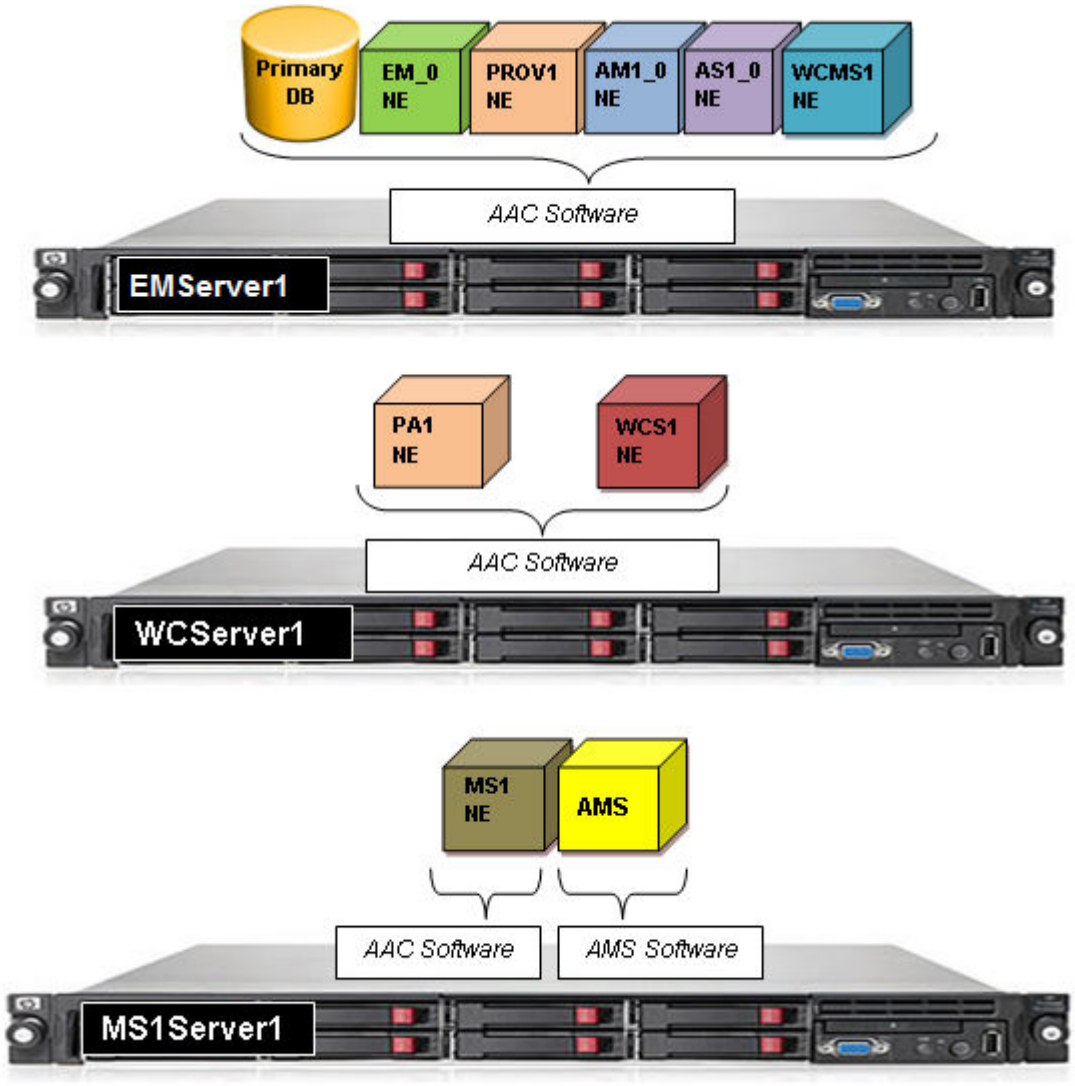


Figure 6: Standalone simplex layout

Related topics:

[System requirements for a standalone simplex layout](#) on page 61

System requirements for a standalone simplex layout

Avaya Aura® Conferencing supports the HP DL360 G7 server for new installations.

The following table provides the system requirements for a standalone simplex layout:

Table 24: System requirements for a standalone simplex layout

Avaya Aura® Conferencing Application Server	Avaya Media Server	Web Conferencing Server for Web Conferencing/ Collaboration Agent	Document Conversion Server for Web Conferencing
HP DL360 G7: • 1U chassis • 2.4 GHz dual quad processor • 12 GB RAM • 2 x 300 GB Hard Disk RAID 1	HP DL360 G7: • 1U chassis • 2.93 GHz dual Hex processor • 12 GB RAM • 2 x 300 GB Hard Disk RAID 1	HP DL360 G7: • 1U chassis • 2.93 GHz dual Hex processor • 12 GB RAM • 2 x 300 GB Hard Disk RAID 1	HP DL360 G7: • 1U chassis • 2.4 GHz dual quad processor • 6 GB RAM • 2 x 300 GB Hard Disk RAID 1 • Windows server 2003/2008 • Microsoft Office 2010 or 2013

Enterprise DMZ deployment

For standalone with redundancy and standalone simplex deployment configurations, you can deploy the Web conferencing server within the Enterprise DMZ of your network firewall. This allows you to connect to an Avaya Aura® Conferencing conference as a member or guest from outside the company firewall while still ensuring a strong and secure network defense. The moderator of a conference can also be located outside of the corporate firewall and still have access to most command functions. You also have the benefit of using Avaya Aura® Conferencing for off-site conferences and events.

Example

The following figure shows a basic DMZ configuration for a standalone with redundancy layout.

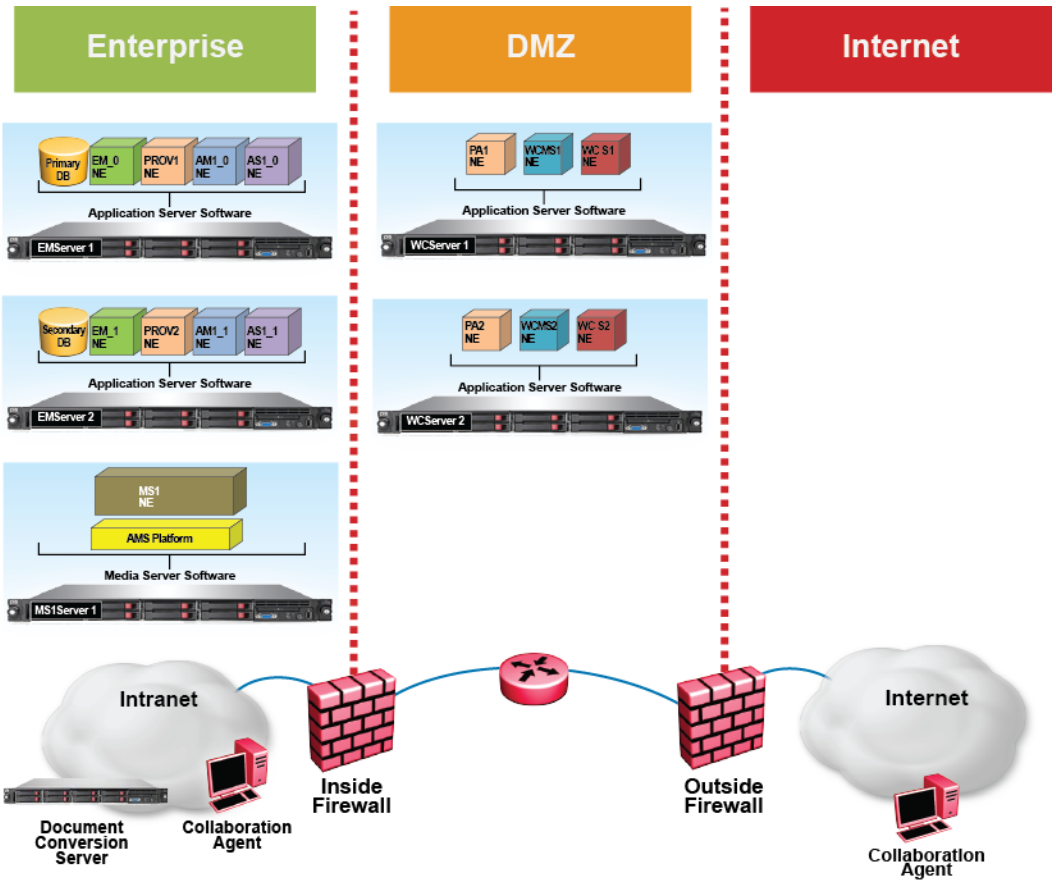


Figure 7: Basic DMZ configuration

In the preceding figure, the components required for interaction on both sides of the corporate firewall (the Personal Agent Manager, Web Conferencing Management Server, and the Web Conferencing Server) are located within the DMZ. These components require a small number of ports opened on the Enterprise and the Internet side, which has minimal firewall impact. With this configuration, conference members can connect to a conference outside of the corporate entity while continuing to maintain firewall integrity. The Document Conversion Server is located within the Enterprise side of the firewall and is fully protected; however, the Web Conferencing Server can still access and disperse the required documents.

Feature interactions

A moderator cannot upload documentation to the Document Conversion Server when outside the corporate firewall.

The following are some possible workarounds:

- the moderator can upload the required documents in advance of the offsite meeting while they are still within the corporate firewall
- the moderator can connect to the VPN outside of the firewall and upload the required documents

For information about the port matrix, go to http://support.avaya.com and download the latest version of the Avaya Aura® Conferencing 7.2 Port Matrix.

Related topics:

Migrating to and from a DMZ on page 186
Moving the Web Conferencing Management Server (WCMS) to the enterprise on page 433

Event conferencing

Event conferencing requires a dedicated Avaya Media Server and a dedicated Web Conferencing server. An event conference can support up to 2,000 active audio sessions per Avaya Media Server and 1,500 web sessions per Web Conferencing server. For example, you can host a single event conference with a maximum of 2,000 audio sessions and 1,500 web sessions using an Avaya Media Server and a Web Conferencing server, or you can host multiple event conferences with fewer participants simultaneously using an Avaya Media Server and a Web Conferencing server as long as the total number of audio sessions does not exceed the maximum of 2,000 and the total number of web sessions does not exceed 1,500.

You can add multiple Avaya Media Servers and Web Conferencing servers. However, a single event conference will still support a maximum of 2,000 audio sessions and 1,500 media.

You can also have multiple Avaya Media Servers in one location, enabling you to host multiple event conferences across multiple Avaya Media Servers in one location. In this scenario, once a conference starts on an Avaya Media Server, you are limited to the capacity of that Avaya Media Server. For example, if the first conference has 1,500 audio sessions, then the second conference that starts on that same Avaya Media Server will be limited to a maximum of 500 audio sessions.

The following table describes the capacities associated with event conferencing.

Table 25: Target capacities for Event conferencing

Servers (dedicated for Event conferencing)	Active audio sessions	Web sessions	Scalable by increasing the number of Event conferences only	Redundancy with an N+m configuration
Avaya Media Server	2,000 **Note:** Audio sessions are dedicated to a single server.	—	Yes **Note:** You can increase the number of simultaneous event	Yes

Servers (dedicated for Event conferencing)	Active audio sessions	Web sessions	Scalable by increasing the number of Event conferences only	Redundancy with an N+m configuration
			conferences by adding additional servers. However, each server supports a maximum of 2,000 audio sessions for all event conferences occurring on that server.	
Web Conferencing Server (primary and secondary)	—	1,500 **Note:** Web sessions are dedicated to a single server.	Yes **Note:** You can increase the number of simultaneous event conferences by adding additional servers.	Yes

Chapter 3: Network planning and design considerations

This chapter describes how to plan and design your network for use with Avaya Aura® Conferencing.

Network considerations

When engineering an Avaya Aura® Conferencing system in an IP network, there are a number of factors that must be taken into consideration. This section provides an overview of the supported Avaya Aura® Conferencing topologies and provides important factors to help create an optimized system design.

Conference usage patterns

Within an organization, conference usage patterns depend on many factors, such as the nature of work, communities of interest, and numerous other variables. Statistics gathered from existing conference solutions can be useful in predicting usage patterns with Avaya Aura® Conferencing.

Related topics:

Communities of interest on page 67
Avaya Media Server usage on page 68

Communities of interest

The communities of interest between different locations are an important factor when designing an optimal conferencing deployment. For example, a location where many participants are joining common conferences will benefit from a locally deployed Avaya Media Server.

Avaya Media Server usage

Several Avaya Media Servers can be deployed in a single cluster to support a required number of simultaneous participants. Gathering port usage statistics from an existing conference solution can be beneficial in engineering Avaya Aura® Conferencing. If the enterprise does not have an existing conferencing solution, consider one active user for every ten users to determine the Avaya Media Server usage.

For more information about the number of Avaya Media Servers required for a specific number of participants, see *Avaya Aura® Conferencing Overview and Specification*.

QoS

QoS provides the ability to configure differentiated services to a user, voice packets, and data packets. QoS guarantees quality to data flow.

To enable QoS, assign a QoS tag when you configure video. If a QoS tag is not assigned , the network uses its best effort for a video transmission.

Classifying users for QoS

Users can be classified as normal or priority users. To classify priority users, perform the following steps:

1. Set up a priority class of service (CoS) group.
2. Assign priority IP video to the priority CoS group.
3. Assign a user to the priority CoS group.
4. Assign a higher maximum call bit rate for priority IP multimedia.

For users of H.323 endpoints, you can set up separate bandwidth pools within a network region for priority video users.

Note:

This document does not include procedures on how to implement QoS.

DSCP tags

Tagging packets with DSCP tags ensures that, during network congestion, routers drop packets in the following order:

1. Data packets
2. Video packets

Comments? infodev@avaya.com

3. Audio packets of a video call
4. Audio packets of an audio call

The following table lists the recommended DSCP tags for the different types of packets:

Packet	DSCP tag
Audio	EF – DSCP 46: Expedited Fowarding: RFC-2598
Audio packets in video calls	AF41 – DSCP 34: Assured Forwarding: Class 4, Low Drop Precedence: RFC 2597
Video packets in video calls	AF42 – DSCP 36: Assured Forwarding: Class 4, Medium Drop Precedence: RFC 2597
Data	AF11 – DSCP 10: Assured Forwarding: Class 1, Low Drop Precedence

Bandwidth capacity

Network wide bandwidth management is performed in the Avaya Aura® architecture by a number of software components that manage bandwidth at various levels of granularity. Session Manager tracks all usage of audio and video bandwidth against the maximum capacity of each location and rejects any requests that exceed the maximum capacity. All bandwidth usage by clients and endpoints involved in multimedia applications that are provided Avaya Aura® Conferencing must first be allocated by the Session Manager so that overall network usage can be properly managed.

To provide a number of advanced capabilities that optimize bandwidth and provide priority-based quality control, Avaya Aura® Conferencing must manage bandwidth usage on an individual location basis and track the characteristics of individual sessions. These sessions are then modified to optimize multimedia sessions from a bandwidth perspective.

To achieve the granularity within Avaya Aura® Conferencing while ensuring overall bandwidth usage is controlled in the network, the Session Manager allows requests for bandwidth allocation updates on an individual location basis. Avaya Aura® Conferencing uses a SIP PUBLISH method to request an update to usage within a minimum/maximum range. Avaya Aura® Conferencing can determine through the Session Manager whether bandwidth can be allocated to allow new sessions or changes in media usage. To maintain an accurate accounting of audio and video bandwidth usage, these updates are requested by Avaya Aura® Conferencing at the start of each new session and then periodically throughout the session, if required.

The Session Manager interface used by Avaya Aura® Conferencing for bandwidth management is also used by other SIP entities that require management of local bandwidth

resources and the Avaya Communication Server 1000 when in an integrated site role in the network. This ensures the administrator for Session Manager has a complete view of the bandwidth usage of the network. Detailed scenarios of the Communication Manager and Avaya Communication Server 1000 are not covered in this document.

The following figure shows an architectural overview of the bandwidth management of Avaya Aura® Conferencing with call admission control (CAC).

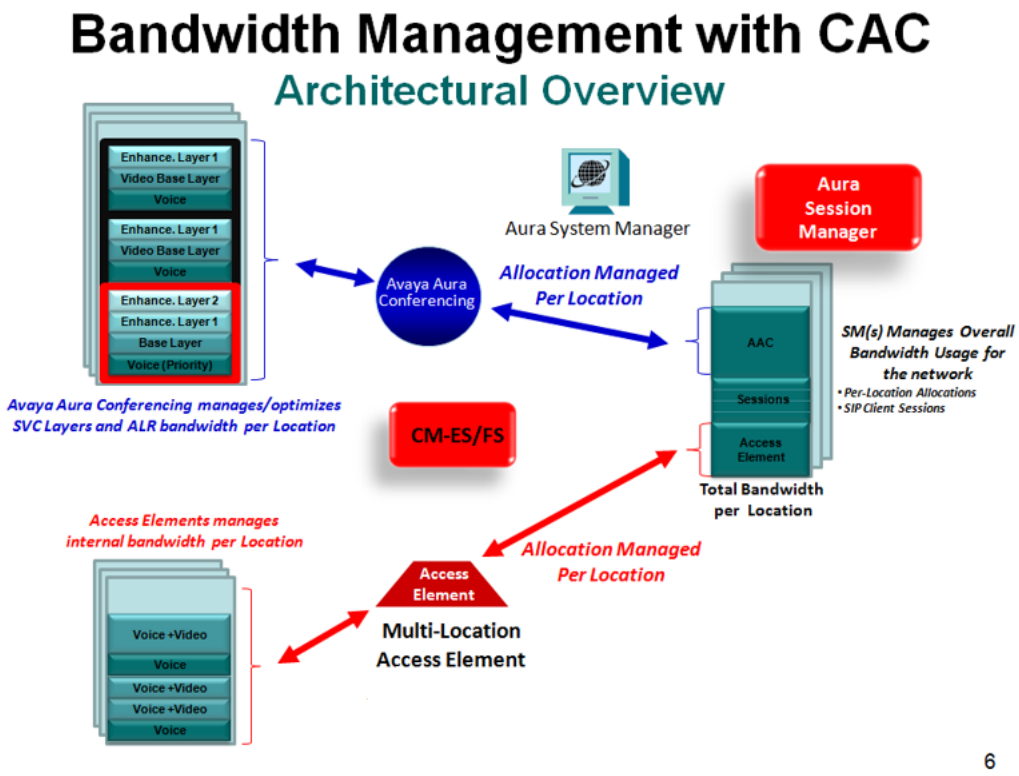


Figure 8: Bandwidth management with CAC

Related topics:

Event conferencing considerations on page 70

Event conferencing considerations

When considering the network deployment of Event conferencing resources, there are several factors that depend on the nature of the planned scenarios to be supported. These factors are specific to each situation as it occurs. For example, Event conferences that involve a large number of callers from the public require consideration for the point of entry into the network so that the required bandwidth capacities can be accommodated in the network. In this scenario, deployment of an Event conferencing Avaya Media Server that is collocated with

PSTN gateways or session border controls (SBC) would minimize the WAN bandwidth requirements to support the expected calling patterns.

Reliability can also be a key requirement for Event conferences due to the impact of a system failure. Avaya recommends that you place the Event conferencing resources within a highly reliable location.

Network impact on audio

As with all real time communications over an IP network, network delays must be managed to avoid user dissatisfaction with the provided audio quality. Generally, end-to-end delay between any two participants in a conference depends on the performance of the network and several other factors. The delays involved when participating in a conference include all network delays between the clients and servers in the media path between any two participants, as well as delays introduced in processing the media.

Effects of delay on audio quality

The following chart shows the impact of delay on quality as published in the ITU G.114 specification from “Mouth” to “Ear”. For example, all delays including the network, assuming no other impediments, such as packet loss, jitter, compression, and others.

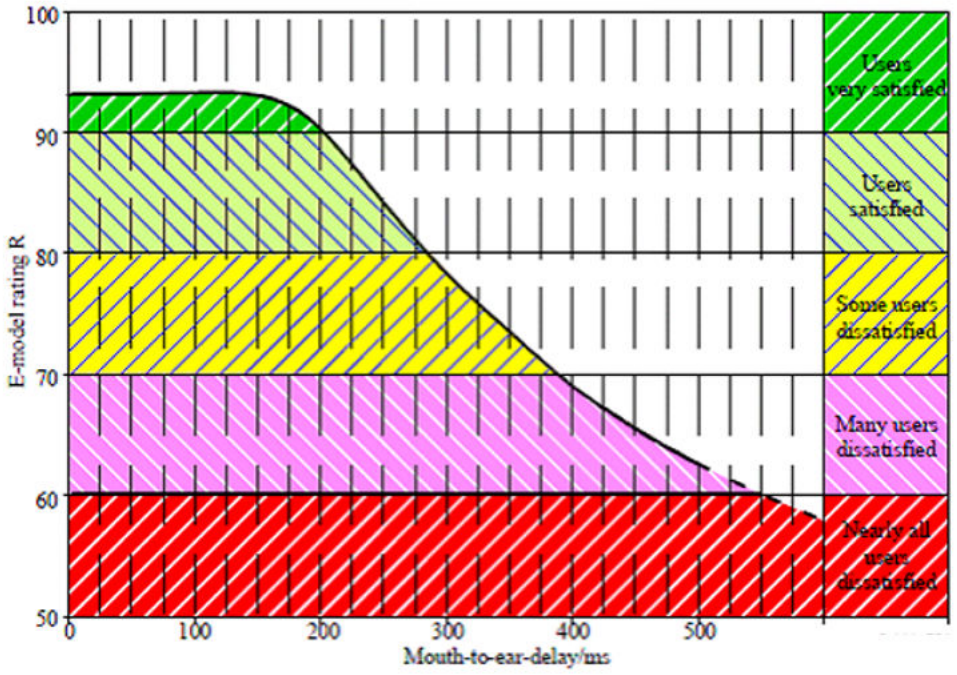


Figure 9: ITU G.114 Determination of the effects of absolute delay by the E-model

Related topics:

[Audio delays without media cascading](#) on page 72
[Audio delays with media cascading](#) on page 73

Audio delays without media cascading

If conferencing using centralized hosting without media cascading, the following figure shows the delays to consider.

Delays to consider:

- d1: Device delay to WAN
- d2: WAN delay to host
- d3: Avaya Media Server hosting delay
- d4: WAN delay to device
- d5: Device delay to ear

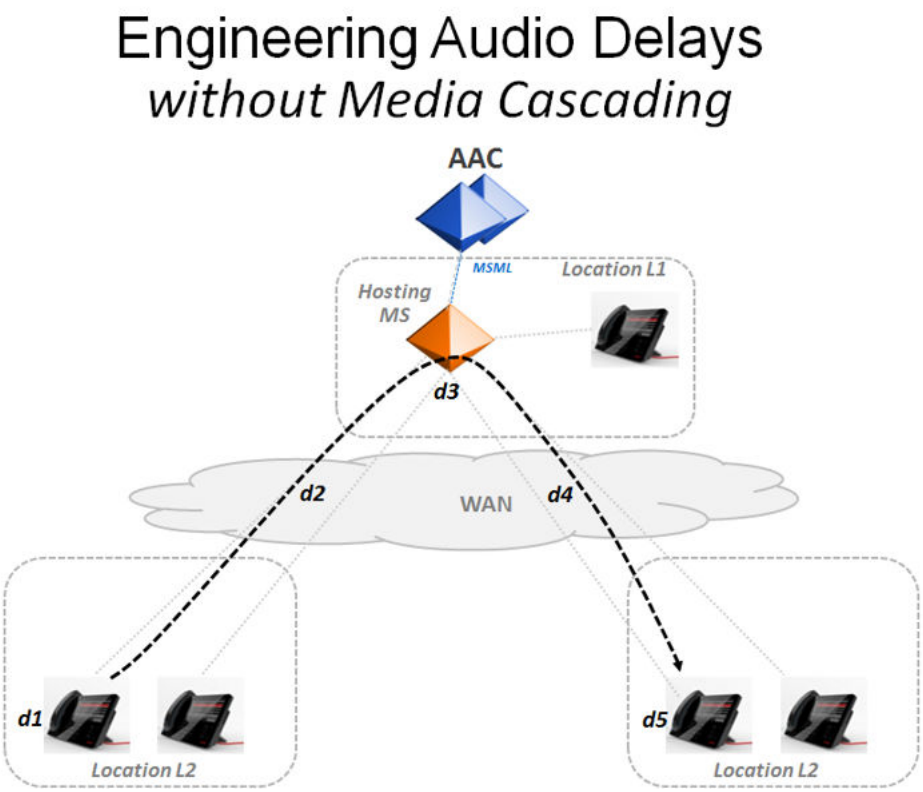


Figure 10: Engineering audio delays without media cascading

Audio delays with media cascading

Depending on location, media cascading can contribute to the delays between some participants. The following figure shows the delays to consider when media cascading is enabled.

Delays to consider:

- d1: Device delay to Avaya Media Server
- d2: Avaya Media Server delay to WAN
- d3: WAN delay to host
- d4: Avaya Media Server hosting delays
- d5: WAN delay to cascading location
- d6: Avaya Media Server delay to device
- d7: Device delay to ear.

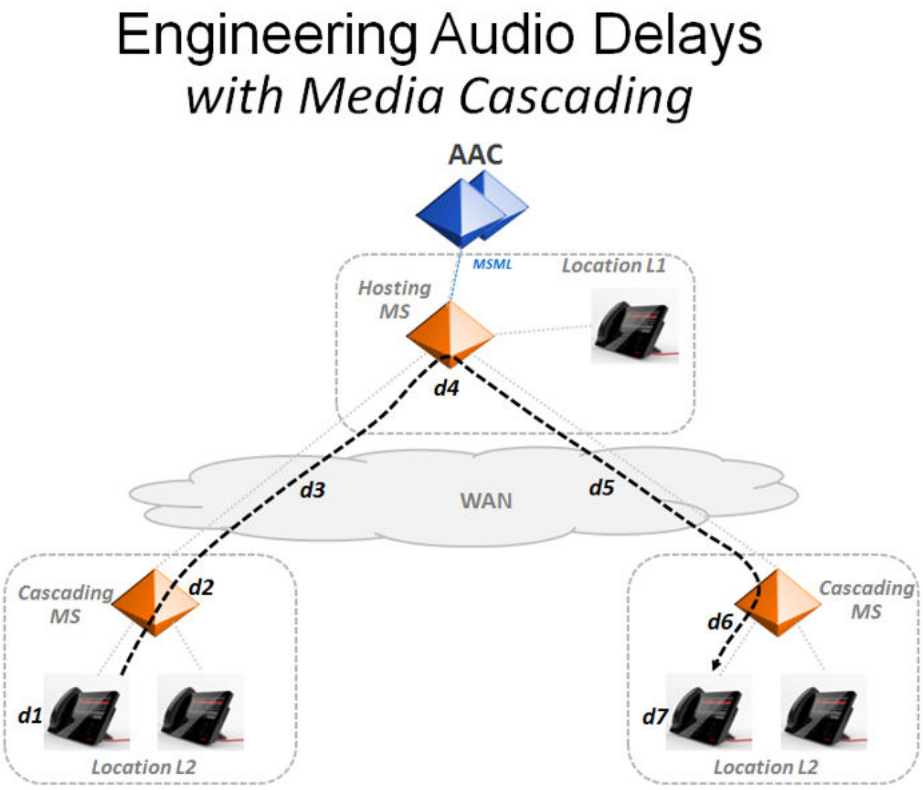


Figure 11: Engineering audio delays with media cascading

Note:

More complex media flows can involve delays from locations outside of the Enterprise network, such as PSTN gateways, VPN, and Internet. These delays are not shown in the preceding figures but must also be considered where applicable.

Network impact on video

Multiple network parameters affect the quality of video, such as the bit rate, the frame rate, the packet loss ratio, the content type, the compression method, jitter, and intra-frame coding. Each of these parameters might impact the quality of experience of a user.

VMOS

The VMOS method is based on objective and subjective parameters in real-time and uses an advanced measurement technology. The technology is based on network and video content and combines both the network impairment data and the video metrics to determine the video quality.

Packet loss

Packet loss is the ratio of packets lost in transit from the total packets transmitted. Packet loss severely impacts the video quality. A small ratio of packet loss might lead to a significant deterioration in quality. Multiple parameters, such as the codec type, the video format, and other codec characteristics, impact the ratio of packet loss and the duration of the impact. Unreliable networks and over-utilization of the available bandwidth also impacts the quality of video.

Packet loss after the intra-frame coding

The packet loss ratio after the intra-frame coding is determined from the point when the last intra-frame is received. When an intra-frame is received, the frame information is refreshed and the previous packet loss does not impact the video quality. However, packets lost after the intra-frame is received impacts the video quality.

Latency

The delay in the transmission of packets impacts the video quality, which deteriorates the user experience.

Bandwidth

The available bandwidth might impact the video quality, which depends on the codec, such as H.263 and H.264, and the video profile, such as QCIF, CIF, VGA, and HD.

For example, H.264 with CIF requires a minimum of 384 Kbps of available bandwidth while H.264 with 720p requires a minimum of 1.8 Mbps of bandwidth.

Jitter

Jitter impacts the video quality by causing variability in the latency. This variability impacts the flow of packets, which deteriorates the video quality.

Frame rate

The frame rate impacts the motion perception of a user. A high frame rate ensures good video quality. The frame rate can be from 10 to 60 fps.

Sharpness mode

The sharpness mode emphasizes the sharpness of video frames as the most significant parameter in the video quality evaluation. In this mode, blocky frames severely impact the video quality while the impact of uneven motion is reduced.

Motion mode

The motion mode emphasizes the motion perception as the most signification parameter in the video quality evaluation. In this mode, uneven motion severely impacts the video quality while the impact of blocky frames is reduced.

Recommended specifications

The following table lists the recommended values for the network parameters that impact the video quality:

Network parameter	Recommended value
One-way network delay	<= 80 ms to 180 ms
Network packet loss for video	<= 0.2 %
Latency	< 300 ms
Jitter	<= 20 ms
Frame rate	>= 26 fps
MOS	4 to 5

Service level agreements for audio queues

Avaya recommends that service level agreements be in place to ensure that the delay, jitter, and packet loss characteristics are predictable and managed.

Virtual Private Network location and bandwidth management

The Session Manager typically uses the IP address of a client during registration or the IP address of the media streams described within SIP signaling to determine the current location of a client. If using the Virtual Private Network (VPN) to access to the private network, the address allocated by the VPN infrastructure determines the location to be used for bandwidth management purposes.

The IP mapping to location defined within Session Manager reflects the data path that must be managed from a bandwidth management perspective. This ensures that any limitations in bandwidth at the point of entry to the enterprise network are managed appropriately and provide optimal use of cascading Media Servers within these locations.

Note:

The VPN infrastructure adds to the overall delays in media which negatively impacts the overall quality of audio.

Conference dial out

If dial out is enabled for the conference, the moderator can make a dial out call regardless of where the moderator is when joining the conference, for example, at the hosting location or at a cascaded location. The dial out call must be made from the hosting Avaya Media Server regardless of which Avaya Media Server the moderator is connected to. The called party joins the conference at that Avaya Media Server regardless of the called party's location. Therefore, media cascading does not apply to conference dial out calls.

Adhoc conferences

The optimization of media streams by media cascading is applicable only to MeetMe conferences. Adhoc conferences use the hosting Avaya Media Server without media cascading.

Network location information

Accurate information about the location of a participant is critical to bandwidth management, call admission control, and optimal selection of Avaya Media Server in a conference. Therefore, all locations within the network must be provisioned within the Session Manager and Avaya Aura® Conferencing. It is also critical that all sessions be associated with one of these locations, either through network address mapping within the Session Manager or by provisioning a SIP Entity Location field within the Session Manager. Sessions that cannot be associated with a location are blocked by Avaya Aura® Conferencing if bandwidth management is enabled because the bandwidth for these sessions cannot be managed within Avaya Aura® Conferencing. An alarm is produced when any blocking of this type occurs. The administrator can then detect, isolate, and repair the configuration of location information.

Voice activity detection and silence suppression

Audio silence detection and suppression (Voice Activity Detection/VAD) can be employed by endpoints that support this capability on audio media streams from client endpoints to the cascading Avaya Media Server. However, silence suppression cannot be performed by the Avaya Media Servers on outgoing audio streams to the client endpoints.

Cascading Avaya Media Server capacity

If a new participant of an existing conference cannot be accommodated by the capacity of an existing Cascading Avaya Media Server, the new session will block. For audio conferences, each server can support 2,000 or more participants before blocking (using G.729 codec capacity as an example). For video conferences, this limitation depends on the type of video being processed. This limitation is addressed by the scalable conference enhancement by adding another cascading Avaya Media Server if available, or if another cascading Avaya Media Server is not available, redirect the new session directly to the hosting Avaya Media Server.

Blocking due to cascading bandwidth capacity

If Media Cascading is enabled and adequate bandwidth is not available to establish an audio media stream between the cascading Avaya Media Server and the hosting Avaya Media Server, participation in the conference is blocked and an announcement provides information about how to join the conference. Users can retry the call if the bandwidth blocking is temporary or dial an alternative number to join the conference (if provided), such as a toll-free number that is always routed through the PSTN.

DTMF signaling by H.323 devices with Communication Manager

Dual tone multifrequency (DTMF) digits are used for conference identification or controls. If sending DTMF digits, the Communication Manager Media Server with indirect media is temporarily placed in the media path so it can provide DTMF signaling within the RTP stream. Bandwidth is temporarily allocated within the location of the Media Server to accommodate DTMF signaling. Avaya recommends that the Communication Manager Media Server, which provides the signaling, to be collocated with the H.323 devices, if possible, to minimize the possibility of blocking the signaling due to bandwidth restrictions.

Direct media with Communication Manager

Use the Direct Media option, if devices that are controlled by an Avaya Aura® Communication Manager participate in Avaya Aura® Conferencing conferences to minimize media path delay and network bandwidth utilization during certain scenarios.

Robustness and reliability

Application Server placement in the network is a critical factor in the overall reliability of the system. This section provides guidelines for server deployment.

Related topics:

Application server redundancy on page 79
Avaya Media Server redundancy on page 80
Web server redundancy on page 81

Application server redundancy

Avaya Aura® Conferencing supports redundancy. The redundancy option is necessary when reliability of services is critical, especially if a large number of users are dependent on these services. In addition to the redundancy option, application servers must be deployed at network locations with the following attributes:

- highly reliable access to the entire network
- adequate bandwidth capacities for signaling
- highly reliable access to primary and secondary Session Managers that provide session routing and shared bandwidth management interfaces to Avaya Aura® Conferencing

The application servers providing high availability (HA) must be connected within a layer 2 subnet to accommodate sharing of a virtual IP address.

The network design used to deploy application servers must avoid single points of failure in the networking components. For example, LAN switches used to connect redundant servers must also provide network redundancy, including items such as switches and power sources. See the following figure for a redundant network design. Capacity engineering of servers, such as Avaya Media Server, Web servers must consider the availability of resources in the event of any single networking component failure.

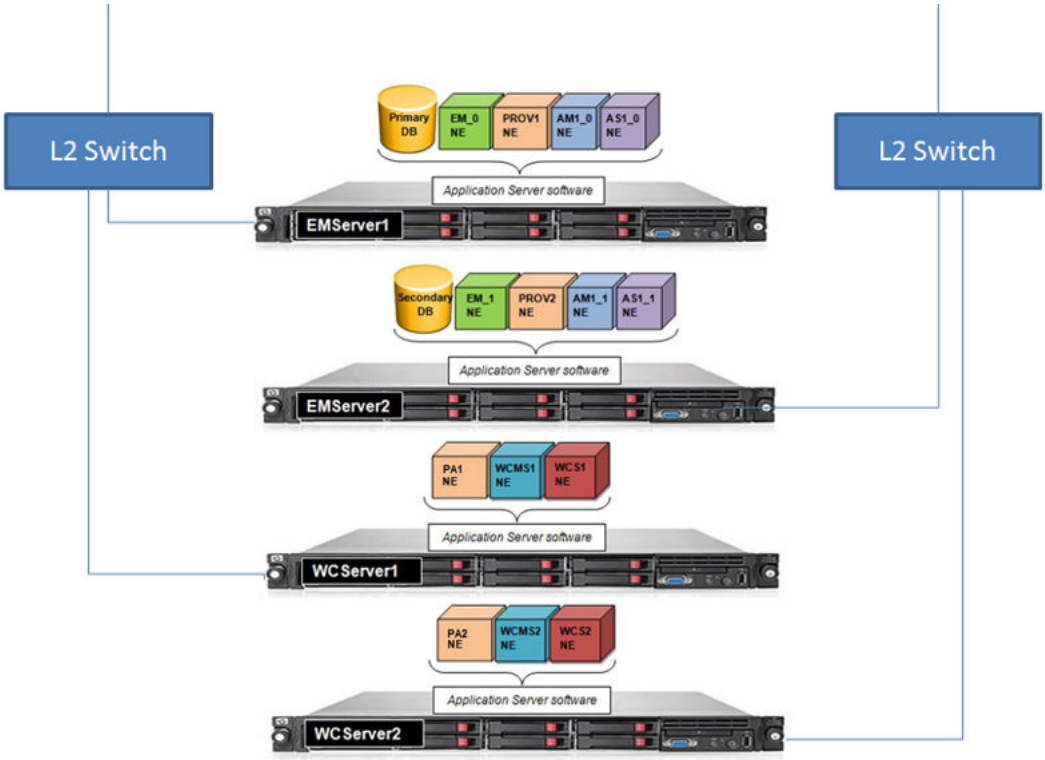


Figure 12: Redundant network design

In a redundant deployment, active sessions are retained when a failure occurs on the primary application server. After a five second detection time expires on the primary application server, the secondary application server detects the failure and takes over the active role within about one minute after the initial failure. During this recovery time period, users do not receive any feedback from the application server and any attempts to establish a new session fail.

Avaya Aura® Conferencing maintains interfaces with primary and secondary Session Managers for routing of SIP sessions and managing of network bandwidth. Upon loss of connectivity to the primary Session Manager, current sessions are lost and new sessions are routed to Avaya Aura® Conferencing using the secondary Session Manager. Bandwidth allocations for Avaya Aura® Conferencing are republished to the secondary Session Manager so that network bandwidth management can resume.

Avaya Media Server redundancy

Avaya Media Server deployment can provide several forms of redundancy that improve the reliability of services in the network.

Related topics:

Hosting locations on page 81

Cascading locations on page 81
Locations with Media cascading on page 81

Hosting locations

Multiple Avaya Media Servers can be placed in a cluster to provide n+1 load-sharing redundancy of Avaya Media Servers used for hosting conferences. In the event of a Media Server failure, existing sessions in the conference currently hosted by the server are released and new sessions that arrive are allocated resources from the operational servers.

Cascading locations

Multiple cascading Avaya Media Servers can be placed in a cluster to provide n+1 load balanced redundancy for Media Servers. In the event of a failure of an Avaya Media Server, existing sessions using the failing cascading Avaya Media Server is released and new sessions are allocated resources from the operational servers.

Locations with Media cascading

Multiple Avaya Media Servers can be placed within a location using media cascading to provide additional capacity and reliability. In the event of a failure of an Avaya Media Server, the other servers within the cluster are used for the arrival of new sessions. You can use this approach in a location where there are a large number of users or when you need to continue to use media cascading after a server failure.

If a single Avaya Media Server is deployed at a location using media cascading, failure of the Avaya Media Server causes new sessions to be redirected to the hosting Avaya Media Server directly. If bandwidth management call admission control (CAC) is applied, new sessions can overflow to the PSTN when bandwidth is not adequate for the session to proceed over the IP network.

Note:

This assumes the Avaya Aura® network is provisioned to provide this behavior.

Web server redundancy

The Web server supports redundancy options that are used when reliability of n+1 services is critical, especially if a large number of users are dependent on these services. In addition to

the using high availability (HA) options, application servers must be deployed at network locations with the following attributes:

- highly reliable access to the entire network
- adequate bandwidth capacities for signaling

The HA options for the Web server are defined based on the network elements running on them. The Web conferencing server on the failed unit are dropped. After the user reconnects, the application server directs them to an active Web conferencing server, assuming there is enough capacity on the remaining active units.

The Web conferencing management server network element supports an active-backup redundancy, and is deployed in a 1+1 configuration. During a failure, all active library sharing sessions stop working; however, you can restart the sharing and the Web conferencing server automatically switches over to the backup Web conferencing management server.

The Collaboration Agent network element supports an active-active redundancy, and is deployed in an n+1 configuration to maintain the desired capacity in the event of a failure. During a failure, any active sessions being hosted on the failed unit are dropped. If the user reconnects, the load balancer directs them to an active Collaboration Agent manager, assuming that there is enough capacity on the remaining active units.

To avoid a single point of failure, deploy the load balancer in a redundant model. Most load balancers support an active-backup redundancy and are deployed in a 1+1 configuration. To review the supported redundancy models, see your respective load balancer documentation. For more information about configuring a load balancer, see the document for *Deploying Avaya Aura® Conferencing*.

Avaya Media Server deployment for bandwidth optimization

The optimal deployment topology for Avaya Media Servers in a conference depends upon the factors described in Network considerations on page 67. In general, Avaya Aura® Conferencing determines the optimal media path for all video and audio streams involved in conferences, if the location of participating endpoints and the location of the Avaya Media Servers is known. Avaya Aura® Conferencing sets up the appropriate media streams that flow between clients and the Avaya Media Servers and between the hosting/cascading Avaya Media Servers . These media paths require WAN bandwidth to be allocated at all involved locations for each media path involved prior to setting up the media streams.

You can calculate the WAN bandwidth requirements for various deployment models within a network so that the optimal placement of servers and Media Server roles can be identified.

Related topics:

Estimating WAN bandwidth usage on page 83
Hosting locations without media cascading on page 86
Locations without Avaya Media Server on page 87
Estimating bandwidth reductions due to media cascading on page 87
Conference size and media stream bandwidth on page 88
Non-hosting locations with media cascading on page 92
Hosting locations with media cascading on page 92
Multiple hosting locations with media cascading on page 93
Delay engineering guidelines on page 93
Minimizing overall delays with packet time selection on page 96

Estimating WAN bandwidth usage

The amount of bandwidth required to support participants at a location depends on the deployment model used to provide conference services. The bandwidth required to support conferencing cannot be precisely calculated due to variable factors that can change the calling patterns at any time. However, there are some techniques, as described in the following paragraphs to help determine an estimate for bandwidth requirements.

The distributed Avaya Media Server architecture of Avaya Aura® Conferencing creates a number of location scenarios, depending on where conferences are hosted for the location and whether media cascading is enabled. These location scenarios include:

Table 26: Location scenarios

Location	Scenario
L1	Hosting locations without media cascading
L2	Locations without Avaya Media Servers
L3	Hosting locations with media cascading
L4	Non-hosting locations with cascading Avaya Media Servers.

For the preceding location scenarios, it is necessary to estimate the peak number of users that will be participating in conferences at each location. This information is used in the various location scenarios for Estimating peak participants by location on page 84 and Calculating WAN bandwidth requirements from peak media streams on page 85.

Related topics:

Estimating peak participants by location on page 84
Estimating WAN bandwidth requirements from audio streams on page 85
Estimating WAN bandwidth requirements from video streams on page 85

Estimating bandwidth requirements from Web conferencing on page 86

Estimating peak participants by location

The Erlang-B model can be used to estimate the number of media streams required to support the peak participants at each location, assuming an average usage for each provisioned user, for example, 0.1 Erlang and a probability of blocking, for example P=0.001, as shown in the following table. It is assumed that users are participating in audio conferencing at a rate of 0.1 Erlang, which is roughly equivalent to 10% of the time. For conferencing alone, this example uses a high usage rate and is for illustration purposes only. The actual average usage will be different than what is used in the example.

Table 27: Estimating peak participants by location

Location	Provisioned users	Erlang (0.1 per user)	Peak participants (P0001)	Peak WAN media streams
L1 (hosting)	5,000	500	555	0
L2 (without Media Server)	3,000	300	345	345
L3 (without Media Server)	500	50	64	64
L4 (without Media Server)	200	20	30	30
All locations hosted at L1	8,700	870	994	439

The following provides a description of the columns in the preceding table:

- Provisioned users. Shows the number of users that use the conferencing system from a location either directly over the network or through gateways deployed within that location.
- Erlang (0.1 per user). Shows the peak number of participants that is expected for a location given the total usage. This peak is determined by referencing a standard Erlang B traffic table assuming a specific probability of blocking (for example, P=0.001), which provides the number of channels required to support this level of usage. For example, at location L1, 555 media streams are required to support 500 Erlang of usage at a probability of P=0.001.
- Peak WAN media streams. Shows the peak number of media streams that travel over the WAN. In the centralized conferencing model, the example shows the media streams within the hosting location (L1) stay within this location and consume no WAN bandwidth. It assumes that any gateways involved in external calls, either by dialing into the conference or by dialing out from within a conference, are deployed within the hosting location. Because dialed-out participants are established with media streams from the

Comments? infodev@avaya.com

hosting Avaya Media Server either directly or through locally deployed gateways, dialed-out participants also remain within the location.

Estimating WAN bandwidth requirements from audio streams

After estimating the peak WAN media streams, the total audio bandwidth requirement can be calculated for the codecs being used. The bandwidth estimates for supported audio codecs are listed in the following table.

Table 28: Bandwidth usage (kbps)

Codec/Ptime	10 ms	20 ms	30 ms	60 ms
G.711	102	83	77	71
G.729	46	27	21	15
G.722	102	83	77	71

SIP clients that are capable of receiving Active Speaker notifications for conferences consume additional bandwidth within the audio media streams for this capability. Audio media streams used for media cascading always enable Active Speaker which results in the bandwidth estimates in the following table.

Table 29: Bandwidth usage (kbps) with active speaker

Codec/Ptime	10 ms	20 ms	30 ms	60 ms
G. 711	106	85	78	71
G.729	50	29	22	15
G.722	106	85	78	71

For example, using the preceding table, client audio streams using a G.722 codec with a 20 ms packet time without Active Speaker enabled consumes about 83 kbps of bandwidth, while audio media streams used for cascading using a G.722 codec with a 10 ms packet time and Active Speaker enabled consumes about 106 kbps of bandwidth.

Estimating WAN bandwidth requirements from video streams

The bandwidth usage of video streams varies widely. The bandwidth usage depends on various factors of an enterprise network, which include:

- Video codecs
- Types of video devices

- Video usage pattern of users
- Locations of users

The following table provides estimates of the bandwidth used by different codecs. These estimates will help you estimate the video bandwidth requirements:

Table 30: WAN bandwidth requirements from video streams

H.264 SVC	Profile-Level-ID	Level	Resolution	Cumulative layer Bitrate (kbps)	Independent layer bitrate (kbps)
Class C	42400D	1.3	320 x 180	128	128
	42401E	3.0	640 x 360	512	384
	42401F	3.1	1280 x 720	1536	1024
Class D	42401E	3.0	640 x 360	512	512
	42401F	3.1	1280 x 820	1536	1024

Estimating bandwidth requirements from Web conferencing

Web conferencing uses a reliable transport protocol and does not use the same network traffic class as audio and video. The bandwidth usage of Web conferencing varies widely. This bandwidth usage depends on various factors, which includes:

- Web conferencing usage pattern of users
- The timing rate of page sharing
- Document library or screen sharing usage pattern of users

Hosting locations without media cascading

If media cascading is not enabled for a hosting location, the WAN bandwidth usage is directly dependent on the number of users participating in the conference from locations other than the hosting location. Bandwidth within the location is assumed to be adequate and is not managed by theAvaya Aura® system.

To estimate the amount of WAN bandwidth required for users participating in conferences from locations other than the hosting location, see Table 27: Estimating peak participants by location on page 84. Using this table, the peak number of participants using WAN bandwidth at the hosting location (L1) is 439 (L2 + L3 + L4). For more information about calculating the WAN bandwidth requirements at the hosting location (L1) in this deployment model and for

the particular assumptions about codecs used, see the *Avaya Aura® Conferencing Product Overview and Specification* document.

For example, assuming that the G.722 audio codec uses a 20 ms packet time, the following calculation shows the amount of bandwidth required at hosting location L1:

L1: 439 X 83 kbp = 36,437 kbps WAN bandwidth.

Locations without Avaya Media Server

With a hosting Avaya Media Server that is centrally deployed, all participants that are not at the conference hosting location use WAN bandwidth for their media streams. The WAN bandwidth required for locations that do not have an Avaya Media Server locally deployed can be estimated by determining the peak number of conference participants expected at one time. This WAN bandwidth can be estimated by determining the peak number of users and calculate bandwidth requirements based on the codecs that are to be used. In the following example, locations L2, L3 and L4 have an estimated peak number of participants of 345, 64, and 30 respectively.

For example, assuming that the G.722 audio codec with a 20 ms packet time is used, the amount of bandwidth required at hosting location L1 is:

- L2: 345 X 83 kbps = 28,635 kbps WAN bandwidth
- L3: 64 X 83 kbps = 5,312 kbps WAN bandwidth
- L4: 30 X 83 kbps = 2,490 kbps WAN bandwidth

For more information about calculating WAN bandwidth requirements, see the *Avaya Aura® Conferencing Overview and Specification* document for the codecs to be used.

Estimating bandwidth reductions due to media cascading

Media cascading starts to provide benefits when two or more users are participating within a conference. The reduction in bandwidth is significantly higher for large conferences that have more participants sharing a common media stream over the WAN. For individual conferences, the reduction in bandwidth provided by media cascading depends on the number of participants in the conference. For example, conferences that have two participants from a location would have a 50% reduction in WAN media streams while conferences with three participants would have a 67% reduction in WAN media streams, and so on. The following table shows the reduction in media streams in a conference for various participant counts from a single location.

Participants from the same cascading location	Reduction in media streams (percentage)
2	50%
3	67%
4	75%
5	80%
6	83%
...	...
50	98%

If estimating the total WAN bandwidth requirements for a cascading location, you need an estimate for the total number of media streams that remain within the location. One method to estimate local traffic is to assume that conferencing has communication patterns that are similar to other call types with respect to communities of interest. For more information about estimating local traffic, see the *Avaya Aura Conferencing Overview and Specification* document. With this assumption, the number of conferences with at least two participants from the same location can be estimated by assuming that they are proportional to general intralocation (Intercom) usage.

Conference size and media stream bandwidth

Conferences that have more than two participants from a cascading location provide even more benefit in media cascading. Ideally, the average distribution of conference sizes is known and can be used to provide the most accurate estimate of expected bandwidth savings due to cascading.

The peak bandwidth capacity requirements for a WAN can influence the cost of a network significantly. A strategy that lowers the peak capacity of the network normally results in cost savings. Bandwidth capacity depends on the number of media streams that are in use during this peak period.

If estimating the conferencing peak bandwidth usage, it is helpful to look at the number of conferences by various sizes when performing analysis. The following figure provides an example of conference statistics showing the number of conferences by various conference sizes. In this example, the number of conferences that exceed four participants is 30 percent.

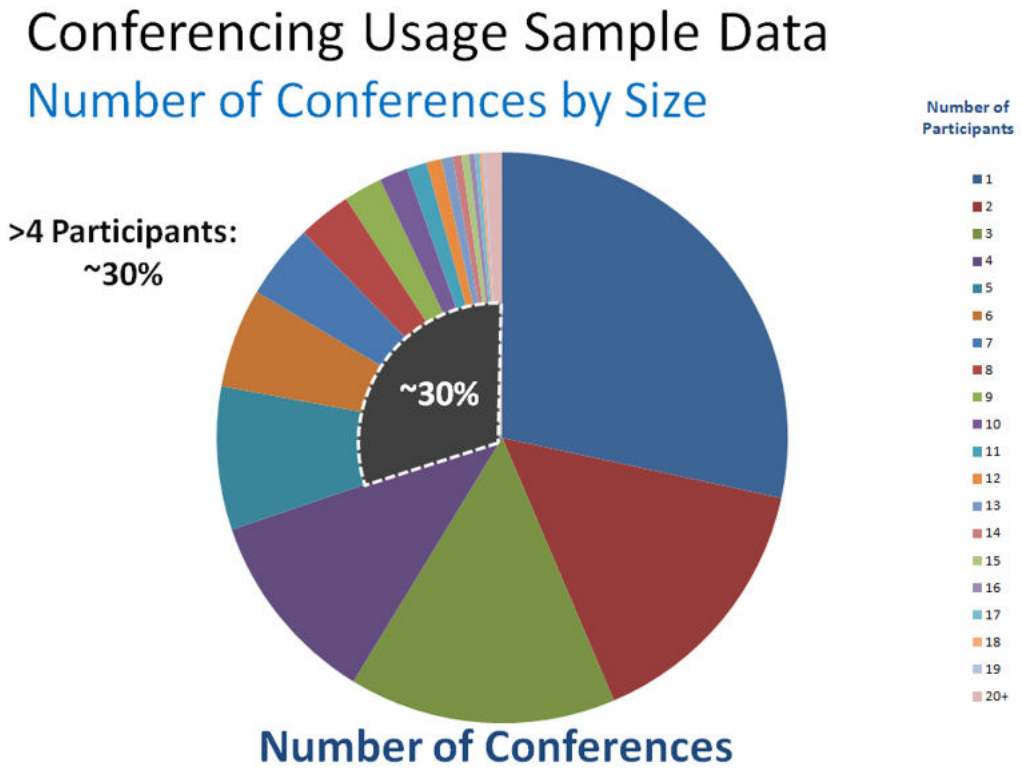


Figure 13: Conferencing usage sample data by number and size

In a centrally hosted conferencing topology, the peak bandwidth usage is not only dependent on the number of conferences but also on the total time spent by participants sending or receiving media streams in a conference. Using the same conferencing statistics when taking the total time of participation into consideration, the following figure shows the total participant time spent using bandwidth for media streams. Although there are many smaller conferences, the conferences that are larger than four participants consume about 78 percent of the bandwidth usage.

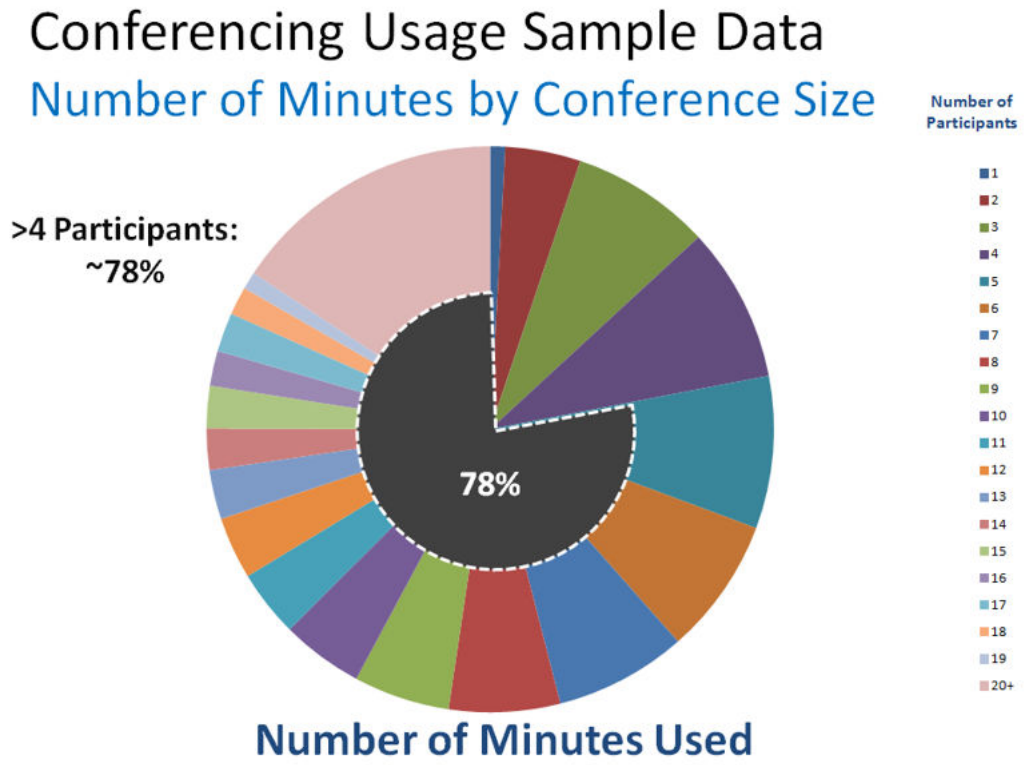


Figure 14: Conferencing usage sample data by size and number of minutes

An intralocation factor can be calculated based on the portion of communications that stays within a location. For example, assuming that intralocation (intercom) usage, inbound and outbound traffic for a site are estimated at 40, 30, and 30 Erlangs, respectively, the intralocation factor would be 40 percent. That is, 40 percent of the media streams would have at least two participants within a location.

Table 31: Reduction in client media streams due to media cascading

	Pro-visioned users	Erlang 0.1 per user	Peak Part-icipants (P001)	Peak WAN Media streams without cas-cading	Intra-locatio n factor	Intra-locatio n media stream s	Media stream s used for Intra-locatio n cas-cading	Total peak WAN media streams
Location L1 (hosting)	5,000	500	555	0	—	—	—	—
Location L2	3,000	300	345	345	40%	(138)	35	242

	Pro-visioned users	Erlang 0.1 per user	Peak Part-icipants (P001)	Peak WAN Media streams without cas-cading	Intra-locatio n factor	Intra-locatio n media streams	Media streams used for Intra-locatio n cas-cading	Total peak WAN media streams
(cas-cading)								
Location L3 (cas-cading)	500	50	64	64	40%	(26)	7	45
Location L4 (no Media Server)	200	20	30	30	—	—	—	30
All locations hosted at L1	8,700	870	994	439	—	(164)	42	317

In the preceding table, the reduction in client media streams due to media cascading is based on an average of four parties who are participating in each conference, providing an average of 75 percent reduction for intralocation media streams. The reduction can be significantly greater if larger conference sizes are expected during peak traffic periods.

The following provides a description of the columns in the preceding table (See Table 27: Estimating peak participants by location on page 84 for more column descriptions):

- Intralocation factor. Shows the portion of media flows that are expected to remain within a location. This is based on the communities of interest and calling patterns. This factor is used to estimate the number of media streams that benefit from media cascading within conferences. In this example, a factor of 40 percent is assumed.
- Intralocation media streams. Shows the number of media streams between participants within the same location. Calculate by multiplying the intralocation factor by the peak WAN media streams without cascading. For example, in location L2, the intralocation media streams is 40% X 345 = 138.
- Media streams used for intralocation cascading. Shows the number of media streams that are required to carry the intralocation media streams to the hosting Avaya Media Server over the WAN. It is calculated by applying an average media cascading savings for conferences, such as 75 percent, to the intralocation media streams. For example, in location L2, 138 media streams can be carried in 138 X 25% = 35 cascading media

streams. This is a savings of 103 media streams due to media cascading, that is 138 – 35 = 103.

- Total peak WAN media streams. Shows the total number of media streams that are required to carry all conference media over the WAN. This is calculated by adjusting the total number of media streams without cascading by the savings due to media cascading. For example, in location L2, the savings of 103 media streams reduces the total media streams over the WAN from 345 to 242, that is 345 – 103 = 242.

Assuming the audio codecs in the preceding table, the following calculations show the total bandwidth estimated for locations L1, L2, and L3:

- L1: 317 X 106 kbps = 33,602 kbps (hosting of L1, L3, and L4)
- L2: 242 X 106 kbps = 25,652 kbps
- L3: 45 X 106 kbps = 4,770 kbps

If the network delays are such that cascading media streams with 20 ms packet times can be used, for example, 85 kbps, the bandwidth is reduced further, as shown in the following calculations:

- L1: 317 X 85 kbps = 26,945 kbps
- L2: 242 X 85 kbps = 20,570 kbps
- L3: 45 X 85 kbps = 3,825 kbps

Non-hosting locations with media cascading

Locations with media cascading enabled that are not hosting conferences locally, benefit from the shared streams in situations where two or more participants are in the same conference. As shown in Table 31: Reduction in client media streams due to media cascading on page 90, the WAN bandwidth at the cascading location can be estimated by first determining the peak number of media streams expected and adjusting this estimate by the reduction of streams expected due to cascading at the cascading locations. Also, the peak WAN media streams for locations L2 and L3, after adjusting for media cascading, is estimated at 242 and 45, respectively.

Hosting locations with media cascading

If media cascading is enabled for locations that are hosted by a central location, WAN bandwidth is reduced at both the hosting location and the cascading location. As shown in Table 31: Reduction in client media streams due to media cascading on page 90, the WAN bandwidth at the hosting location can be estimated by first determining the peak number of media streams expected and adjusting this estimate by the reduction of streams expected due to cascading at all locations using that hosting location.

The hosting location L1 has a reduction in peak media streams of 122, which reflects the total reduction in peak media streams of cascading locations L2 and L3 from 439 to 317.

Multiple hosting locations with media cascading

An additional benefit of an Avaya Aura® Conferencing distributed Media Server architecture is the flexibility to select a hosting Avaya Media Server that is optimal for users within a location. You can then define multiple hosting locations to further optimize network resources. With this deployment model, conferences that include only participants from within the hosting location do not consume any WAN bandwidth.

For example, a conference call with three participants, including one caller using a PSTN gateway and two participants within the same location, does not require WAN bandwidth if the location is hosting the conference. There are many factors that influence the probability of local-only conferencing, including calling patterns and communities of interest, that prevents a general rule that covers engineering of all scenarios. However, if local conferencing can be estimated, the number of media streams used for cascading can be reduced by the number of local conferences for each hosting location.

Delay engineering guidelines

The end-to-end delay for media paths can have an effect on the audio quality of conference sessions. For more information, see Network considerations on page 67. Depending on the number of servers in the path, the Media Servers that handle the audio add to the overall delay in the media path. The following table provides a summary of the approximate delays introduced by Avaya Media Servers for direct and cascaded scenarios, assuming the use of a G.722 codec with 20 ms packet times by the participating clients:

Table 32: Direct or cascaded hosting delays

Direct or cascaded	Avaya Media Server (MS) packet times
Direct hosting: single Media Server	MS1: ~60 ms
One cascaded site (two Media Servers)	MS1: ~55 ms MS2: ~50 ms
Two cascading sites (three Media Servers)	MS1: ~55 ms MS2: ~45 ms MS3: ~50 ms

With a delay introduced within the communications devices, there are also delays caused by the network or Avaya Media Servers. In the following examples, the device delays are assumed to be approximately 70 ms including both clients involved in the media flow, which is characteristic of the Avaya 9600 series IP Deskphones using a G.722 codec with 20 msec

packet times. The delay introduced by other devices is dependent on the client implementation of a number of features, such as jitter buffer management, media handling algorithms, codec in use and packet times.In both figures, the 70 ms delay is shown as 30 ms at the transmitting client and 40 ms at the receiving device.

The following figure shows delay calculations for a media path without media cascading. The following calculation shows the overall delay after determining the values for each type of delay to be considered. A client codec G.722/G.711 is assumed with a packet time of 20 ms.

Delays to consider:

- d1: 30 ms
- d2: 30 ms (60 ms RTD)
- d3: 60 ms
- d4: 30 ms (60 ms RTD)
- d5: 40 ms
- Total 190 ms

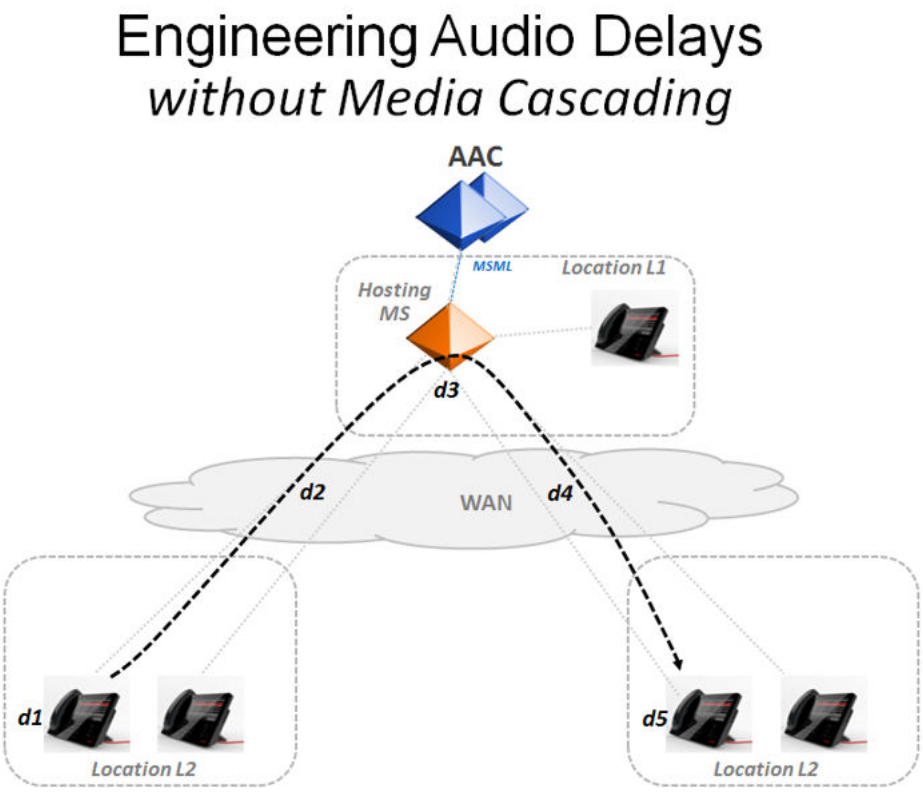
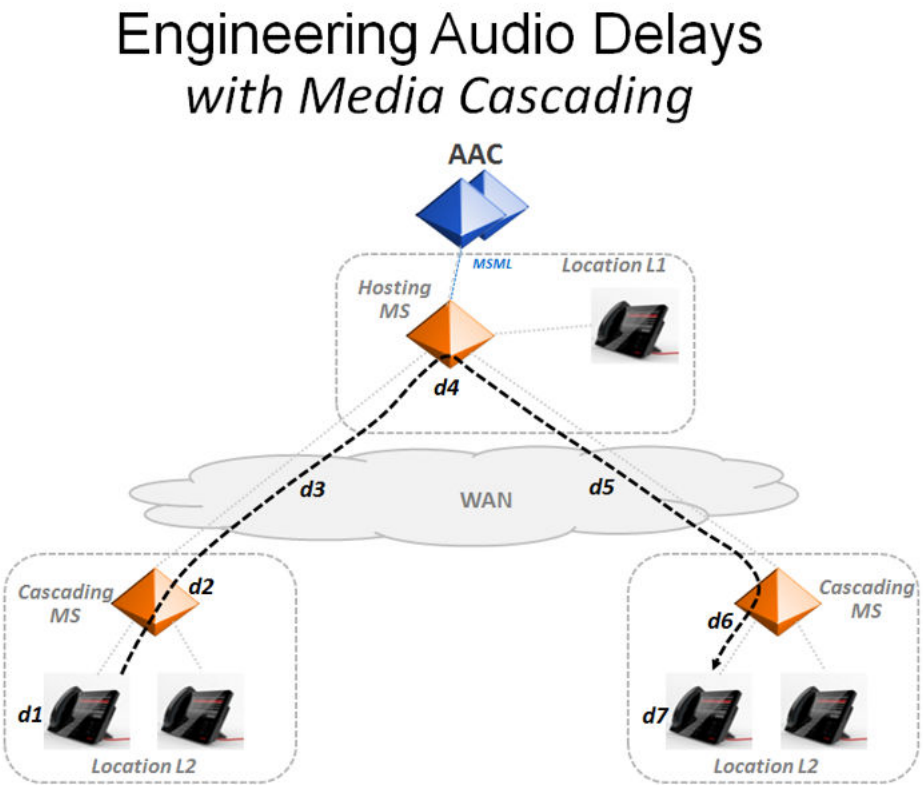


Figure 15: Engineering audio delays without media cascading

The following figures shows delay calculations for a media path that includes media cascading. A client codec G.722/G.711 is assumed with a packet time of 20 ms.

Delays to consider:

- d1: 30 ms
- d2: 55 ms
- d3: 30 ms (60 ms RTD)
- d4: 45 ms
- d5: 30 ms (60 ms RTD)
- d6: 50 ms
- d7: 40 ms
- Total 280 ms



For more information about the effect these delays have on the overall audio quality of the conference, see Effects of delay on audio quality on page 71. The additional delay introduced by media cascading is approximately 90 ms, due to the additional buffering and processing required (approximately 150 ms for media processing with cascading compared to 60 ms without cascading). In the preceding figures, the packet time used for the media streams between the cascading Avaya Media Server and the hosting Avaya Media Server is assumed to be 10 ms, which reduced the delays in media path when compared to 20 ms packet times.

Minimizing overall delays with packet time selection

An approach to consider that further minimizes the delay that is introduced by media cascading is to use a 10 ms codec between the clients and the cascading Avaya Media Servers

Note:

This feature will be available in a future client release.

This approach lowers the delays introduced by all Avaya Media Servers involved from 150 ms to about 130 ms when compared to a 20 ms packet time.

Shared bandwidth management

As described in the Network considerations on page 67, bandwidth management in an Avaya Aura® network is performed by the Avaya Aura® Session Manager with the cooperation of Avaya Aura® Conferencing using a SIP-based shared bandwidth management interface. Bandwidth that is required for an Avaya Aura® Conferencing session must first be allocated through this interface before the session can proceed. Other SIP sessions that are routed through the Avaya Aura® Session Manager can also consume bandwidth from this shared resource pool. This allows network bandwidth to be shared among applications under the control of the Avaya Aura® Session Managers.

Bandwidth that is required for sessions that are controlled within the Communication Manager or the Avaya Communication Server 1000 that are not routed through the Avaya Aura® Session Manager must be managed within the bandwidth management services of these elements until the shared bandwidth management interface is supported by these elements. This requires a portion of the available bandwidth for each network location to be dedicated to the Avaya Aura® Session Manager and a separate portion to be dedicated to the Communication Manager or the Avaya Communication Server 1000 systems.

Related topics:

Monitoring bandwidth usage on page 96

Monitoring bandwidth usage

If the communications patterns are uncertain prior to the introduction of Avaya Aura® Conferencing, bandwidth and port usage can be monitored closely during a phased rollout of the service to ensure that bandwidth usage is occurring as expected.

Key performance indicators (KPI) are provided by the Avaya Aura® Conferencing management tools, including information on bandwidth usage. The following data is reported on an individual location basis:

- Requested bandwidth: The bandwidth that is required without media cascading
- Negotiated bandwidth: The bandwidth that is required after media cascading is applied
- Actual bandwidth: A real time measurement of bandwidth usage, as measured by the Avaya Media Server. This can be used to determine whether there is a gap between the bandwidth requested within SIP signaling and bandwidth that is actually consumed.

The following figure shows one of the reports available in the Element Manager monitoring reporting tools to monitor usage patterns for a location. This report also shows an example of optimization that can be provided by media cascading by comparing the peak requested bandwidth with the peak negotiated bandwidth for a location. Bandwidth savings depends on a number of factors that can be unique to a location.

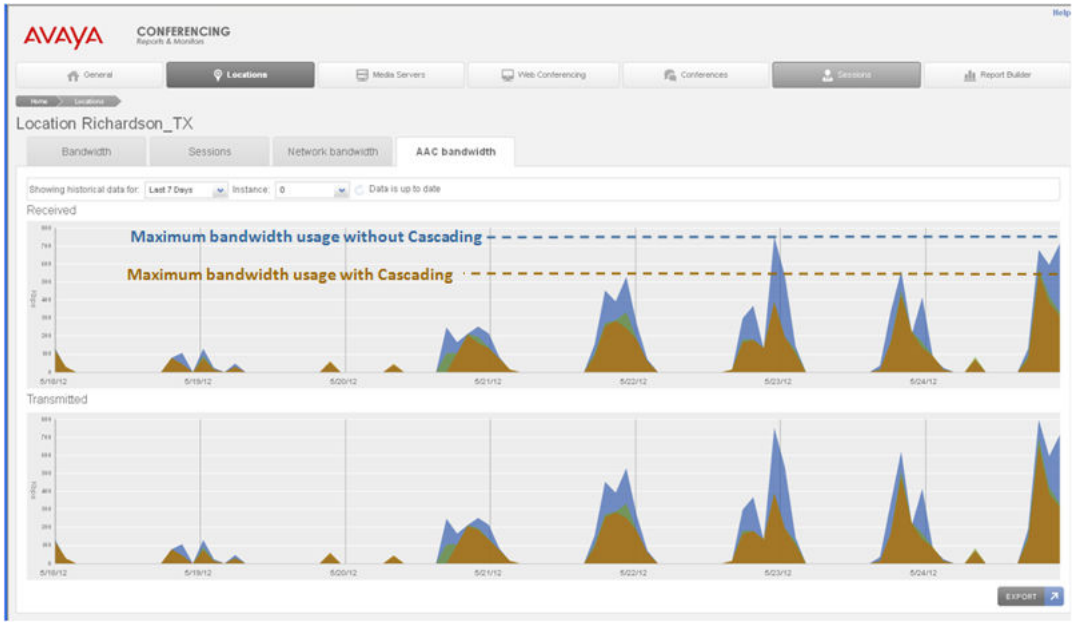


Figure 16: Location report — AAC bandwidth

Chapter 4: Before you begin

Before you begin checklist

The following checklist provides the high level steps and considerations prior to beginning your Avaya Aura® Conferencing installation.

Note:

If you are upgrading from Avaya Aura® Conferencing Release 7.0, go to "Chapter 27: Upgrading to Release 7.2."

#	Task	Description	Notes	✔
1	Ensure that version 6.2 is installed for System Manager, Session Manager, and Communication Manager prior to installing Avaya Aura® Conferencing. Obtain the System Manager IP address and FQDN.	See Solution requirements on page 21.		
2	Ensure that the **Ignore SDP for Call Admission Control** setting is disabled in System Manager. **Important:** The **Ignore SDP for Call Admission Control** setting in System Manager *must be* disabled for Avaya Aura®	Perform the following steps: 1. Log on to System Manager. 2. On the System Manager console, click **Session Manager** in the Elements section. 3. In the left navigation pane, click **Session Manager Administration**. 4. In the Global Settings section on the Session Manager Administration page, make sure		

#	Task	Description	Notes	✔
	Conferencing to operate properly.	the **Ignore SDP for Call Admission Control** check box is not checked. 5. If you changed the **Ignore SDP for Call Admission Control** setting, click **Save**.		
3	Download the Avaya Aura® Conferencing Intelligent Workbook from the Avaya Web site.	Go to http://support.avaya.com/ to download the Avaya Aura® Conferencing Intelligent Workbook.		
4	Determine your deployment layout type based on the capacity and scaling requirements for your location.	Include this information in the Avaya Aura® Conferencing Intelligent Workbook For information about deployment types, see Introduction to deployment layout options on page 27.		
5	Install your HP ProLiant DL360 G7 server. **Note:** If you are upgrading from Avaya Aura Conferencing 6.0 or Meeting Exchange 5.2, you must save your existing data on your Dell™ PowerEdge™ R610 or an IBM S8800 server and then install a new HP ProLiant DL360 G7 server. To save your existing data, see Introduction to migrating your data on page 541.	See Downloading HP documentation on page 105.		

#	Task	Description	Notes	✔
	You can repurpose your existing Dell™ PowerEdge™ R610 or IBM S8800 as a host for the Web Conferencing server and/or Flash Media Gateway server in the DMZ.			
6	Obtain the latest Avaya Aura® Conferencing disks for software installation and patches: • AAC platform DVD-ROM • Application Bundle DVD-ROM • Platform patches DVD-ROM	DVD-ROM disks are provided. You can also download from Avaya PLDS and burn your own CD- or DVD-ROM (for advanced users only).		
7	Use the Avaya Aura® Conferencing Intelligent Workbook for the following: • Determine the required number of IP addresses for your deployment configuration, hostnames, and FQDNs. • Register the required FQDNs with the appropriate DNS servers. **Important:** FQDNs are required for single	See the Avaya Aura® Conferencing Intelligent Workbook you previously downloaded.		

#	Task	Description	Notes	✔
	sign-on (SSO) to enable you to administer all the components using System Manager. DNS integration is required for SSO to work. **Note:** To use SSO, the System Manager FQDN, Element Manager FQDN, and Provisioning Client FQDN (if required) must belong to the same root domain.			
8	If you are deploying your system with TLS enabled, ensure Certificate Authorities are imported and certificates are assigned.	See Checklist for configuring Transport Layer Security on page 153.		
9	Obtain the supported Web browsers.	See Supported Web browsers.		
10	Obtain the License key file from Avaya and install the key on the WebLM server which resides on System Manager.	See Installing the license key on on page 151.		
11	If you are using a DMZ deployment, consider the following: • Ensure you have configured the required servers,	Contact your network specialist or administrator if you have a standalone with redundancy or standalone simplex deployment and require a DMZ configuration. For more information, see Enterprise DMZ deployment on page 62. For the complete *Port Matrix: Avaya Aura®*		

#	Task	Description	Notes	✔
	routers, and firewalls. • Ensure the required port modifications are made.	*Conferencing* document, go to http://support.avaya.com.		

Chapter 5: Installing hardware

Downloading HP documentation

Use this procedure to find and download the HP ProLiant DL360 G7 documentation.

Procedure

1. Open a browser and go to http://support.avaya.com.
2. Expand **Documentation** in the left hand menu.
3. Click **View All Documents**.
4. Click **C** in the alphabetical list along the top of the screen.
5. Scroll down to **Common Servers** in the C products.
6. Download the documents that you need.

HP DL360 document set

See the following documents for HP DL360 server information and procedures.

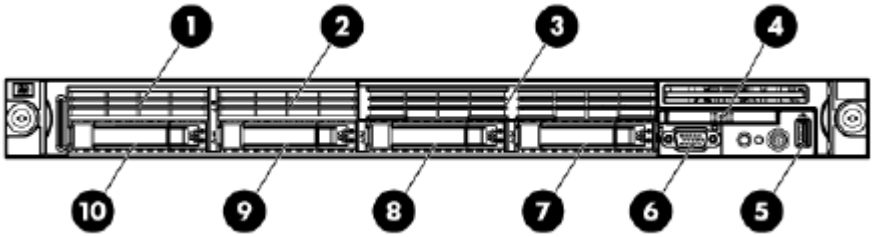
Documents

- HP ProLiant Servers Safety Information
- HP ProLiant DL360 G7 Server Maintenance and Service Guide
- HP ProLiant Servers Troubleshooting Guide
- HP ProLiant DL360 G7 Server User Guide

Documents included in the shipping container

Abbreviation	Title	Part number
1URH	1U Rack Hardware Installation Instructions	365 494–004
PCS	Power Cord Strain Relief Kit	407 454–021

Front view of HP DL360 G7 Server

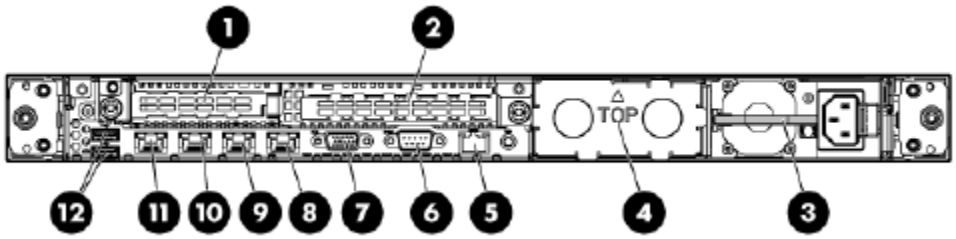


Note:

Servers ship with 2–4 hard disk drives, depending upon product requirements.

No.	Description
1	Not present
2	Not present
3	DVD-RW
4	HP Systems Insight Display
5	Front USB connector
6	Video connector
7	Hard drive bay 4
8	Hard drive bay 3
9	Hard drive bay 2
10	Hard drive bay 1

Back view of HP DL360 G7 Server



No.	Description
1	Slot 1 PCIe2 x8 (8, 4, 2, 1) **Note:** Servers might ship with a PCI card installed, depending upon product requirements.
2	Slot 2 PCIe2 x16 (16, 8, 4, 2, 1), 75W +EXT 75W* **Note:** Servers might ship with a PCI card installed, depending upon product requirements.
3	Power supply bay 1 (populated)
4	Power supply bay 2
5	iLO 3 connector
6	Serial connector
7	Video connector
8	NIC 4 connector
9	NIC 3 connector
10	NIC 2 connector
11	NIC 1 connector
12	USB connectors (2)

*This expansion slot provides 75 W of power to an adapter, with an additional 75 W of power supplied by external power.

HP DL360 G7 Server environmental specifications

Specification	Value
Temperature range	**Note:** All temperature ratings shown are for sea level. An altitude derating of 1°C per 300 m (1.8° per 1,000 ft.) to 3048 m (10,000 ft.) is applicable. No direct sunlight allowed.
Operating	10°C to 35°C (50°F to 95°F)
Shipping	-40°C to 70°C (-40°F to 158°F)

Specification	Value
Maximum wet bulb temperature	28°C (82.4°F)
Relative humidity (noncondensing)	**Note:** Storage maximum humidity of 95% is based on a maximum temperature of 45° C (113°F). Altitude maximum for storage corresponds to a pressure minimum of 70 kPa.
Operating	10% to 90%
Non-operating	5% to 95%

HP DL360 G7 Server physical specifications

Type	Description
Dimensions	Height: 4.32 cm (1.70 in)
	Width: 42.62 cm (16.78 in)
	Depth: 69.53 cm (27.38 in)
Weight (maximum; two processors, two power supplies, eight hard disk drives)	15.97 kg (35.20 lb)
Weight (minimum; one processor, one power supply, no hard drives)	14.51 kg (32.00 lb)
Weight (no drives installed)	14.06 kg (31.00 lb)

Installing the server in the rack

This installation checklist contains the principle steps that are necessary to install the server in the rack. Each task refers to an existing HP document and the topic title(s) that contains the step-by-step procedures. Where applicable, additional information and clarifications appear in the *Avaya recommendation* column. Perform each task in the order specified.

Note:

Although not used frequently, Avaya customers are required to have a monitor, keyboard, and mouse available for use by servicing technicians.

No.	Task	Reference	Avaya recommendation	✔
1	Observe safety warnings	ISI UG: *Rack warnings*		
2	Examine contents of shipping container (Avaya provided equipment)	UG: *Contents of the server shipping carton*	Ensure that the 6-digit material code on the order matches the 6-digit material code on the shipping container.	
3	Verify that the rack is installed according to the manufacturer's instructions and in accordance with all local codes and laws			
4	Examine installation environment (customer provided equipment)	UG: *Optimum environment*		
5	Verify that the rack is grounded in accordance with local electrical code.	UG: *Electrical grounding requirements*		
6	Remove the cabinet doors, if necessary.			
7	Determine and plan the vertical spacing of the servers in the frame.		Note that air flows into the front of the server and out the air vents located on the top surface of the server chassis. A 1U spacing is sufficient.	
8	Attach the rails to the rack.		The rails included with the server will accommodate most square-hole racks. If these rails do not fit the rack, the customer must provide rails or a shelf for rack installation. Also, the rails included with the server **might**	

No.	Task	Reference	Avaya recommendation	✔
			not work with round-hole racks, in which case the customer can obtain rails and/or a shelf from any distributor, for example http://www.racksolutions.com/. The customer-provided rails and rack must be on site prior to the first day of installation. **Note:** The customer is responsible for any rack screws.	
9	Attach the server to the rack.	UG: *Installing the server into the rack*		
10	(Optional) Install the cable management arm.			
11	Connect to the network.			
12	Connect the power cord(s).	SP: *Connecting the power cord to the power supply* UG: *Powering up and configuring the server*		
13	Power up the server.	UG: *Powering up and configuring the server*		

Updating the HP DL360 G7 server power management settings

Use this procedure to update the BIOS of the HP DL360 G7 server to enable its maximum performance mode of operation. Maximum performance mode provides the best real-time performance option for the server.

Note:

Running the HP DL360 G7 server in maximum performance mode places the highest requirements on power usage by the server. Consult the HP DL360 G7 server documentation for maximum power requirements and ensure the power circuit hosting this server has adequate amperage to supply this server and all other servers that share the circuit.

Before you begin

- Ensure the server is installed in the rack, is properly cabled, and has proper ventilation.
- Ensure the power circuit that hosts this server can provide sufficient amperage for all servers that share the circuit with this server, accounting for maximum power utilization by this group of servers.
- You must be able to access the server console through a locally attached keyboard and monitor or a keyboard, video card, and monitor (KVM) switch.
-

Procedure

1. Power up or reboot the HP DL360 G7 server to start its BIOS initialization sequence.
2. When the message `F9 = Setup` appears at the bottom of the screen, and press **F9**.
3. When the Setup Utility screen appears, select **Power Management Options** from the menu, and press **ENTER**.
4. Select **HP Power Profile** from the menu, and press **ENTER**.
5. Select **Maximum Performance** from the menu, and press **ENTER**.
6. Select **Advanced Power Management Options** from the menu, and press **ENTER**.
7. Select **Dynamic Power Savings Mode Response** from the menu, and press **ENTER**.
8. Select **Fast** from the menu, and press **ENTER**.
9. Select **Collaborative Power Control** from the menu, and press **ENTER**.
10. Select **Disabled** from the menu, and press **ENTER**.
11. Select **Turbo Boost Optimization** from the menu, and press **ENTER**.
12. Select **Optimization for Performance** from the menu, and press **ENTER**.
13. Press **ESC** twice to return to the main Setup Utility screen.
14. At the main Setup Utility screen, press **ESC** to exit the Setup Utility.
15. Press **F10** to confirm that you want to exit the Setup Utility.

The server continues the BIO initialization/reboot sequence.

Chapter 6: Installing software

Introduction to software installation

This chapter provides installation information for the following:

- Linux operating system and Base level packages
- Linux patches
- Element Manager
- Avaya Media Server

Two DVDs of the software components (Platform and Application Bundle) are provided with the hardware.

Software installation procedure

The following table provides a high-level view of the tasks involved in installing the platform and applications software.

#	Task	Description	Notes	✔
1	Ensure you have planned your deployment layout and populated your data in the Avaya Aura® Conferencing Intelligent Workbook.	See Before you begin checklist on page 99.		
2	Review the prerequisites.	See Prerequisites for software installation on page 115.		
3	Start the installation process.	See Installing the AAC Platform on page 116.		

#	Task	Description	Notes	✔
	Important: The Installing Linux procedure guides you through the installation process with links to individual procedures. Upon completion of each step, return to the next step in the Installing Linux procedure by clicking the link at the end of each individual procedure.			
4	Verify that all the required components are operational and error free after completing the Linux Operating System installation.	See Verifying the AAC Platform installation on page 129.		
5	Install the components for Avaya Aura® Conferencing.	See Installing the components for Avaya Aura Conferencing on page 135.		
6	Install the Avaya Media Server.	See Installing Avaya Media Server on page 134.		
7	Patch database software.	See Patching database software on page 492.		
8	Log on to Element Manager Console for the first time.	See Accessing Element Manager Console using local login on page 147.		

Prerequisites for software installation

- The following components must be installed and operational prior to installing Avaya Aura® Conferencing.
  - Avaya Aura® Session Manager Release 6.2
  - Avaya Aura® System Manager Release 6.2 or 6.3
  - one of the following IP telephony servers:
    - Communication Manager Release 5.2.1, 6.0.1, or 6.2
    - Avaya Communication Server 1000 Release 7.6

    Note:

    If you want to support video conferencing with CS 1000, you must install the Collaboration Pack feature.

  For more information about installing these components, see Solution requirements on page 21.
- The Deployment layout type has been chosen based on the capacity and scaling requirements.
- The following data has been gathered:
  - Avaya Aura® System Manager VSP IP address
  - Avaya Aura® System Manager OAM IP address
  - Avaya Aura® System Manager OAM Fully Qualified Domain Name (FQDN)
  - Avaya Aura® Session Manager Signaling Service IP Address
- The data in the Avaya Aura® Conferencing Intelligent Workbook has been completed and the required number of IP addresses obtained. For more information, see How to use this document on page 20.
- Obtain the latest installation disks for Linux, software installation and patches:
  - AAC 7.2 Platform DVD-ROM
  - Application Bundle DVD-ROM
  - AAC Platform patch (if released)
  - AAC DB sofware patches (if released)
  - AAC Application patches (if released)

- The target servers meet the following requirements:
  - All Application Servers have the same hardware type with the same disk, CPU, memory, and network interface configuration.
  - All servers meet the minimum hardware and configuration requirements for Avaya Aura® Conferencing.
  - All servers are connected and installed into the target environment including cables and network connections.
  - All servers have the Motherboard BIOS and the disk controller BIOS settings configured to ensure installation of the server platform software.
- The host environment meets the following:
  - Networking is in place to host the target servers and it is configured to route traffic between servers, firewalls, routers, switches, DMZ, and any other equipment in the host network, for example, management stations.
  - Up to two NTP clock sources available for the system to receive clocking information.
  - A desktop computer or server (other than the one hosting the target server), that can execute ICMP ping requests.
  - A Windows based PC with Internet Explorer 8.0 or 9.0, or Firefox 4.0 or later.
  - A desktop computer or server that is synchronized to the same external NTP clock sources used by the target servers.
- A backup is performed on the target server or the required files are transferred.
- Obtain any certificates that are to be used from either an Enterprise Certificate Authority or from some other well-known trusted Certificate Authority.

Installing the AAC Platform

This section provides the procedures for installing the Avaya Aura® Conferencing platform operating system and base level packages to the target servers required for the initial system installation.

Before you begin

- Obtain the latest Avaya Aura® Conferencing 7.2 Platform DVD-ROM and the Application Bundle DVD-ROM.
- Obtain the Linux service pack patch disk.
- Ensure that the DVD-ROM drive is selected as the first priority boot device in the system BIOS (typically configured during initial BIOS setup).
- Ensure that the server backup file is on a remote server

- Ensure access to the server console through a locally attached keyboard and monitor or a Keyboard, video card, and monitor (KVM) switch.
- Plan and identify the deployment layout including all network IP addresses, hostnames, and FQDNs using the Avaya Aura® Conferencing Intelligent Workbook.

Note:

Avaya recommends that you implement DNS lookup to synchronize domain names and IP addresses for the Avaya Aura® Conferencing solution. If your deployment does not support DNS lookup, see DNS and Avaya Aura Conferencing on page 589.

- Plan and identify any expansion servers using the Avaya Aura® Conferencing Intelligent Workbook.

About this task

Avaya Aura® Conferencing must be installed on a Linux platform. Use the following procedure to install the Avaya Aura® Conferencing platform operating system and base level packages on the HP ProLiant DL360 G7 server.

Procedure

1. Insert the AAC Platform DVD-ROM, and reboot the server.
   The following message on the installation welcome screen appears:

   ```
   Welcome to the MCP Core Linux System Installer
   ```

2. At the boot prompt, type `install-kvm`, and press **Enter**.
3. To check the integrity of the system, type `y`, and press **Enter**.

   Important:

   If you do not check the integrity, a defective DVD-ROM or optical drive can go undetected and result in an installation failure.

   If you receive a message indicating that the integrity check has failed, follow the recommendations to clean or replace DVD-ROM, or replace the optical drive.

   If there are no issues with the integrity check, the installation continues to the next prompt.

4. At the prompt, `Would you like to view licensing information? (Y/N) [Y]?`

   - Type `n` if you have already viewed the licensing information from a previous server installation, and press **Enter**. Proceed to Step 5 on page 118.

     OR

   - Type `y` to acknowledge the licensing attributes, and press **Enter**.

     You are prompted for the following:

   a. At the prompt, `Enter Selection`, select one of the following:

- Enter `1` for a Licensing overview.
- Enter `2` for a summary of Open Source RPMs and Licenses.
- Enter `3` to exit.

b. Press **Enter** until the `Enter Selection` prompt appears again.

c. At the prompt to acknowledge the licensing information, type `y`, and press **Enter**.

Warning:

In the following step, the installer erases all existing data on the attached disk drives.

5. At the `Continue [c], abort [a]` prompt, type `c` to continue, and press **Enter**.
6. At the prompt, `Do you want to keep this date and time (Y/N) [Y].`
   - Type `y` to keep the current system date and time, and press **Enter**. Proceed to the next step.
   - Type `n` to change the system date and time from the BIOS clock, and press **Enter**. Proceed to Modifying the BIOS clock on page 119.
7. The installer attempts to identify the hardware type of the target server, perform one of the following:
   - If the installer has detected your target server as a known reference server:

     Type `A` to accept and proceed to Step 9 on page 118 or type `O` and proceed to Classifying the hardware environment on page 120.

     OR

   - The installer does not detect your target server as a known reference server:

     At the prompt, type a number that corresponds to your hardware type, and press **Enter**. For example, type `3` to select HP ProLiant DL360 G7.

     ```
     1. Other
     2. IBM-X3550
     3. HP-Proliant-DL360-G7
     4. Dell-PowerEdge-R610
     Hardware type (1-4) [1]:
     ```
8. At the prompt, `Is this information correct? y/n`, type `y` to continue or `n` to correct.
9. At the prompt to choose the install type, type `1` to select Manual Install, and press **Enter**.

10. On the System Configuration screen, at the prompt, `Press the Enter Key to begin configuration`, press **Enter**, and proceed to Configuring the system on page 121.
11. Configure the NTP clock source settings. See Configuring the NTP clock on page 123.
12. Configure the Syslog Server. See Configuring the Syslog Server on page 125.
13. View the User Accounts and Passwords. See Viewing the user accounts and passwords on page 126.
    The data entry phase of the installation is finished.

    Next, the system partitions the hard drives and formats the file systems. Upon completion, the `Post System Configuration Complete` message appears, the disk automatically ejects and can be removed. The system restarts.
14. After the server restarts, create the initial logon passwords. See Creating the initial logon password on page 126.
15. Apply the server platform patches to the target server. See Applying server platform patches on page 127.
16. Verify that all the required components are operational and error free. See Checklist for verifying Linux Operating System installation on page 129.

Next steps

Proceed to Installing the components for on page 135.

Related topics:

Modifying the BIOS clock on page 119
Classifying the hardware environment on page 120
Configuring the system on page 121
Configuring the NTP clock on page 123
Configuring the Syslog Server on page 125
Viewing the user accounts and passwords on page 126
Creating the initial logon password on page 126
Applying server platform patches on page 127
Verifying the AAC Platform installation on page 129

Modifying the BIOS clock

During the software installation of the target server, you can modify the BIOS clock.

Before you begin

The procedure for Installing the license attributes is completed.

Procedure

1. At the prompt `Enter the month (1-12) [x]` type the number that represents the current month, and press **Enter**. For example, 1 represents January and 12 represents December.
2. At the prompt `Enter the day (1-xx) [x]` type the value for the current date, and press **Enter**.
3. At the prompt `Enter the year (YYYY) [xxxx]` type the current year, and press **Enter**.
4. At the prompt `Enter the hour (0-23) [xx]` type the value for the current hour using the 24–hour clock, and press **Enter**. For example, the first hour of the day is 0 and the last hour of the day is 23.
5. At the prompt `Enter the minutes (0-59) [xx]`, type the minutes using the 24–hour clock, and press **Enter**. For example, the first minute of the day is 0 and the last minute of the day is 59.
6. At the prompt `Do you want to keep this date and time (Y/N) [Y] ?`, type `y` to save your changes, and press **Enter**.

Next steps

Proceed to Step 7 on page 118 in Installing the AAC Platform on page 116 to continue the Linux installation process.

Classifying the hardware environment

During the software installation of the target server, you can classify the server hardware as either a known reference server or as a non-reference server. The installer usually determines this classification but it can be manually changed in the following procedure.

Note:

If two disks have been detected and the reference server does not support the RAID-1 software, the two physical disks are identified by the installer as a single disk drive. If a single disk has been detected and the reference server requires two disks for RAID-1 disk mirroring, the installation aborts.

About this task

Configure the target server as a reference or non-reference server and to change the default hardware.

Procedure

1. If the installer identifies the target server as a reference server, choose the number in the list that corresponds to the hardware type, and proceed to Step 3 on page 121. For example, type `7` for HP DL360 G8.
2. If the installer does not detect the server as a reference server, a list of hardware options appears, type `1` for Other, and press **Enter**. Proceed to Step 4 on page 121.
3. If the target server is a reference server, at the prompt, `Hardware Environment: <hardware platform>`, for example, HP DL360 G8, type `y`, and press **Enter**.
4. If the installer detects a non-reference server, at the prompt, `Hardware Environment: Other`, type `y`, and press **Enter**.
5. A message appears to indicate the size and number of disks. If the physical disk configuration matches the requirements for the reference server, press **Enter** to continue.
   - If one of the two disks detected on the target server is not a RAID logical disk, at the prompt, type `y`, and press **Enter** to configure RAID-1 between the two disks.
   - If configuring RAID-1, a message appears indicating the size of the disk, press **Enter**.

   The hardware is configured.

Next steps

Proceed to Step 9 on page 118 in Installing the AAC Platform on page 116 to continue the Linux installation process.

Configuring the system

During the Linux operating system installation, you are prompted to configure the usernames, passwords, server time, IP address, DNS, and hardware type for your system.

About this task

Configure the system.

Procedure

1. On the Network Configuration screen, at the prompt `Enter hostname`, type a hostname for the server.
2. At the prompt `Enter bond name [bond0]`, press **Enter** to accept the default.

A list of available Ethernet Network interfaces appears.

3. At the prompt `Enter the first slave [eth0]` type the Bond0 Slave0 value for the server or press **Enter** to accept the default value.
4. At the prompt `Enter the second slave [eth1]`, type the Bond0 Slave1 value for the server or press **Enter** to accept the default value.
5. At the prompt `Enter VLAN ID (0=no VLAN) (0-4094)`, type 0 as this is not supported, and press **Enter**.
6. At the prompt `Enter subnet name [sn0]`, press **Enter** to accept the default value.
7. At the prompt `Enter IP address`, type the Network IP address of the server, and press **Enter**.
8. At the prompt, `Enter subnet prefix length (1-32)`, type the Network Prefix of the server, and press **Enter**.
9. At the prompt `Enter gateway IP address`, type the Network Default Gateway, and press **Enter**.
10. At the prompt `Do you want to configure DNS Client? (Y/N) [Y]`, type `y` and press **Enter**.
    The following prompt appears:

    ```
    Please select one of the following actions:
    - [A]dd Domain Suffix(es)
    - Re[S]elect all Domain Suffix(es)
    - [C]ontinue
    ```

11. At the prompt, type `c` to continue or `a` to add suffixes, and press **Enter**.
12. At the prompt `How many DNS Servers would you like to reference (1-3) [1]`, type the number of available DNS servers, and press **Enter**.
13. At the prompt `Enter DNS Server`, type the IP address of the DNS server, and press **Enter**.
14. At the prompt `You entered "<IP address>". Is this correct? (Y/N) [N]`, verify the IP address.
15. If the IP address is correct, type `y` and press **Enter**.
16. The System Console Redirection screen appears. At the prompt `Select an option (1-3)`, type `3` to select `Do not redirect the system console after installation` as the default, and press **Enter**.
17. The Timezone Selection screen appears. At the prompt `Enter Region (1-62)`, type the number that corresponds to the Timezone Field1 for the target server, and press **Enter**.

18. If you see the screen Timezone Selection for Region, at the prompt `Enter Timezone`, type the number that corresponds to the Timezone Field2 for the target server, and press **Enter**.
19. The Configuration Validation screen appears. Type `y` to accept the values or type `n` to reenter the information. Press **Enter**.

Result

Proceed to Configuring the NTP clock or return to step 11 on page 119 in Installing the AAC Platform on page 116 to determine where you are in the installation process.

Configuring the NTP clock

During the software installation, you are prompted to configure the Network Time Protocol (NTP) settings.

Note:

You must use the same NTP sources that are being used on the System Manager. For more information about the NTP server IP addresses, see the Avaya Aura® Conferencing Intelligent Workbook.

About this task

Configure the NTP clock settings.

Procedure

1. At the prompt, `Please indicate the Clock Source function of this server:`
   a. `Primary Clock Source server (primary Element Manager server machine)`. For example, EMServer1.
   b. `Secondary Clock Source server (secondary Element Manager server machine)`. For example, EMServer2.
   c. `This server is NOT a Clock Source server (all other server machines)`. If you select this option, continue to Step 5 on page 124.

   `Select an option (1-3):`

   Note:

   If this is a simplex layout and you are configuring a server hosting Element Manager, type `1`, and press **Enter**.

2. The primary clock source server requires an external clock. At the prompt, `Select External Clock for time source(s) external to this server. Select Internal clock to use the system clock as the time source.`

   `E – External Clock Source (IP Addresses)`

   `I – Internal Clock (Unreliable)`

   `Select an option (E, I):` Type `e`, and press **Enter**.

3. At the prompt `How many external clock sources would you like to reference (1-2) [1]`, type a number based on the following:

   - If both External Clock Source #1 and External Clock Source #2 have an IP address, type `2`, and press **Enter**.
   - If there is only one external clock source, type `1` or press **Enter** to accept the default.

4. At the prompt `Enter Clock Source IP address #1`, type the IP address for the external clock source.

   If you have more than one clock source, a second prompt appears.

5. At the prompt, `Enter IP Address of Primary Clock Source`, type the IP address for the Primary Clock Source, and press **Enter**.

   If you have a secondary clock source, a second prompt appears.

6. At the prompt, `Enter IP Address of Secondary Clock Source`, type the IP address for the Secondary Clock Source, and press **Enter**.

   Note:

   For simplex layouts, you can use the same IP address for primary and secondary clock source.

7. At the prompt, `Is this information correct? Y/N [N]`, type `y` to continue or `n` to correct.

8. At the prompt, `Please indicate the Clock Source function of this server:`

   a. `Primary clock Source server (primary Element Manager server machine)`

   b. `Secondary Clock Source server (secondary Element Manager server machine)`

   c. `This server is NOT a Clock Source server (all other server machines)`

   `Select an option (1-3) [1].` Type `2`, and press **Enter**.

9. At the prompt, `The Secondary Clock Source server requires the use of an external clock.`

Comments? infodev@avaya.com

Select External Clock for time source(s) external to this server.

Select Internal Clock to use the local system clock as the time source.

```
E - External Clock source (IP Addresses)
I - Internal Clock (Unreliable)
Select an option (E, I):
```

Type `e`, and press **Enter**.

10. At the prompt, `How many external clock sources would you like to reference (1-2) [1]`, type `2`, and press **Enter**.
11. At the prompt, `Enter IP Address of Primary Clock Source:`, type the IP address, and press **Enter**.

Next steps

Proceed to configuring the Syslog Server or return to step 12 on page 119 in Installing the AAC Platform on page 116 to determine where you are in the installation process.

Configuring the Syslog Server

During the Linux operating system installation, you are prompted to configure the Syslog Server.

About this task

Configure the settings for the Syslog Server, if required.

Procedure

1. On the Syslog Configuration screen, at the prompt `Do you wish to configure a Syslog Server IP address (Y/N) [N]?`, type `n` (default), and press **Enter**. Proceed to the next section for viewing the user accounts and passwords.
   - If you want to configure the Syslog Server IP address, type `y`, and press **Enter**. Proceed to the next step.
2. At the prompt `Enter the Syslog Server IP address`, type the value for the Syslog IP address, and press **Enter**.
3. On the Configuration Validation screen, if the values are correct, type `y`, and press **Enter** to accept and continue or type `n`, and press **Enter** to reenter the data.

Next steps

Proceed to Viewing the user accounts and passwords or return to step 13 on page 119 in Installing the AAC Platform on page 116 to determine where you are in the installation process.

Viewing the user accounts and passwords

During the Linux operating system installation, the list of user accounts and passwords appear.

About this task

View the list of user accounts and passwords.

Procedure

1. On the User Accounts & Passwords screen, the list containing the user accounts and passwords appears. Press **Enter** to continue.
2. At the prompt `Press the Enter Key to continue with the installation`, press **Enter**.

Result

The data entry phase of the installation is now finished. The system completes the process for partitioning the hard drives, formatting the file systems, and installing software packages.

Next steps

After the system restarts, proceed to Step 14 on page 119 in Installing the AAC Platform on page 116 to continue the system installation process.

Creating the initial logon password

Upon completion of the Linux software installation process and a server restart, you are prompted for the initial logon password.

About this task

Change the initial logon password for the following accounts:

- root
- ntsysadm (SSA role)
- ntappadm (AA role)
- ntsecadm (SA role)
- ntbackup (BA role)
- ntdbadm (DBA role)
- ntossadm (OSS role)

Procedure

1. On the server console, at the prompt `[<hostname>] login`, type `root`, and press **Enter**.
   Where <hostname> is the short name of the FQDN. For example, the shortname of the FQDN EMServer1@avaya.com is EMServer1.
2. At the prompt `Password`, type `password`, and press **Enter**.
3. At the prompt `(current) UNIX password`, type `password`, and press **Enter**.
4. At the prompt `New UNIX password`, type the new password for the account, and press **Enter**.

   Note:

   You are required to enter a complex password.
5. At the prompt `Retype new UNIX password`, retype the new password, and press **Enter**.
   The password successfully changed if you see the system message `Authorized users only. All activity may be monitored and reported.`
6. Type `logout`, and press **Enter**.
7. Repeat steps 1 on page 127 to 6 on page 127 or use the **`passwd`** command to create passwords for the following accounts:
   - ntsysadm
   - ntappadm
   - ntsecadm
   - ntbackup
   - ntdbadm
   - ntossadm

Next steps

Proceed to Applying server patches or return to 15 on page 119 in Installing the AAC Platform on page 116 to determine where you are in the installation process.

Applying server platform patches

About this task

Apply server platform patches to the target server.

Procedure

1. Log on to the server as `ntsysadm` through ssh or directly on the server console.
2. Enter **`su -`** to log on as root.
3. At the prompt `password`, type the root password, and press **Enter**.
4. Insert the server platform patch DVD-ROM.
5. Type `mcpExtractContent.pl -aat`, and press **Enter**.
6. Type `1`, and press **Enter** for optical drive.

   Note:

   A warning appears to inform you that no feedback appears on the screen for several minutes while the disk contents are extracted.
7. Type `cd /var/mcp/os/install/images` to change the directory, and press **Enter**.
8. Type `ls`, and press **Enter** to see a list of files. The file ending in .iso is the patch image.
9. Type `patchPlatform.pl <filename>.iso -np`(where <filename> is the name of the patch iso file), and press **Enter**.

   If the patching tool is out of date, the system resident tool is updated and the server automatically restarts. The following message appears: `The system-resident patching tool (patchPlatform.pl) has been updated from version x.x.x to version y.y.y. Please re-execute the (updated) "patchPlatform.pl" command.`

   Warning:

   The server restarts.
10. After the server completes the restart, log on to the server, and type `patchPlatform.pl <filename>.iso –np` again, and press **Enter**.

    The patchPlatform.pl script checks to determine if there is an updated patch image file. You can omit this step if you always install the latest patch.

    - If no patches are required, the following message appears.

      `No applicable patch(es). Number of patches applied: 0.`

    - If patches are required, the patches are listed and automatically applied to the system.

      Note:

      After the last patch has been applied, the server automatically restarts.

11. After the server restarts, log on with any account through ssh or directly at the console, and type `mcpRelease.pl`, and press **Enter** to verify the release level. For example, if you were previously on OS version 17.0.17 and then applied the patch to 17.0.22, you see the following output:
    ```
    System Type: mcp_core_linux_ple2 Release Level: 17.0.22 (via patching)
    ```
    The release level in the previous example shows the version corresponding to your patch file.

    The patches have been applied.

Next steps

Proceed to the post operating system installation verification checklist or return to 16 on page 119 to determine where you are in the installation process.

Verifying the AAC Platform installation

Use the procedures in the following table to verify that all the required components of the AAC Platform are operational and error free.

Table 33: AAC Platform verification checklist

#	Task	Description	Notes	✔
1	Ping the Network IP Address from a network other than the one hosting this server.	Verify a successful route through the hosting default gateway is established.		
2	Attempt to access the logon prompt for the target server through ssh or the server console. Log on to ntsysadm.	Verify a successful logon.		
3	On the command line, type **`date`**, and press **Enter**. Verify the reported date and time match the current date and time for the hosting time zone, accurate to the second. For a continuous display of the time, type: **`watch -n1 date`** and cancel by pressing **Control+C**. Compare this with another system that already	Verify the date and time are successfully synchronized.		

#	Task	Description	Notes	✔
	has the external NTP clock source synchronized.			
4	If Syslog was configured in 12 on page 119, verify the streaming of syslogs to the remote server. Log on as ntsyadm and type the command **`logger test message`**, and press **Enter**.	Use a test message to verify that a syslog entry is created on the remote server .		

Note:

Complete the AAC Platform installation process and basic configuration for each server before proceeding to Installing the components for Avaya Aura Conferencing on page 135.

Introduction to the Avaya Media Server (MS)

In a co-resident deployment, the conferencing media server and the recording media server reside on the same physical server. This server is a HP DL360 with 2X300GB and 2X900GB in a RAID 1 configuration. In a standalone deployment, the conferencing media server and the recording media server do not reside on the same server.

So, if you have a co-resident deployment, you can simply install the media server. There is no need to install a separate conferencing media server and a separate recording media server. The two servers are bundled together.

However, if you have a standalone deployment, you must install the recording media server and also install a separate conferencing media server.

Note:

The conferencing media server is sometimes also known as the Avaya Media Server (MS).

Before you begin

You must install and verify the AAC platform.

Procedure

1. Reconfigure the RAID 1 arrays using the HP SmartStart CD.
   See Reconfiguring the RAID 1 arrays using the HP SmartStart CD on page 131.

2. Format and mount the second RAID.
   See Formatting and mounting the second RAID on page 132.
3. Install the Avaya Media Server (MS).
   See Installing the Avaya media server on page 134.
4. **(Optional)** If you have a standalone deployment, you must also install a separate conferencing media srever.
   See Installing the Avaya media server on page 134 (for a second time).

Related topics:

Reconfiguring the RAID 1 arrays using the HP SmartStart CD on page 131
Formatting and mounting the second RAID on page 132
Installing Avaya Media Server on page 134

Reconfiguring the RAID 1 arrays using the HP SmartStart CD

Before you begin

- You have installed the two 900 Gb hard drives from the AAC 7.2 Upgrade Kit.
- You have the HP SmartStart CD.

About this task

Use this procedure to configure the four hard drives to two RAID 1 arrays on the HP DL360 G7 server.

Procedure

1. On the HP DL360 G7 server, insert the HP SmartStart CD into the CD-ROM drive.
2. Boot the system from the HP SmartStart CD.
3. When prompted, select the language you want to use, and then click **Next**.
4. Read the user license agreement.
5. To accept the user license agreement, click **Agree**.
6. When prompted to select the operation you want to begin, click **Maintenance**.
7. When prompted to select the maintenance operation you want to begin, click **HP Array Configuration and Diagnostics**.
8. In the Array Configuration Utility, select the device (for example, **Smart Array P410I in Embedded Slot**).
   The list of logical drives is displayed.
9. Remove all logical drives:

a. Select the logical drives in the left panel.
b. Click **Delete** in the right panel.
c. When prompted, confirm that you want to remove the logical drives.
The list of unassigned drives is displayed.

10. Create the first RAID:
    a. Click the **Wizard** tab.
    b. On the Wizard tab, click **Add Logical Drive**.
    c. Select the first two hard drives (HDD1 300 Gb in hard drive bay 1 and HDD2 300 Gb in hard drive bay 2), and click **Next**.
    d. When prompted to add remaining hard drives to the RAID, click **Next** to skip this step.
    e. In the Fault Tolerance section, select **RAID 1**, and click **Next**.
    The first RAID is now created.
11. Create the second RAID:
    a. Click the **Wizard** tab.
    b. On the Wizard tab, click **Add Logical Drive**.
    c. In the Select Logical Drive Creation Method section, select **Create Logical Drive or New Array**.
    d. Select the two remaining hard drives (HDD3 900 Gb in hard drive bay 3 and HDD4 900 Gb in hard drive bay 4), and click **Next**.
    e. In the Fault Tolerance section, select **RAID 1**, and click **Next**.
    The second RAID is now created.
12. On the bottom, left-corner of the window, click **Exit ASU** and exit from HP SmartSmart Tools.
    The server reboots.
13. Eject the HP SmartStart CD from the server.
    The hard drives are configured to the RAID arrays.

Formatting and mounting the second RAID

Before you begin

You have installed the two 900 Gb hard drives from the AAC 7.2 Upgrade Kit.

About this task

Use this procedure to format and mount the second logical drive on the HP DL360 G7 server.

Note:

The Recording feature requires the second logical drive. You must format and mount the second logical drive before installing the Avaya Media Server platform.

Procedure

1. Log on to the server as a user with the SSA role (for example, `ntsysadm`) through ssh or directly on the server console.
2. Enter **`su -`** to log on as root.
3. At the prompt `password`, type the root password, and press **Enter**.
4. Type `mcpDataDiskMgt.pl -q`, and press **Enter** to check that the second logical drive is available.
   The system should display information indicating that the RAID status is okay and the query command succeeded. An example of the output is:

   ```
   The expected data partition '/dev/cciss/c0dlpl' is not
   present on the system.
   The raid controller reports:
   A logical drive is available.
   It is 838.2 GB large and RAID 1.
   It has a RAID status of OK.
   Query command succeeded.
   ```

5. Type `mcpDataDiskMgt.pl -f`, and press **Enter** to format the second logical drive.
   The system displays the following information:

   ```
   Are you certain that you wish to reformat this disk?
   All information that is currently on it will be lost! (Y/N) [N]?
   ```

6. Type `y`, and press **Enter** .
   The system should display the following information:

   ```
   Format command succeeded.
   ```

7. Type `mcpDataDiskMgt.pl -q`, and press **Enter** to check that the second logical drive is ready for mounting.
   The system should display information indicating that the RAID status is okay and the query command succeeded. An example of the output is:

   ```
   The expected data partition '/dev/cciss/c0dlpl' is not
   currently mounted on /var/mcp/datadisk.
   The raid controller reports:
   A logical drive is available.
   It is 838.2 GB large and RAID 1.
   It has a RAID status of OK.
   Query command succeeded.
   ```

8. Type `mcpDataDiskMgt.pl -m`, and press **Enter** to mount the second logical drive.
   The system should display the following information:

   ```
   Created mount point
   Mount command succeeded.
   ```

9. Type `mcpDataDiskMgt.pl -q`, and press **Enter** to check that the second logical drive is mounted.
   The system should display information indicating that the correct data partition is mounted. An example of the output is:

```
The correct data partition is mounted on the expected mount point.
The mount point information reported by the operating system is:
/dev/ciss/c0dlpl /var/mcp/datadisk ext3 rw, nosuid, nodev, data=ordered 0
The raid controller reports:
A logical drive is available.
It is 838.2 GB large and RAID 1.
It has a RAID status of OK.
Query command succeeded.
```

Installing Avaya Media Server

Avaya Media Server is a software-based, media processing server. All media processing required by Avaya Aura® Conferencing is performed by the Avaya Media Server. The Avaya Media Server architecture facilitates unique scalability for all core functions of the platform, including signaling, application execution, content management, and media processing.

About this task

Extract the application software and install the Avaya Media Server for standalone with redundancy and standalone simplex system configurations.

Note:

The Avaya Media Server is installed automatically for co-resident deployment configurations.

Procedure

1. Log on to Avaya Media Server as ntappadm through ssh or directly at the server console.
2. Insert the Application Bundle DVD-ROM.
3. Type `mcpExtractContent -at mcp_ams_platform`, and press **Enter** to extract the Avaya Media Server load build.
4. If prompted, type the password for the ntappadm account, and press **Enter**.
5. At the prompt, `The following files have been found, [1] Optical drive, [2] Quit`, type `1`, and press **Enter** to extract the files from the CD in the optical drive.
6. Type `ll/var/mcp/loads`, and press **Enter** to verify the Media Server load zip file entitled MCP_MediaServer_7.5.0.###_YYYY.MM.DD_##.zip is available. For example, MCP_MediaServer_7.5.0.329_2011.10.17_77.zip.

The application software files for Avaya Media Server are extracted.

7. Log on as ntsysadm through ssh.
8. Enter **su -** to log on as root.
9. At the `Password` prompt, type the password for the root account, and press **Enter**.
10. Enter `mcpMsInstall.pl`.

    Note:

    The message `mcpMsInstall.pl script has no input parameters` appears and you are prompted to select an Avaya Media Server load to install.

    The install script finds the zip file.
11. At the prompt, `Use this load? (Y/N) [Y]`, type `y`, and press **Enter**.
12. At the prompt, `Continue installation (Y/N)? [Y]`, press **Enter** to accept the default.

Result

The message `Installation completed SUCCESSFULLY` appears. The Avaya Media Server load is now installed.

Next steps

Proceed to patching the database software or return to the Checklist for software installation on page 113 to determine where you are in the process.

Installing the components for Avaya Aura® Conferencing

Use the following procedure for a fresh installation of the Avaya Aura® Conferencing components on a new system.

Before you begin

- The AAC Platform operating system is installed.
- You have obtained the installation properties and identified the tags file based on your deployment type. To assist, use the Avaya Aura® Conferencing Intelligent Workbook. For more information, see How to use this document on page 20.
- You have obtained the required number of IP addresses for your deployment layout type, see IP address table for deployment types on page 138.

About this task

This procedure uses an automated mcpInstaller script that installs the following components in the following order:

- Avaya Aura® Conferencing Application Database: The Avaya Aura® Conferencing application requires a database in which all configuration, provisioning, and operational data is stored. The database software is installed on the server(s) that host the Element Manager.
- Avaya Aura® Conferencing Application software: This is the core conferencing application. After the installation is complete, the primary instance (0) of Element Manager is running, along with the primary and optionally (if redundant system) secondary database instances. The Element Manager administration console can be accessed after this step is complete.
- Avaya Media Server (co-resident configurations only): The Avaya Aura® Conferencing application requires one or more Avaya Media Servers for media processing. For standalone configurations, this installation step is manual. For more information, see Installing Avaya Media Server on page 134.

Procedure

1. Log on to EMServer1 as ntappadm through ssh or directly at the server console.
2. At the password prompt, type the password for ntappadm.
3. Insert the Application Bundle DVD-ROM.

   Note:

   For advanced users: As an alternative to installing the application bundle from the DVD-ROM, you can install the application bundle using an ISO image file. Prior to running the mcpInstaller script, you can download an ISO image file from the Avaya PLDS and transfer this file to EMServer1 in the directory `/var/mcp/extract/`. The script prompts you to select installing from either the ISO image file or from the optical drive.
4. Type `mcpInstaller`, and press **Enter**.
5. Type the password for ntappadm, and press **Enter**.
6. Type `y` to continue with the installation.
   The following prompt appears:

```
Searching for installation software...

The following application load instances have been found:

[1] /var/mcp/extract/
dvd_AAC_MCP_17.1.1.00_2013-10-18-1344_coreApps.iso

[2] Optical Drive

Please select which load instance you wish to install [1..2]:
```


Comments? infodev@avaya.com

7. Type the number of the staging file you want to use, and press **Enter**.
8. Complete the prompts, as shown in the following table:

Prompt	Response
`MCP load name`	Enter a load name. For example, MCP_17.0.5.0_2013_05_08-1638.
`EM IP Address (address of local host)`	Enter the IP address.
`EM Base Port (0-65535)`	Enter base port. For example, 12100.
`EM NE Name`	Enter the Network Element name. For example, EM.
`EM Instance (0 or 1)`	Enter 0 for EMServer1 or 1 for EMServer2.
`Please enter number [1 to <x>] of selection`	Enter the value that corresponds to your Engineering Configuration.
`Primary Database Host Address`	Enter the network IP address of EMServer1 (primary).
`Database Host Platform?`	Enter the database host platform. For example, linux
`DB NE name`	Enter the database Network Element name. For example, mcpdb
`Database Type (SINGLE/REPLICATED)?`	Type `Single` if your deployment is a co-resident simplex or standalone simplex configuration or `Replicated` if your deployment is a co-resident with redundancy or standalone with redundancy layout.
If you chose Replicated in the previous step, you see the prompt, `Secondary Database host address`	Type the network IP address of EMServer2 (secondary), and press **Enter**.
`Perform Database Backups (Y/N)`	Type `y` to backup database.
Verify the data and make corrections.	Type `y` to make corrections or `n` to continue.

9. At the prompt `Please enter the value for <tag name> [<default>]`, provide the information from the Avaya Aura® Conferencing Intelligent Workbook, and press **Enter**.

The list of tags for the various deployment layout types is shown in Populating tags on page 139.

10. At the prompt to verify the data and make any corrections, type `y`, and press **Enter**.
11. A summary of the installation parameters appears. Type `y` to accept and begin the installation or `n` to edit the information before installing, or **Control+C** to quit the installer.

Note:

This process can take greater than 30 minutes to complete.

Result

The message `Avaya Aura® Conferencing has been installed successfully on your system. You can access the EM Console via a web browser at https://<EMAddress>:<EMPort>` appears.

- Where EMAddress is the value you entered in Step 8 on page 137 for the installprops population.

AND

- Where EMPort is the value you entered in Step 8 on page 137 (EMPort + 21). For example, if you previously entered the IP address 192.168.150.130 and base Port is 12100, then you type in your browser: `https://192.168.150.130:12121`.

Next steps

For standalone configurations, proceed to Installing Avaya Media Server on page 134 to install Avaya Media Servers on the appropriate physical servers per the deployment configuration.

Related topics:

IP address table for Avaya Aura Conferencing deployment types on page 138
Populating tags on page 139
Checklist for verifying software versions on page 145

IP address table for Avaya Aura® Conferencing deployment types

Use the following table to assist in gathering the required number of IP addresses prior to running the mcpinstaller script.

Table 34: IP addresses for each server and deployment type

Deployment layout type	Basic Deployment	Additional Avaya Media Servers	Additional Web Conferencing Servers	Optional: Document Conversion Server
Co-resident with redundancy	10	1	2	1
Co-resident simplex	7	1	2	1
Standalone with redundancy	11	1	2	1
Standalone simplex	8	1	2	1
Co-resident with redundancy with DMZ	12	1	2	1
Co-resident simplex with DMZ	8	1	2	1

Populating tags

The following tables identify the parameters that are required to configure your specific deployment layout. Tags are used to enter configuration data such as IP address and hostname for all elements of a particular deployment layout. You are prompted to enter these tags after starting the mcpInstaller script on the initial install. The tags can also be manually modified by using the command **`populateTagsFile.pl –t <tag file name>`**. Prior to starting your installation, populate the tags in the Configuration Data tab of the Avaya Aura® Conferencing 7.2 Intelligent Workbook. The following tables contain the tag file names by deployment layout type.

Note:

To use single sign-on (SSO), the System Manager FQDN, Element Manager FQDN, and Provisioning Client FQDN (if required) must belong to the same root domain.

Co-resident with redundancy

Table 35: Tag population—Co-resident with redundancy

Installation properties and tag prompts	Property or tag name	Example value
IPv4 address of the System Manager	TAG_SMGR1_SVR_ADDR	192.168.100.1
Asset/Signaling IP address of Session Manager	TAG_ASM1_SVR_ADDR	192.168.100.2
Internal OAM (Default) IPv4 address of the secondary Element Manager server	TAG_EM_SVR2_INT_OAM_ADDR	192.168.100.3
Service IPv4 address of Element Manager	TAG_EM_INT_OAM_SVC_ADDR	192.168.100.4
Service IPv4 address of Accounting Manager	TAG_AM1_INT_OAM_SVC_ADDR	192.168.100.5
Service IPv4 address of Application Server	TAG_AS1_INT_OAM_SVC_ADDR	192.168.100.6
Media IPv4 address of the primary Avaya Media Server	TAG_EM_SVR1_MEDIA_ADDR	192.168.100.7
Media IPv4 address of the secondary Avaya Media Server	TAG_EM_SVR2_MEDIA_ADDR	192.168.100.8
Service IPv4 address of the primary Web Conferencing Server	TAG_WCS1_SVC_ADDR	192.168.100.9
Service IPv4 address of the secondary Web Conferencing Server	TAG_WCS2_SVC_ADDR	192.168.100.10
Site Name of the Avaya Aura® Conferencing installation.	TAG_SITE_NAME	Belleville
Site Long Name of the Avaya Aura® Conferencing installation.	TAG_SITE_LONG_NAME	

Co-resident simplex

Table 36: Tag population—Co-resident simplex

Installation properties and tag prompts	Property or tag name	Value
IPv4 address of the System Manager	TAG_SMGR1_SVR_ADDR	192.168.100.1
Asset/Signaling IP address of Session Manager	TAG_ASM1_SVR_ADDR	192.168.100.2
Service IPv4 address of Element Manager	TAG_EM_INT_OAM_SVC_ADDR	192.168.100.3
Service IPv4 address of Accounting Manager	TAG_AM1_INT_OAM_SVC_ADDR	192.168.100.4
Service IPv4 address of Application Server	TAG_AS1_INT_OAM_SVC_ADDR	192.168.100.5
Media IPv4 address of the primary Avaya Media Server	TAG_EM_SVR1_MEDIA_ADDR	192.168.100.6
Service IPv4 address of the primary Web Conferencing Server	TAG_WCS1_SVC_ADDR	192.168.100.7
Site Name of the Avaya Aura® Conferencing installation.	TAG_SITE_NAME	Belleville
Site Long Name of the Avaya Aura® Conferencing installation.	TAG_SITE_LONG_NAME	

Standalone with redundancy

Table 37: Tag population—Standalone with redundancy

Installation properties and tag prompts	Property or tag name	Example value
IPv4 address of the System Manager	TAG_SMGR1_SVR_ADDR	192.168.100.1
Asset/Signaling IP address of Session Manager	TAG_ASM1_SVR_ADDR	192.168.100.2
IPv4 address of the primary Avaya Media Server	TAG_MS1_SVR1_INT_OAM_ADDR	192.168.100.3

Installation properties and tag prompts	Property or tag name	Example value
Internal OAM (Default) IPv4 address of the secondary Element Manager server	TAG_EM_SVR2_INT_OAM_ADDR	192.168.100.4
Service IPv4 address of Element Manager	TAG_EM_INT_OAM_SVC_ADDR	192.168.100.5
Service IPv4 address of Accounting Manager	TAG_AM1_INT_OAM_SVC_ADDR	192.168.100.6
Service IPv4 address of Application Server	TAG_AS1_INT_OAM_SVC_ADDR	192.168.100.7
IPv4 address of the primary Web Conferencing Server	TAG_WC_SVR1_ADDR	192.168.100.8
Service IPv4 address of the primary Web Conferencing Server	TAG_WCS1_SVC_ADDR	192.168.100.9
IPv4 address of the secondary Web Conferencing Server	TAG_WC_SVR2_ADDR	192.168.100.10
Service IPv4 address of the secondary Web Conferencing Server	TAG_WCS2_SVC_ADDR	192.168.100.11
Site Name of the Avaya Aura® Conferencing installation.	TAG_SITE_NAME	Belleville
Site Long Name of the Avaya Aura® Conferencing installation.	TAG_SITE_LONG_NAME	

Standalone simplex

Table 38: Tag population—Standalone simplex

Installation properties and tag prompts	Property or tag name	Value
IPv4 address of the System Manager	TAG_SMGR1_SVR_ADDR	192.168.100.1
Asset/Signaling IP address of Session Manager	TAG_ASM1_SVR_ADDR	192.168.100.2

Installation properties and tag prompts	Property or tag name	Value
IPv4 address of the primary Avaya Media Server	TAG_MS1_SVR1_INT_OAM_ADDR	192.168.100.3
Service IPv4 address of Element Manager	TAG_EM_INT_OAM_SVC_ADDR	192.168.100.4
Service IPv4 address of Accounting Manager	TAG_AM1_INT_OAM_SVC_ADDR	192.168.100.5
Service IPv4 address of Application Server	TAG_AS1_INT_OAM_SVC_ADDR	192.168.100.6
IPv4 address of the primary Web Conferencing Server	TAG_WC_SVR1_ADDR	192.168.100.7
Service IPv4 address of the primary Web Conferencing Server	TAG_WCS1_SVC_ADDR	192.168.100.8
Site Name of the Avaya Aura® Conferencing installation.	TAG_SITE_NAME	Belleville
Site Long Name of the Avaya Aura® Conferencing installation.	TAG_SITE_LONG_NAME	

Co-resident with redundancy with DMZ

Table 39: Tag population—Co-resident with redundancy with DMZ

Installation properties and tag prompts	Property or tag name	Example value
IPv4 address of the System Manager	TAG_SMGR1_SVR_ADDR	192.168.100.1
Asset/Signaling IP address of Session Manager	TAG_ASM1_SVR_ADDR	192.168.100.2
Internal OAM (Default) IPv4 address of the secondary Element Manager server	TAG_EM_SVR2_INT_OAM_ADDR	192.168.100.3
Service IPv4 address of Element Manager	TAG_EM_INT_OAM_SVC_ADDR	192.168.100.4
Service IPv4 address of Accounting Manager	TAG_AM1_INT_OAM_SVC_ADDR	192.168.100.5

Installation properties and tag prompts	Property or tag name	Example value
Service IPv4 address of Application Server	TAG_AS1_INT_OAM_SVC_ADDR	192.168.100.6
Media IPv4 address of the primary Avaya Media Server	TAG_EM_SVR1_MEDIA_ADDR	192.168.100.7
Media IPv4 address of the secondary Avaya Media Server	TAG_EM_SVR2_MEDIA_ADDR	192.168.100.8
IPv4 address of the primary Web Conferencing Server typically located in a DMZ to support external access	TAG_DMZ_WC_SVR1_ADDR	192.168.100.9
Service IPv4 address of the primary Web Conferencing Server typically located in a DMZ to support external access	TAG_DMZ_WCS1_SVC_ADDR	192.168.100.10
IPv4 address of the secondary Web Conferencing Server typically located in a DMZ to support external access	TAG_DMZ_WC_SVR2_ADDR	192.168.100.11
Service IPv4 address of the secondary Web Conferencing Server typically located in a DMZ to support external access	TAG_DMZ_WCS2_SVC_ADDR	192.168.100.12
Site Name of the Avaya Aura® Conferencing installation.	TAG_SITE_NAME	Belleville
Site Long Name of the Avaya Aura® Conferencing installation.	TAG_SITE_LONG_NAME	

Co-resident simplex with DMZ

Table 40: Tag population—Co-resident simplex with DMZ

Installation properties and tag prompts	Property or tag name	Value
IPv4 address of the System Manager	TAG_SMGR1_SVR_ADDR	192.168.100.1
Asset/Signaling IP address of Session Manager	TAG_ASM1_SVR_ADDR	192.168.100.2
Service IPv4 address of Element Manager	TAG_EM_INT_OAM_SVC_ADDR	192.168.100.3
Service IPv4 address of Accounting Manager	TAG_AM1_INT_OAM_SVC_ADDR	192.168.100.4
Service IPv4 address of Application Server	TAG_AS1_INT_OAM_SVC_ADDR	192.168.100.5
Media IPv4 address of the primary Avaya Media Server	TAG_EM_SVR1_MEDIA_ADDR	192.168.100.6
IPv4 address of the primary Web Conferencing Server typically located in a DMZ to support external access	TAG_DMZ_WC_SVR1_ADDR	192.168.100.7
Service IPv4 address of the primary Web Conferencing Server typically located in a DMZ to support external access	TAG_DMZ_WCS1_SVC_ADDR	192.168.100.8
Site Name of the Avaya Aura® Conferencing installation.	TAG_SITE_NAME	Belleville
Site Long Name of the Avaya Aura® Conferencing installation.	TAG_SITE_LONG_NAME	

Checklist for verifying software versions

Use the following checklist to verify the software installation.

#	Task	Description	Notes	✔
1	Verify the Linux operating system.	1. Log on as `ntappadm` to the primary Element Manager server (EMServer1). 2. Type `mcpRelease.pl`, and press **Enter**. 3. Verify the value in the Release Level with the output. For example, MCP OS 17.0 with patch level 24 shows: `Release Level: 17.0.24`		
2	Verify the database software.	1. Log on as `ntdbadm` to the primary Element Manager server (EMServer1). 2. Type `/opt/mcp/db/bin/dbRelease.pl`, and press **Enter**. 3. Verify the DB version and DB patch values in the output. For example, if you installed database version 9.0.6.11, the output displays: `DB_version = 9.0.6 DB_patch = 11`		
3	Verify the application software.	Log on to Element Manager Console using a Web browser at https://<EMAddress>:<EMPort+1>. The currently installed application software version appears in the window title. For example, `MCP_17.0.6.0_2015-05-01-2201`.		
4	Verify the Avaya Media Server platform software.	**Note:** This procedure only works if the Avaya Media Server platform is installed.		

#	Task	Description	Notes	✔
		1. Log on as `ntappadm` to the primary Element Manager server (EMServer1). 2. Type **`cat /etc/mcpms.properties`**. 3. Check the value of installer.dir property. For example, you see `installer.dir=/var/mcp/loads/MCP_MediaServer_7.5.0.441_2011.10.08_97/` for the Avaya Media Server installer MCP_MediaServer_7.5.0.441_2001.10.08_97.zip.		

Accessing Element Manager Console using local login

There are two ways to log on to the Element Manager Console:

- locally (as described in this procedure)
- single sign-on access through Avaya Aura® System Manager

Note:

To configure single sign-on, see the chapter for Configuring single sign-on for Element Manager Console and Provisioning Client.

About this task

Use this procedure to log on to the Element Manager Console for the first time.

Procedure

1. On the management PC, open the browser.
2. In the Address box, enter the following address: `http://<IP address>:12120`.

   where *<IP address>* is the EM Internal OAM Service IP address. (This is the logical IP address of the server running Element Manager Console.)
3. Press **Enter**.

A Web page appears displaying the IP address you entered and the link **Launch Element Manager Console**.

4. On the <IP address> page, click **Launch Element Manager Console**.
5. From the IPv4 Service Address box on the Element Manager Console window, select the IP address of the server running Element Manager Console.
6. Click **Connect**.
7. In the Element Manager Authentication window, click the **Accept the certificate for this session only** option button.
8. Click **Apply**.
   A connection is established to the active Element Manager instance.
9. In the UserID box on the Element Manager Console window, enter `admin`.
10. In the Current Password box, enter `admin`.
11. Click **Ok**.
    The Element Manager Console window appears. It is normal to see one major alarm displayed. (An orange alarm appears below the tool bar and displays `Major: 1`.) This alarm appears because the secondary instance (EM_1) of the Element Manager network element is not deployed or running. (The `Peer presumed failed` alarm is generated against the Element Manager network element.)

    Note:

    If you have a co-resident simplex or standalone simplex deployment, this alarm does not appear.

12. Verify the `Peer presumed failed` alarm:
    a. In the navigation pane of the Element Manager Console, click **Servers**.
    b. Click the Element Manager server name to highlight the row.
    c. Click **Logical View**.
    d. In the Logical View window, expand the **Element Manager** folder, and click **Element Manager_0**.
    e. Click **Alarm Browser** on the bottom left of the window.
       The Alarm Browser window for Element Manager_0 appears. This window displays the `Peer presumed failed` alarm.
    f. Click the AlarmName `Peer presumed failed` to view the alarm details.

       Note:

       If the alarm description specifies a reason other than the EM_1 instance not running, contact the Avaya support Web site at http://support.avaya.com to open a service request.
    g. Close the Alarm Browser and Logical View windows.

Next steps

Proceed to the next chapter for installing the Avaya Aura® Conferencing license key.

Chapter 7: Installing the Avaya Aura® Conferencing license key

Installing the Avaya Aura® Conferencing license key on Avaya Aura® System Manager

About this task

License keys are installed on the WebLM server, which resides with Avaya Aura® System Manager. WebLM has a client/server model where many clients share the same WebLM server and also the same license key. The license key is an XML file.

Use the following procedure to install the Avaya Aura® Conferencing license key on Avaya Aura® System Manager.

Procedure

1. In the Address box of the Web browser, enter the following address: `http://<SMGR OAM FQDN>`.
2. In the User ID field, enter your System Manager logon ID.
3. In the Password field, enter your password.
4. Click **Log On**.
5. In the Services area of the System Manager home page, click **Licenses**.
6. In the navigation pane, click **Install license**.
7. On the Install license page, click **Browse**.
8. In the Choose File to Upload dialog box, select the license file, and click **Open**.
9. Click **Install**.
10. In the navigation pane, click **Conferencing** to view information about the license.

Chapter 8: Configuring Transport Layer Security

Checklist for configuring Transport Layer Security

The following checklist provides a high-level view of the tasks involved in configuring Transport Layer Security (TLS).

#	Task	Description	Notes	✔
1	Review the guidelines for certificate configuration.	See Guidelines for certificate configuration on page 156.		
2	Retrieve the CA certificate for the System Manager Certificate Authority and add to the Web browser trusted certificate store.	See Adding the System Manager CA certificate to the Administrator Internet Explorer browser on page 158. **OR** See Adding the System Manager CA certificate to the administrator Firefox browser on page 159.		
3	Create an administrator End Entity on the System Manager so the administrator can view the Session Detail Record Browser and the Key Performance Indicator for the Avaya Media Server,	See Creating an administrator End Entity for identity certificates from on page 160.		

#	Task	Description	Notes	✔
4	Install an administrator identity certificate on the adminstrator browser.	For Internet Explorer, see Installing an administrator identity certificate on the administrator Internet Explorer Web browser on page 161. For Firefox, see Installing an administrator identity certificate on the administrator Firefox Web browser on page 162.		
5	Obtain the enrollment password.	See Obtaining enrollment password from System Manager on page 165.		
6	Create X.509 Certificates for all the network elements that require certificates for securing management and signaling traffic to either the System Manager or the System Manager for components such as Application Server, Element Manager, Avaya Media Server, and the Provisioning Manager.	See Creating Network Element certificates signed by System Manager on page 165.		
7	Import certificates signed by a Certificate Authority other than the System Manager CA into a PKCS#12 file for importing to the keystore.	See Importing certificates from a third party CA on page 167.		

#	Task	Description	Notes	✔
8	Import Certificate Authority certificates signed by a Certificate Authority other than the System Manager CA.	See Importing CA certificates from a third party CA on page 168.		
9	Assign a certificate to the Element Manager.	See Assigning a certificate to the Element Manager on page 169.		
10	Assign a certificate to the Provisioning Manager.	See Assigning a certificate to the Provisioning Manager on page 171.		
11	For co-resident with redundancy or co-resident simplex deployments: Assign a certificate to the Personal Agent Manager.	See Assigning a certificate to the Personal Agent Manager on page 172		
12	Assign a certificate to the Application Server.	See Assigning a certificate to the Application Server on page 173.		
13	Assign certificates for each Avaya Media Server.	See Assigning certificates to the Avaya Media Servers on page 174.		
14	Assign a certificate to the Web Conferencing Server.	See Assigning a certificate to the Web Conferencing Server on page 175.		
15	Assign a certificate to the Web Conferencing Management Server.	See Assigning a certificate to the Web Conferencing Management Server on page 176.		

Introduction to Transport Layer Security

Avaya Aura® Conferencing uses the Transport Layer Security (TLS) protocol to prevent eavesdropping and tampering of communications sent across a network. The TLS protocol (Version 1.0) is comprised of two layers: the TLS Handshake protocol and the TLS Record protocol. The TLS Handshake protocol allows the server and client to authenticate each other using X.509 certificates and to negotiate an encryption algorithm and cryptographic keys. Authentication of either the client or server makes use of a Public Key Infrastructure (PKI). The TLS Handshake protocol uses the Public Key Infrastructure (PKI) for authentication. The use of the X.509 certificate is an integral part of the PKI. An X.509 certificate includes the public key of the server and general information that is pertinent to the owner (such as name and organization) in the subject Distinguished Name (DN) field of the certificate. The Common Name (CN) attribute of the DN identifies some unique name of the end-entity the certificate represents. For example, the CN can represent a Web server address such as CN=wcs1.domain.com. In addition, an independent Certificate Authority (CA) digitally signs each certificate. Any entity that has a copy of the CA certificate can use the CA certificate to validate the signature on the signed certificate. The TLS Record protocol performs symmetric cryptographic encryption and message integrity checks on the message payload.

Guidelines for certificate configuration

The CA that is used to sign certificates and the requirements for the common name of the certificates, for each Network Element interface, is shown in the following table. The Network Elements that require certificates to be signed by the System Manager CA can also be signed by another CA instead, for example, an intermediate enterprise CA. In this situation, the System Manager CA is configured as an intermediate CA of an enterprise CA.

For information about the elements that run on each server, see Server components on page 43.

Important:

If the System Manager CA is mentioned, there must be a trust relationship between that Network Element and the System Manager.

Note:

If TLS is enabled for the SIP interfaces, TLS must be enabled on each of the SIP interfaces, as shown in the following table. Avaya recommends that you deploy the system with TLS

enabled but it is not mandatory. However, TLS is always required for the HTTPS and OAM interfaces.

Table 41: Guidelines for certificates

Network Element interface	Certificate Authority	Logical Name	Common Name	Example (Common Name)
EM Internal OAM	System Manager CA	EMIntOAMCert	FQDN of Element Manager service address	emsrv.domain.com
EM External OAM	N/A	N/A	N/A	N/A
Prov Internal OAM HTTPS	System Manager CA	Prov1IntOAMCert	FQDN of server address	prov1.domain.com
Prov External OAM HTTPS	N/A	N/A	N/A	N/A
Prov/PA SIP	System Manager CA	PA1SIPCert	IP address of server address	192.168.10.10
PA HTTPS	Enterprise/ Public CA	PA1Cert	FQDN of server address	aac.domain.com
PA SIP	System Manager CA	PA2SIPCert	IP address of server address	192.168.10.11
AS SIP	System Manager CA	ASSIPCert	IP address of service address	192.168.10.12
Media Server SIP[1]	System Manager CA	AMS1Cert	IP address of server address	192.168.10.13
Media Server SOAP[1]	System Manager CA	AMS1Cert	IP address of server address	192.168.10.13
WCMS	System Manager CA	WCMS1Cert	IP address of server address	192.168.10.14
WCS External HTTPS	Enterprise/ Public CA	WCS1Cert	FQDN of service address	wcs1.domain.com
DCS	Enterprise/ Public CA	N/A	FQDN of server address	dcs1.domain.com

[1] For co-resident deployments, the media IP address only handles media traffic. The main IP address of the server handles the SIP and HTTP(S) traffic. As a result, the certificate for SIP/SOAP traffic must use the server's IP address and not the media IP address.

Adding the System Manager CA certificate to the Administrator Internet Explorer browser

The Certificate Authority (CA) certificate used on the System Manager CA must be installed in the Web browser trusted certificate store for the administrator in order to prevent security warning dialogs appearing while managing the system.

Note:

If you use Firefox as your browser, skip this section and proceed to Adding the System Manager CA certificate to the administrator Firefox browser on page 159.

About this task

Use the following procedure to retrieve the CA certificate for the System Manager Certificate Authority for installation on the Internet Explorer browser for the administrator.

Procedure

1. Log on to System Manager.
2. On the System Manager console, click **Services** > **Security**.
3. In the navigation pane, click **Certificates** > **Authority**.
4. On the CA Functions page, click **Download to Internet Explorer**.
5. Click **Save**.
6. Select a location on your computer, and click **Save**.
7. Click **Open**.
8. Click **Install Certificate**.
9. In the Welcome to the Certificate Import Wizard dialog box, click **Next**.
10. In the Certificate Store dialog box, click **Place all certificates in the following store**.
11. Click **Browse**, and select **Trusted Root Certification Authorities**, and click **OK**.
12. Click **Next**.
13. In the Completing the Certificate Import Wizard, click **Finish**.
14. In the Security Warning dialog box, click **Yes** to install the certificate.
15. Click **OK**.
16. Click **OK**.

Result

The CA certificate is installed in the Windows Trusted Root Certificate Authorities store.

Next steps

Proceed to adding the System Manager CA certificate to the administrator Firefox browser.

Adding the System Manager CA certificate to the administrator Firefox browser

The Certificate Authority (CA) certificate used on the System Manager CA must be installed in the Web browser trusted certificate store for the administrator in order to prevent security warning dialogs appearing while managing the system.

Note:

If you use Internet Explorer as your browser, skip this section and proceed to Adding the System Manager CA certificate to the Administrator Internet Explorer browser on page 158.

About this task

Use the following procedure to retrieve the CA certificate for the System Manager Certificate Authority for installation on the Firefox browser for the administrator.

Procedure

1. Log on to System Manager.
2. On the System Manager console, click **Services** > **Security**.
3. In the navigation pane, click **Certificates** > **Authority**.
4. On the CA Functions page, click **Download to Netscape**.
5. Select the check box, **Trust this CA to identify web sites**.
6. Click **OK**.

Result

The CA certificate is installed in the Firefox certificate authority database.

Next steps

Proceed to obtaining enrollment password from the System Manager.

Creating an administrator End Entity for identity certificates from System Manager

An identity certificate is required on the administrator Web browser for an administrator to view the Session Detail Record Browser and Key Performance Indicators for the Avaya Media Server and to download logs from the Avaya Media Server. You must define an End Entity for the administrator on the System Manager before the administrator can request an identity certificate from the System Manager.

About this task

Use the following procedure to provision an End Entity for an identity certificate for an administrator Web browser signed by the System Manager.

Procedure

1. Log on to System Manager.
2. Click **Services** > **Security**.
3. In the navigation pane, click **Certificates** > **Authority**.
4. In the navigation pane, click **Add End Entity**.
5. In the Add End Entity window, complete the following fields:
   - **End Entity Profile**: Select **OUTBOUND_TLS** from the list.
   - **Username**: Enter the user name for the specific administrator. For example, admin.
   - **Password**: Enter a password for the administrator. Use this password when creating the certificate.
   - **Confirm Password**: Type the password again.
   - **Email**: Type the email address of the administrator. For example, admin@mail.example-enterprise.com.
   - **CN, Common Name**: Enter the userID for the specific administrator. For example, admin.
   - **OU, Organization Unit**: Keep the default value. This value is based on the profile.
   - **O, Organization**: Keep the default value. This value is based on the profile.
   - **C, Country (ISO 3166)**: Keep the default value. This value is based on the profile.
   - **Certificate Profile**: Select **ID_CLIENT** from the list.
   - **CA**: Keep the default value. This value is based on the profile.

- **Token**: Select **User Generated** from the list.

6. Click **Add End Entity**.
7. Repeat this procedure for each administrator that requires access to the Session Detail Record Browser and Key Performance Indicators interfaces.

Next steps

As determined by your Web browser, proceed to either Installing administrator identity certificate on the administrator Internet Explorer Web browser or Installing administrator identity certificate on the administrator Firefox Web browser.

Installing an administrator identity certificate on the administrator Internet Explorer Web browser

Before you begin

- A new End Entity has been created for the administrator. See Creating an Administrator End Entity for identity certificates from System Manager.
- The username and password created for the end entity has been provided to the administrator.

Note:

If you use Firefox as your browser, skip this procedure and proceed to Installing an administrator identity certificate on the administrator Firefox Web browser.

About this task

Use the following procedure to install the administrator identity certificate on the administrator Internet Explorer Web browser.

Note:

You can create only one identity certificate for each username. If you use more than one computer or use both Firefox and Internet Explorer, then export the identity certificate and private key from the respective browser and install the identity certificate on the other computer or browser.

Procedure

1. Log on to System Manager.
2. Click **Services** > **Security**.
3. In the navigation pane, click **Certificates** > **Authority**.
4. In the navigation pane, click **Public Web**.

5. In the navigation pane of the new browser window or tab, click **Create Browser Certificate**.
6. Type the Username and password, and click **OK**.
7. If the Web Access Confirmation dialog box appears, click **Yes** to allow the operation.
8. In the **Options** panel, click **OK**.
9. In the Creating a new RSA signature key dialog box, click **OK**.
10. In the VBScript: Certificate Management dialog box, click **OK**.
11. Close the browser window.

Result

The identity certificate is installed on the Administrator Web browser.

Installing an administrator identity certificate on the administrator Firefox Web browser

Before you begin

- A new End Entity has been created for the administrator. See Creating an Administrator End Entity for identity certificates from System Manager.
- The username and password created for the end entity has been provided to the administrator.

Note:

If you use Internet Explorer as your browser, skip this procedure and proceed to Installing an administrator identity certificate on the administrator Internet Explorer Web browser.

About this task

Use the following procedure to install the administrator identity certificate on the administrator Firefox Web browser.

Note:

You can create only one identity certificate for each username. If you use more than one computer or use both Firefox and Internet Explorer, then export the identity certificate and private key from the respective browser and install the identity certificate on the other computer or browser.

Procedure

1. Log on to System Manager.
2. Click **Services** > **Security**.
3. In the navigation pane, click **Certificates** > **Authority**.
4. In the navigation pane, click **Public Web**.
5. In the navigation pane of the new browser window or tab, click **Create Browser Certificate**.
6. Type the Username and password, and click **OK**.
7. In the Options panel, click **OK**.
8. In the Alert dialog box, click **OK** to acknowledge that a new certificate has been installed.
9. Close the browser window or tab.

Result

The identity certificate is installed in the Administrator Web browser.

Installing an administrator identity certificate on the Element Manager Console

Before you begin

- You must have installed the administrator identity certificate on the administrator Web browser.
- You must have the following:
  - A PCKS#12 file that contains the signed certificate and key
  - The PCKS#12 file is accessible on the workstation where you launch Element Manager Console
  - The password used to access the contents of the PCKS#12 file

Note:

You can export the certificate and key as a PCKS#12 file from either the Internet Explorer or Firefox browsers.

Procedure

1. In the Address box of the Web browser, enter the following address:`https://<FQDN>:12121`
   where *<FQDN>* is the EM Internal OAM Service fully qualified domain name.
2. Press **Enter**.
   A Web page appears displaying the FQDN you entered and the link **Launch Element Manager Console**.
3. On the <FQDN> page, click **Launch Element Manager Console**.
4. From the IPv4 Service Address box on the Element Manager Console window, select the IP address of the server running Element Manager.
5. Click **Advanced**.
6. In the Advanced Connection Configuration dialog box, click the **Key Store Certificates** tab.
7. Click **Add**.
8. In the PCKS#12 File dialog box, click **Browse**.
9. In the Select PKCS#12 File dialog box, select the PCKS#12 file that contains the signed certificate and private key, and then click **Open**.
10. In the Password box in the PCKS#12 File dialog box, type the password used to protect the PCKS#12 file.
11. In the Export Password box, type the password used to protect the PCKS#12 file.
12. Click **Apply**.
13. In the Advanced Configuration Connection dialog box, click **OK**.
14. In the Element Manager Console window, click **Connect**.

Related topics:

Creating an administrator End Entity for identity certificates from System Manager on page 160
Assigning certificates to the Avaya Media Servers on page 174

Obtaining enrollment password from System Manager

The trust management services enables autoenrollment for certificates from System Manager. You are required to know the enrollment password when requesting certificates from the System Manager. If you already know the enrollment password, you can skip this procedure.

About this task

Use the following procedure to obtain the enrollment password.

Procedure

1. Log on to System Manager.
2. On the System Manager console, click **Services** > **Security**.
3. In the navigation pane, click **Certificates**.
4. Click **Enrollment Password**.
5. On the Enrollment Password screen, in the Existing Password field, record the password for use in the following procedure.
6. On the Security tab, click **x** to close the Security window.

Next steps

Proceed to Creating Network Element certificates signed by the System Manager.

Creating Network Element certificates signed by System Manager

The System Manager can be used on your network as a Certificate Signing Authority for Network Elements that require certificates to establish trust with the System Manager. This trust relationship is required in order for the System Manager to push subscriber data down to the Avaya Aura® Conferencing Network Elements and also for using single sign-on (SSO) for administrative access. Integration with the System Manager Trust Management service allows certificate enrollment for certificates issued by the System Manager to the Avaya Aura® Conferencing components directly from the Avaya Aura® Conferencing Element Manager.

Before you begin

You must know the enrollment password as completed in Obtaining enrollment password from System Manager on page 165.

About this task

Use the following procedure to create X.509 Certificates for all the Network Elements that require certificates for securing management and signaling traffic to either the System Manager or the Session Manager for components such as Application Server, Element Manager, Avaya Media Server, and the Provisioning Manager.

Procedure

1. In the Address box of the Web browser, enter the following address:`https://<IP address>:12121`

   where *<IP address>* is the EM Internal OAM Service IP address. (This is the logical IP address of the server running Element Manager Console.)
2. Press **Enter**.
   A Web page appears displaying the IP address you entered and the link **Launch Element Manager Console**.
3. On the <IP address> page, click **Launch Element Manager Console**.
4. From the IPv4 Service Address box on the Element Manager Console window, select the IP address of the server running Element Manager.
5. Click **Connect**.
6. On the Element Manager Authentication window, click the **Accept the certificate for this session only** option button.
7. Click **Apply**.
   A connection is established to the active element manager (EM) instance.
8. In the UserID box on the Element Manager Console window, enter `admin`.
9. In the Current Password box, enter `admin`.
10. Click **Ok**.
11. In the navigation pane of Element Manager Console, click **Security** > **Certificate Management** > **Enrollment Request**.
12. In the Certificate Enrollment window, complete the following fields:
    - **Logical Name**: Type a logical name for the certificate to be assigned to a specific managed network element, for example, EMIntOAMCert.
    - **Bit length**: Select 1024, 2048, or 4096 from the list. If your security policy does not specify bit length, select **1024**.
    - **Common name**: Type the FQDN or IP address, see Guidelines for certificate configuration on page 156 to determine if the Network Element requires an IP address or FQDN.
    - **Enrollment password**: This password must match the current Enrollment Password that is configured on System Manager.
13. Click **Submit**.

Note:

If you are making a certificate enrollment request for the first time, a Warning dialog box appears as the Element Manager cannot validate the certificate of the enrollment server. In the Warning: CA Authentication dialog box, click **Apply** to install the CA certificate into the Element Manager trust store. Future certificate requests are automatically authenticated against the trust store.

14. Repeat this procedure for each network element that uses the System Manager as the Certificate Signing Authority, as shown in Table 41: Guidelines for certificates on page 157.

Result

The certificate is automatically installed on the Element Manager Keystore.

Note:

Prior to certificate expiry, Avaya recommends that you generate a new certificate using a new logical name and then refresh the certificate by changing the network element to use the new logical name. The expired certificate can then be removed from the Element Manager Keystore.

Next steps

After you have completed creating network element certificates for each network element that uses System Manager as the Certificate Signing Authority, return to the Checklist for configuring Transport Layer Security on page 153.

Importing certificates from a third party CA

Use this procedure when Network Elements require certificates signed by a Certificate Authority other than the System Manager CA. These certificates are acquired from a third party CA, for example, VeriSign or your enterprise CA. The benefit of using certificates signed by a third party CA is that the signing CA is usually already installed on most Web browsers. This allows users to access the various Web components of the system without having to handle browser security warnings or to figure out how to install the appropriate CA certificates onto your clients. The certificate and the private key for the certificate must be contained in a PKCS#12 file when importing the certificate into the Keystore.

Important:

Some client devices do not function properly when the required CA certificates are not configured in the client trust store. If you are using a client device that is not directly supported by the enterprise, Avaya recommends that you use a well-known trusted Certificate Authority.

For a list of Certificate Authorities that Microsoft and Mozilla preconfigure in their solutions, see http://technet.microsoft.com and search for `root certificate members list` or http://www.mozilla.org and search for `certificate authority`.

Before you begin

You must have the following:

- A PKCS#12 file that contains the signed certificate and private key.
- The PKCS#12 file is accessible on the workstation where you launch the Element Manager Console.
- The password used to access the contents of the file.

Note:

For information about creating the PKCS#12 file, see the appendix about Using OpenSSL for Certificate Signing Requests.

About this task

Use the following procedure to import certificates from a third party CA.

Procedure

1. Log on to Element Manager Console.
2. In the navigation pane, click **Security**, **Certificate Management**.
3. Click **Keystore**.
4. In the Keystore window, click **Add (+)**.
5. In the Add PKCS#12 File dialog box, complete the following fields:
   - **Logical Name**: Type a logical name for the certificate to be assigned to a specific managed network element, for example, PA1Cert.
   - **PKCS#12 File**: Click **Browse** and select the PCKS#12 file that contains the certificate key pair to import.
   - **Password**: Type the password used to protect the PKCS#12 file.
   - **Export Password**: Type the password used to protect the PKCS#12 file.
6. Click **Apply**.

Next steps

Proceed to Importing CA Certificates from a third party CA.

Importing CA certificates from a third party CA

If any Network Element uses certificates signed by a CA other than the System Manager CA, the CA root certificate and any intermediate certificates for that CA are required to be in the

Avaya Aura® Conferencing Element Manager Truststore to ensure authentication of the signatures on the certificates. Privacy Enhanced Mail (PEM) Base64 encoded DER or the binary DER file formats are supported. The format is one of the following filename extensions: .pem, .cer, .crt, or .der.

Before you begin

You must have the CA certificates in one of the previously mentioned formats that is accessible from the server where you launch the Element Manager Console.

About this task

Use the following procedure to add an X.509 certificates to the Element Manager Truststore.

Procedure

1. Log on to the Element Manager Console.
2. In the navigation pane of Element Manager Console, select **Security > Certificate Management > Truststore**.
3. In the Truststore window, click **Add (+)**.
4. In the Select File dialog box, select the file containing the certificate you wish to import into the Truststore.
5. Click **Open**.
6. Click **OK**.
7. Repeat this procedure for any additional CA certificates that are required.

Next steps

Proceed to Assigning a certificate to the Element Manager.

Assigning a certificate to the Element Manager

Before you begin

- A certificate for the Element Manager must exist in the Element Manager Keystore, as completed in the previous procedure for Creating Network Element certificates signed by System Manager on page 165.
- Single sign-on from the System Manager to the Element Manager Console requires that the certificate has the FQDN of the EM Service address as the Common Name of the certificate.
- The certificate has been signed by a CA that the System Manager trusts. This is typically the System Manager CA.

About this task

Use the following procedure to assign a certificate to the Element Manager.

Procedure

1. Log on to the Element Manager Console.
2. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager**.
3. In the Element Manager window, select the element manager.
4. Click **Edit (-/+)**.
5. In the Edit Element Manager dialog box, complete the following:
   - **Enable HTTP Port**: Clear this check box.
   - **Internal OAM – HTTPS Certificate**: Select the required HTTPS certificate by logical name, for example, EMIntOAMCert.
6. Click **Apply**.
7. Click **File** > **Exit** on the Element Manager Console to exit.
8. Log on to EMServer1 as `ntappadm` through SSH or directly at the server console.
9. At the password prompt, type the password for ntappadm.
10. Type `emStop.pl`, and press **Enter**.
11. Type `emStart.pl`, and press **Enter**.
12. Log on to the Element Manager Console.
    a. When the Element Manager Authentication Dialog window appears, select **Store the certificate's authority as a trusted certificate for this and future connections**.
    b. Click **Apply**.

Next steps

Proceed to assigning a certificate to the Provisioning Manager.

Assigning a certificate to the Provisioning Manager

Before you begin

- A certificate for the Provisioning Manager must exist in the Element Manager Keystore.
- Single sign-on from the System Manager to the Provisioning Manager requires that the certificate has the FQDN of the server hosting the Provisioning Manager as the Common Name.
- The certificate has been signed by a CA that the System Manager trusts. This is typically the System Manager CA.

About this task

Use the following procedure to assign a certificate to the Provisioning Managers.

Procedure

1. Log on to the Element Manager Console.
2. In the navigation pane of Element Manager Console, select **Feature Server Elements > Provisioning Managers**.
3. In the Provisioning Managers window, select the **PROV1**.
4. Click **Edit (-/+)**.
5. In the Edit PROV1 dialog box, complete the following fields:

   In the Prov section:

   - **Enable HTTP Port**: Clear the check box.
   - **Internal OAM HTTPS Certificate**: Select the required HTTPS certificate by logical name, for example, Prov1IntOAMCert.

   In the PA section:

   - **Enable HTTP Port**: Clear the check box.
   - **HTTPS Certificate**: Select the required HTTPS certificate by logical name, for example, PA1Cert.
   - **Enable SIP TLS Port**: Select this check box to enable it if setting up a system where SIP TLS is used.

     Note:

     If this is enabled, it must also be enabled for the Application Server.
   - **SIP Certificate**: Select the required SIP certificate by logical name, for example, PA1SIPCert.

Note:

The certificates in the PA submenus are required only when the PA is co-hosted with the Provisioning Manager.

6. Click **Apply**.
7. Repeat this procedure for any additional Provisioning Managers.

Next steps

Proceed to assigning a certificate to the Personal Agent Manager.

Assigning a certificate to the Personal Agent Manager

Note:

This procedure is specific to standalone with redundancy and standalone simplex deployments. If you have a co-resident with redundancy or co-resident simplex deployment, you can skip this procedure.

The standalone with redundancy deployment layouts make use of independent Personal Agent Manager Network Elements to provide support for physical separation from the Provisioning Manager Network Element for security and scalability.

Before you begin

Certificates for the Personal Agent Manager must exist in the Element Manager Keystore.

About this task

Use the following procedure to assign a certificate to the Personal Agent Manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Personal Agent**.
2. In the Personal Agent Managers window, select **PA1**.
3. Click **Edit (-/+)**.
4. In the Edit Personal Agent dialog box, complete the following fields:
   - **Enable HTTP Port**: Clear the check box.
   - **PA HTTPS Certificate**: Select the required HTTPS certificate by logical name, for example, PA1Cert.
   - **Enable SIP TLS Port**: Select this check box to enable it if setting up a system where SIP TLS is used.

Note:

If this is enabled, it must also be enabled for the Application Server.

- **SIP Certificate**: Select the required SIP certificate by logical name, for example, PA1SIPCert.

5. Click **Apply**.

Next steps

Proceed to Assigning a certificate to the Application Server.

Assigning a certificate to the Application Server

Before you begin

- A certificate for the Application Server must exist in the Element Manager Keystore.
- The certificate has been signed by a CA that the System Manager trusts. This is typically the System Manager CA.

About this task

Use the following procedure to assign a certificate to the Application Server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Application Servers**.
2. In the Application Servers window, select **AS1**.
3. Click **Edit (-/+)**.
4. In the Edit Application Server dialog box, complete the following fields:
   - **Enable SIP TLS**: Select this check box to enable if you are setting up a system where SIP TLS is used.

     Note:

     If SIP TLS is enabled, it must also be enabled for the Session Manager, Provisioning Managers, Personal Agent Managers, and the Avaya Media Servers.

   - **SIP Certificate**: Select the required SIP certificate from the list. This list corresponds to the logical names in the Keystore, for example, ASSIPCert.
5. Click **Apply**.

Next steps

Proceed to Assigning certificates to the Avaya Media Servers.

Assigning certificates to the Avaya Media Servers

Before you begin

- A certificate for each Avaya Media Server must exist in the Element Manager Keystore.
- The certificate has been signed by a CA that the System Manager trusts. This is typically the System Manager CA.

About this task

Use the following procedure to assign a certificate the Avaya Media Server.

Procedure

1. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers**.
2. In the Media Servers window, select **MS1**.
3. Click **Edit (-/+)**.
4. In the Edit Media Server dialog box, complete the following fields:
   - **Enable SIP TLS**: Select this check box to enable if you are setting up a system where SIP TLS is used.

     Note:

     If SIP TLS is enabled, it must also be enabled for the Application Server.
   - **SIP Certificate**: Select the required SIP certificate from the list. This list corresponds to the logical names in the Keystore, for example, AMS1Cert.
   - **Enable SOAP/TLS**: Select this check box to enable it.
   - **SOAP Certificate**: Select the appropriate certificate from the list. This list corresponds to the logical names in the Keystore. The preceding SIP certificate can be used, for example, AMS1Cert.
5. Click **Apply**.
6. In the navigation pane of the Element Manager Console, click **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers** > <*Media Server Element Name*> > **Configuration Parameters**.
7. Select **TLSAuth** from the **Parm Group** list.
8. Change the value for **EnforceTLSMutualAuthForHTTPS** to **true**.

If you set **EnforceTLSMutualAuthForHTTPS** to **true**, you must also:

- Generate an administrator identity for the server running the Element Manager Console. This certificate should be signed by a Certificate Authority which is in the trusted store in Element Manager. For more information, see Creating an administrator End Entity for identity certificates from System Manager on page 160.
- Import or 'install' the administrator identity certificate on the Element Manager Console. For more information, see Installing an administrator identity certificate on the Element Manager Console on page 163.
- Add the generated keystore or 'install the administrator identity certificate' on your browser. For more information, see Installing an administrator identity certificate on the administrator Firefox Web browser on page 162 or Installing an administrator identity certificate on the administrator Internet Explorer Web browser on page 161.

9. Close the Media Server Configuration Parameters dialog box.
10. Repeat this procedure for any additional Avaya Media Servers.

Next steps

Proceed to Assigning a certificate to the Web Conferencing Server.

Assigning a certificate to the Web Conferencing Server

Before you begin

A certificate with a common name using the FQDN of the Web Conferencing Server must exist in the Element Manager Keystore.

About this task

Use the following procedure to assign a certificate to the Web Conferencing Server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Servers**.
2. In the Web Conferencing Server window, select **WCS1**.
3. Click **Edit (-/+)**.
4. In the Edit Web Conferencing Server dialog box, complete the following fields:
   - **Enable HTTP Port**: Clear this check box.

- **HTTPS External Certificate**: Select the required HTTPS certificate by logical name, for example, WCS1Cert.

5. Click **Apply**.
6. Repeat this procedure for any additional Web Conferencing Servers.

Next steps

Proceed to Assigning a certificate to the Web Conferencing Management Server.

Assigning a certificate to the Web Conferencing Management Server

Before you begin

- A certificate for the Web Conferencing Management Server must exist in the Element Manager Keystore.
- The certificate has been signed by a CA that the System Manager trusts. This is typically the System Manager CA.

About this task

Use the following procedure to assign a certificate to the Web Conferencing Management Server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Management Servers**.
2. In the Web Conferencing Manager Servers window, select **WCMS1**.
3. Click **Edit (-/+)**.
4. In the Edit Web Conferencing Manager Server dialog box, complete the following fields:
   - **Enable HTTP Port**: If enabled, clear this check box to disable.
   - **HTTPS Certificate**: Select the required certificate from the list. This list corresponds to the logical names in the Keystore, for example, WCMS1Cert.
5. Click **Apply**.

Next steps

Proceed to the next chapter.

Chapter 9: Configuring Avaya Media Servers and clusters

Adding additional Avaya Media Server hosts

Before you begin

Install the Avaya Media Server software on a server. For more information, see Installing Avaya Media Server on page 134.

About this task

Use this procedure if you want to add expansion Avaya Media Servers.

Procedure

1. In the navigation pane of Element Manager Console, select **Addresses**.
2. In the Addresses window, click **Add (+)**.
3. In the Add IPv4 Address dialog box, enter the logical name and IP address for the server on which the Avaya Media Server software is installed.
4. Click **Apply**.
5. In the navigation pane of Element Manager Console, select **Servers**.
6. In the Servers window, click **Add (+)**.
7. In the Add Server dialog box, complete the following fields:
   - **Short Name**
   - **Long Server Name**
   - **Internal OAM (Default) Address**: Enter the IP address you specified in Step 3.
   - **Operating System**: Select **linux**.
   - **Host Name**: Enter the short name or FQDN of the server.
8. Click **Apply**.

Next steps

Proceed to Adding an Avaya Media Server network element on page 178.

Adding an Avaya Media Server network element

About this task

Use the following procedure to add an Avaya Media Server network element.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers**.
2. In the Media Servers window, click **Add (+)**.
3. In the Add Media Server dialog box, complete the following fields:
   - **Short Name**
   - **Long Name**
   - **Base Port**: Type `49000`.
   - **Enable SIP TCP**: Select this check box to enable SIP TCP.

     OR

     Enable SIP TLS: Select this check box to enable SIP TLS.
   - **SIP Certificate**: If SIP TLS is enabled, select the certificate you want to use for SIP TLS. For more information, see the chapter for Configuring Transport Layer Security.

   Note:

   Accept the default for all other fields.
4. Click **Apply**.
5. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers** > **<media server you specified in Step 3> Instance**.
6. In the Media Server Instance window, click **Add (+)**.
7. In the Add Media Server Instance dialog box, complete the following fields:
   - **Server**: Select the media server you created in Step 3.
   - **Load or Patch**: Select the software load.
   - **Engineering**: Select the configuration that corresponds to your hardware type and layout.

8. Click **Apply**.

Next steps

Proceed to Adding an additional Avaya Media Server to an existing media server cluster on page 179.

Adding an additional Avaya Media Server to an existing media server cluster

About this task

Use the following procedure to add an additional Avaya Media Server to an existing media server cluster.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters**.
2. In the Media Servers Clusters window, select the media server cluster to which you want to add the Media Server.
3. Click **Edit (-/+)**.
4. In the Edit Media Server Cluster dialog box, specify whether the Media Server you are adding to the cluster is a secondary server (if the cluster has only one Media Server) or a standard media server (if the cluster already has a secondary Media Server).

   Note:

   A media server cluster supports a maximum of eight media servers:

   - one primary
   - one secondary
   - six standard servers

5. Click **Apply**.

Next steps

Proceed to Creating a new Media Server cluster on page 180.

Creating a new Media Server cluster

About this task

Use the following procedure to create a new Media Server cluster.

Note:

A Media Server cluster supports a maximum of eight Media Servers:

- one primary
- one secondary
- six standard servers

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters**.
2. In the Media Server Clusters window, click **Add (+)**.
3. In the Add Media Server Cluster dialog box, complete the following fields:
   - **Short Name**
   - **Long Name**
   - **Primary Server**: Select the Avaya Media Server network element. This list contains only the media server network elements that do not belong to any cluster. You must specify a primary server.
   - **Secondary Server**: If this cluster has two or more Avaya Media Servers, you must specify a secondary server. Otherwise, leave this field blank.
   - **Standard Media Servers**: If the cluster has three or more Avaya Media Servers, add more standard media servers. In the Available box, select the Media Servers you want to add, and then click **>>**.
4. Click **Apply**.

Chapter 10: Configuring Web Conferencing components

Configuration procedure for the Web conferencing server components

The following table provides a high-level view of the tasks involved in configuring the Web conferencing components.

#	Task	Description	Notes	✔
1	Deploy the WCMS instances but do not start these instances.	See Deploying and starting the Web conferencing management Network Elements on page 219.		
2	Setup Rsync.	See Adding a Web Conferencing Management Server Rsync user account on page 184.		
3	Start the Web Conferencing Management Server instances.	See Deploying and starting the Web conferencing management Network Elements on page 219.		

Note:

Avaya recommends that you implement DNS lookup to synchronize domain names and IP addresses for the Avaya Aura® Conferencing solution. If your deployment does not support DNS lookup, see DNS and Avaya Aura Conferencing on page 589.

Configuring the meeting event processor for the Web conferencing management server

About this task

Use the following procedure to configure the meeting event processor.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Management Servers > <*Web conferencing management server name*> > Meeting Event Processing**.
2. From the Meeting Event Processor box, select the Provisioning Manager or Personal Agent for managing meeting events.
3. Click **Apply**.

Next steps

Proceed to configuring the default Web Conferencing Server group or return to the Checklist for configuring the Web conferencing server components on page 181 to determine where you are in the process.

Configuring the default Web Conferencing Server group

About this task

Use the following procedure to configure the default Web Conferencing Server group that is used in Web collaboration for users who do not have a location.

Procedure

1. Log on to the Element Manager Console as an administrator.
2. In the navigation pane, click **Feature Server Elements** > **Web Conferencing** > **Default Web Conference Server Group**.
3. In the Default Web Conferencing Server Group dialog box, complete the following fields:

- **Primary Web Conferencing Server**:
  - For co-resident with redundancy and standalone with redundancy configurations: type **WCS1**, and press **Enter**.
  - For co-resident simplex and standalone simplex configurations: type **WCS1**, and press **Enter**.
- **Secondary Web Conferencing Server**:
  - For co-resident with redundancy and standalone with redundancy configurations: type **WCS2**, and press **Enter**.
  - For co-resident simplex and standalone simplex configurations: Leave this field as <none>.
- **Document Conversion Server**: Select a Document Conversion Server if one exists or leave this field as <none>.

4. Click **Apply**.

   The validation process begins. You receive an error message if the primary and secondary servers are configured with the same server name or you have configured the secondary server field without having first configured the primary server.

Result

The default Web Conferencing Server group is now configured.

Next steps

Proceed to configuring the Web Conferencing Management Server rsync or return to the Checklist for configuring the Web conferencing server components on page 181 to determine where you are in the process.

Configuring Web Conferencing Management Server Rsync

This section provides information about creating a new rsyncappsw user, a Secure Shell (SSH) key, and transferring a copy of the SSH key to the server when multiple Web Collaboration Management Server (WCMS) instances are running.

Before you begin

- A Web Conferencing Management Server instance on each server must be deployed but not started. The following procedures refer to the servers as ServerA and ServerB.

Note:

ServerA is the server where the WCMS1 instance is configured and ServerB is the server where the WCMS2 instance is configured.

- You are able to log on using the ntsysadm account or an account with the SA role assigned.

Related topics:

Adding a Web Conferencing Management Server Rsync user account on page 184
Generating an SSH user key on page 185
Copying the SSH key on page 185

Adding a Web Conferencing Management Server Rsync user account

Procedure

1. Log on to the server through ssh as ntsysadm or an account with the SA role assigned.
2. Type **`userMgt`**, and press **Enter**.
3. Type `1`, and press **Enter** to add new user.
4. At the prompt to enter a username, type `rsyncappsw`, and press **Enter**.
5. At the prompt to enter a user ID (between 1000 and 10000), type a number or press **Enter** to have the system select an ID for you.
6. Type `5` to select the AA role, and press **Enter**.
7. Type `y`, and press **Enter** to continue.
8. At the prompt to Enter a new password, type a password, for example, `ZAQ12wsx`, and press **Enter**.
9. At the prompt to add another user, press **Enter** to skip adding another user.
10. Press **Enter** to exit the userMgt tool.
11. Type `sudo chage --maxdays -1 rsyncappsw`, and press **Enter**.

Next steps

Proceed to generating a user key or return to the Checklist for configuring the Web conferencing server components on page 181 to determine where you are in the process..

Generating an SSH user key

Procedure

1. Type `cd /var/mcp/run/MCP_17.0/<WCMS1_0>/bin`, and press **Enter** to go to the WCMS instance runtime bin directory.
   Where: WCMS1_0 is Server A and WCMS2_0 is Server B.
2. Type **`sudo -u rsyncappsw ./genSSHUserKeys.sh`**, and press **Enter**.
   A new key is generated.
3. Type **`sudo su - rsyncappsw`**, and press **Enter**.
4. Type **`passwd`**, and press **Enter**.
5. Type the old password, as entered in the preceding procedure, for example `ZAQ12wsx`, and press **Enter**.
6. Type a new password at the prompt, and press **Enter**.
7. Retype the new password at the prompt, and press **Enter**.
8. Log on to ServerB through ssh as `ntsysadm` or an account with the SA role assigned
9. Repeat the steps in Adding a Web Conferencing Management Server Rsync user account on page 184 and Generating an SSH user key on page 185 for ServerB.

Result

A new key is generated for ServerA and ServerB.

Next steps

Proceed to transferring a copy of the SSH key or return to the Checklist for configuring the Web conferencing server components on page 181 to determine where you are in the process.

Copying the SSH key

About this task

Transfer a copy of the SSH key to the servers where the WCMS instances are running.

Procedure

1. Log on to ServerA through ssh as `ntsysadm` or an account with the SA role assigned.

2. Type **sudo -u rsyncappsw ssh-copy-id -i /home/rsyncappsw/.ssh/id_rsa.pub <ServerB_IP>**, and press **Enter**.
   The following prompt appears:

   ```
   Are you sure you want to continue connecting (yes/no)?
   ```

3. Type `y` and press **Enter**.
4. At the prompt to enter a password, type the password that you specified when you generated the SSH user key, and press **Enter**.
   The command succeeded if you see `Now try logging into the machine, with "ssh '<IP address>'", and check in:`

   `.ssh/authorized_keys`

   `to make sure we haven't added extra keys that you weren't expecting.`
5. Enter **userMgt**, and press **Enter**.
6. Type `4`, and press **Enter**.
7. Type the number that corresponds to the rsyncappsw user, and press **Enter**.
8. Type **y**, and press **Enter**.
9. Press **Enter** to accept No as the default.
10. Type `8`, and press **Enter**.
11. Log off ServerA.
12. Log on to ServerB through ssh as `ntsysadm` or an account with the SA role assigned.
13. Repeat Step 2 on page 186 and replace <ServerB_IP> with <ServerA_IP> and continue through to Step 10 on page 186.
14. Log off ServerB.

Next steps

Return to step 9 in the Checklist for configuring the Web conferencing server components on page 181.

Migrating to and from a DMZ

In a co-resident deployment, the Avaya Aura® Conferencing components are deployed on the Element Manager servers. If you wish to offer Web collaboration features to participants outside of the enterprise, you must move the Web Conferencing components to a separate server in the Demilitarized Zone (DMZ). In other words, you must migrate from a co-resident

simplex layout to a co-resident simplex with DMZ layout or from a co-resident with redundancy layout to a co-resident with redundancy with DMZ layout. You can also perform the reverse move from a DMZ deployment to one without a DMZ.

Related topics:

Enterprise DMZ deployment on page 62
Checklist for migrating to a DMZ on page 187
Migrating the Web Conference Server to the DMZ on page 188
Migrating the Web Conference Server from the DMZ on page 190
Moving the Web Conferencing Management Server (WCMS) to the enterprise on page 433

Checklist for migrating to a DMZ

The following table provides a high-level view of the tasks involved in migrating to a DMZ.

#	Task	Description	Notes	✔
1	Ensure that you have the appropriate hardware configuration required for this deployment.	See Co-resident simplex with DMZ layout on page 56 or Co-resident with redundancy with DMZ layout on page 53.		
2	Install the appropriate software on the DMZ server. Ensure that you apply the appropriate patches.	See Installing the AAC Platform on page 116. **Important:** The Installing Linux procedure guides you through the installation process with links to individual procedures. Upon completion of each step, return to the next step in the Installing Linux procedure by clicking the link at the end of each individual procedure.		

#	Task	Description	Notes	✔
3	Configure the firewall rules on the DMZ server.	For information about the port matrix, go to http://support.avaya.com and download the latest version of the Avaya Aura® Conferencing 7.2 Port Matrix.		
4	Configure the access control list on the DMZ server.	See Configuring the access control list on page 376.		
5	Migrate the Web conferencing components from the Element Manager servers in the enterprise to the separate servers, located in the DMZ.	See Migrating the web conference server to the DMZ on page 188.		

Migrating the Web Conference Server to the DMZ

About this task

If you have a co-resident deployment, use this task to move the Web Conferencing components from the Element Manager server to a separate server located in the DMZ. If your co-resident deployment has redundancy, perform all of the steps for one Element Manager server and Web Conferencing server and then perform the steps for the second Element Manager server and Web Conferencing server.

Procedure

1. Stop all instances of the Web Conferencing Management Server (WCMS), Web Conferencing Server (WCS), and Provisioning Management (PROV) network elements (NE).

   See Stopping a Network Element instance on page 472.

2. Undeploy the WCS NE instances.

   See Stopping and undeploying a network element instance on page 534.

3. Add the WCS OAM addresses:

   a. In the navigation pane of Element Manager Console, select **Addresses**.

b. In the Addresses window, click **Add (+)**.
c. In the Add IPv4 Address dialog box, complete the following fields:
   - **Logical Name**
   - **IPv4 Address**
d. Click **Apply**.
e. Click **Yes** to confirm.
f. Repeat this procedure for any additional WCS.

4. Change the WCS service addresses to the free IP addresses that belong to the WCS located in the DMZ.
   a. In the navigation pane of Element Manager Console, select **Addresses**.
   b. In the Addresses window, select the WCS service address and click **Edit (-/+)**.
   c. In the Edit IPv4 Address dialog box, change the IP address in the **IPv4 Address** field.
   d. Click **Apply**.
   e. Repeat this procedure for any additional WCS.
5. Add the WCS:
   a. In the navigation pane of Element Manager Console, select **Servers**.
   b. In the Servers window, click **Add (+)**.
   c. In the Add Server dialog box, complete the following fields:
      - **Short Name**
      - **Long Server Name**
      - **IPv4 Internal OAM (Default) Address**: Enter the IP address you specified in Step 3.
      - **Operating System**: Select **linux**.
   d. Click **Apply**.
   e. Repeat this procedure for any additional WCS.
6. Change the servers for the WCS NE instances to Web Conferencing servers.

   For example, in a co-resident simplex (without redundancy) deployment, change the WCS NE instance to WCServer1.
   a. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Servers** > **<WCS NE>** > **Instance**.
   b. In the <WCS> Instance dialog box, select the WCS NE instance.
   c. Click **Edit (-/+)**.
   d. In the Edit <WCS> Instance dialog box, select the WCS from the **Server** list.
   e. Click **Apply**.
   f. Repeat this procedure for any additional WCS.
7. Add Personal Agent Network Element (PA NE) instances.

a. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Personal Agent Managers** > **<PA NE>** > **Instance**.
b. In the <PA NE> Instance dialog box, click **Add (+)**.
c. Select the Web Conferencing server and click **Apply**.
d. Repeat this procedure for any additional WCS.

8. Deploy the WCS and PA NE instances.

   See Deploying a Network Element instance on page 493.

9. Ensure that the WCS Service address is in the same subnet as the WC servers.
10. Change the certificates configured for WCS and PA NEs in accordance with Guidelines for certificate configuration on page 156.

    See Introduction to Transport Layer Security on page 156.

11. Start all stopped Web Conferencing Management Server (WCMS), Web Conferencing Server (WCS), Personal Agent (PA) and Provisioning Management (PROV) Network Element instances.

    See *Deploying and starting the remaining Network Elements*.

Migrating the Web Conference Server from the DMZ

About this task

If you have a co-resident deployment, use this task to move the Web Conferencing components from a separate server located in the DMZ to the Element Manager server. If your co-resident deployment has redundancy, perform all of the steps for one Element Manager server and Web Conferencing server and then perform the steps for the second Element Manager server and Web Conferencing server.

Procedure

1. Stop all instances of the Web Conferencing Management Server (WCMS), Web Conferencing Server (WCS), Personal Agent (PA) and Provisioning Management (PROV) network elements (NE).

   See Stopping a Network Element instance on page 472.

2. Undeploy the WCS NE instances.

   See Stopping and undeploying a network element instance on page 534.

3. Change the servers for the WCS NE instances to Element Manager servers.

   For example, in a co-resident simplex (without redundancy) deployment, change the WCS NE instance to WCServer1.

a. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Servers** > **<WCS NE>** > **Instance**.
b. In the <WCS> Instance dialog box, select the WCS NE instance.
c. Click **Edit (-/+)**.
d. In the Edit <WCS> Instance dialog box, select the Element Manager server from the **Server** list.
e. Click **Apply**.
f. Repeat this procedure for any additional WCS.

4. Delete the Personal Agent Network Element (PA NE) instances.
   a. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Collaboration Agent Managers (Personal Agent Managers)** > **<PA NE>** > **Instance**.
   b. In the <PA NE> Instance dialog box, click **Delete (-)**.
   c. Click **Yes** to confirm.
   d. Repeat this procedure for any additional WCS.
5. Ensure that the WCS Service address is in the same subnet as the EM servers.
6. Change the certificates configured for WCS in accordance with Guidelines for certificate configuration on page 156.

   See Automated security.
7. Start all stopped Web Conferencing Management Server (WCMS), Web Conferencing Server (WCS), Personal Agent (PA) and Provisioning Management (PROV) Network Element instances.

   See Deploying and starting the remaining network elements on page 209.

Chapter 11: Installing and configuring the Document Conversion Server

The Document Conversion Server and the Microsoft Office® operating system

You must install the Microsoft Office Professional 2013 operating system before you install the Document Conversion Server (DCS). This requirement is due to changes made in the Microsoft activation process for the 2013 version. These changes mean that the licensing is not available outside of the United States and Canada through the Avaya distribution process. As a result, the Microsoft Office Professional 2013 operating system can no longer be shipped with the DCS. One benefit of this separation is that customers have greater flexibility to provide their own security settings on the Microsoft Windows server. Additionally, customers may choose to deploy the DCS on their own hardware, as long as it meets with the Avaya requirements.

Introduction to installing and configuring the Document Conversion Server

This chapter outlines the process involved in installing and configuring the Document Conversion Server for every Avaya Aura® Conferencing Windows server.

Prerequisites

- The following components are required for converting documents on the Document Conversion Server for use in your Web conferencing sessions:
  - Microsoft Windows server 2008 R2 operating system
  - Microsoft Office 2010 or 2013 is required to convert Microsoft Office documents
  - Microsoft Visual C++ 2008 Redistributable
  - FQDN of the Document Conversion server Windows server
  - DNS routing for the Document Conversion Server FQDN
  - Document Conversion Server Access Key: A six-digit number.

- SSL certificate for the Document Conversion Server Windows server FQDN/ hostname

- Open communication to the Windows server between the Document Conversion Server, the Web Conferencing Management Server (WCMS), and the Avaya Flare® Experience/ Collaboration Agent hosts to ensure the Document Conversion Server does not get blocked by your network or operating system firewall or proxies.
- Java 1.6 or later is required to run the Web Conferencing Document Conversion Server Web application.

Installation and configuration process

To install and configure the Document Conversion Server, you must perform the following steps:

1. Disable automatic installation of Microsoft Windows updates on the Microsoft Windows server where you will install the Document Conversion Server software. (This is the Document Conversion Server.) See Disabling automatic installation of Microsoft Windows updates on page 195.
2. Verify the Java version on the Document Conversion Server. See Verifying the Java version on page 195.
3. Configure the Java bin folder on the Document Conversion Server. See Configuring the Java bin folder through Windows on page 196.
4. Configure the SNMP service on the Document Conversion Server. See Configuring the SNMP service on page 197.
5. Activate the license for Microsoft Office 2013. See Activating Microsoft Office 2013 license on page 198.
6. Install Microsoft Visual C++ 2008 on the Document Conversion Server. See Installing Microsoft Visual C++ 2008 Redistributable on page 199.
7. Disable the macros in Microsoft Office. See Disabling macros in Microsoft Office on page 200.
8. Install the Document Conversion Server software. See Disabling macros in Microsoft Office on page 200.
9. Restrict access to the Document Conversion Server. See Restricting access to the Document Conversion Server on page 201.
10. Configure SSL/TLS on the Document Conversion Server. See Configuring SSL/TLS on the Document Conversion Server on page 202.
11. Start and stop the Document Conversion Server. See Starting and stopping the Document Conversion Server on page 204.
12. Configure the Document Conversion Server to start automatically. See Configuring the Document Conversion Server to start automatically on page 205.
13. Add the Document Conversion Server on Element Manager. See Adding the Document Conversion Server on Element Manager on page 205.

14. Configure the Document Conversion Server on Element Manager. See Configuring the Document Conversion Server on Element Manager on page 206.
15. Optional: Disable SSL/TLS on the Document Conversion Server. See Optional: Disabling SSL/TLS on the Document Conversion Server on page 207.

Disabling automatic installation of Microsoft Windows updates

About this task

Use this procedure to prevent Microsoft Windows updates from being automatically installed on the Document Conversion Server.

Procedure

1. On the Windows server, click **Start > Control Panel**.
2. In the Control Panel window, click **System and Security**.
3. In the System and Security window, click **Windows Update**.
4. In the navigation pane of the Windows Update window, click **Change settings**.
5. From the Important updates drop-down list box , select **Download updates but let me choose whether to install them** .
6. Click **OK**.

Next steps

Proceed to Verifying the Java version on page 195.

Verifying the Java version

About this task

Use this procedure to verify that Java version 1.6 or later (32- or 64-bit) is installed prior to installing the Document Conversion Server software on the Windows server.

Procedure

1. Click **Start**, and select **Run**.
   The Run window appears.
2. In the Open field, enter `cmd`, and click **OK**.

3. On the command-line interface (CLI), type `java -version` and press **Enter**.
   The Java version number appears.

   Note:

   Your Java version must be version 1.6 or later.

4. If you have an older Java version, download and install an updated version at http://www.java.com.

Next steps

Proceed to Configuring the Java bin folder through Windows on page 196.

Configuring the Java bin folder through Windows

About this task

Use the following procedure to configure the Java bin folder from the system path in Windows on the Document Conversion Server.

Procedure

1. Click **Start**, and select **Control Panel**.
2. Click **System**.
3. Click the **Advanced** tab or the **Advanced system settings** tab.
4. Click **Environment Variables**.
5. In the Environment Variables window, in the System Variables section, scroll through the list in the Variable column, and select *Path*.
6. Click **Edit**.
   The Edit System Variable window appears.
7. In the Variable value field, if the Java bin folder is not visible, append the filepath to the end of the current path. For example, `C:\Program Files\Java\jre7\bin`.

Next steps

Proceed to Configuring the SNMP service on page 197.

Configuring the SNMP service

About this task

Use this procedure to configure the SNMP service on the Document Conversion Server.

Procedure

1. On the Windows server, click **Start > Administrative Tools > Server Manager**.
2. In the Server Manager window, click **Features**.
3. In the Features section, expand **Features Summary**, and click **Add Features**.
4. In the Add Features Wizard window, click **SNMP Services**, and then click **Next**.
5. Click **Install**.
6. Restart the Windows server.
7. On the Windows server, click **Start > Administrative Tools > Server Manager**.
8. In the Server Manager window, click **Configuration > Services**.
9. Right-click **SNMP Service**, and select **Properties**.
10. In the SNMP Service Properties window, click the **Security** tab.
11. In the Accepted community names section on the Security tab, click **Add**.
12. From the Community rights drop-down list box, select **READ ONLY**.
13. In the Community Name box, enter the appropriate information. The default is `public`. You can configure this information via Element Manager Console.
14. Click **Add**.
15. On the Security tab, click **Accept SNMP packets from any host**.
16. Click **OK**.

Next steps

Proceed to Activating Microsoft Office 2013 license on page 198.

Activating Microsoft Office 2013 license

Before you begin

- You must have the Microsoft Office 2013 product key to proceed with the activation. Your product key is on the card from the box.
- You will need an Internet connection and preferably have the Enhanced Security Configuration Feature (IE ESC) disabled on Microsoft Internet Explorer.

Note:

You cannot activate Microsoft Office 2013 without the product key.

About this task

Use this procedure to activate Microsoft Office 2013 on the Document Conversion Server prior to installing the Document Conversion Server software.

Procedure

1. From the Start menu, select **All Programs > Microsoft Office**.
2. In the Now let's get started! window, click **Activate**.
3. In the Enter your product key window, enter the product key on the card from the box, and click **Continue**.
4. In the Add this key to an account window, click **Redeem Online**.
5. On the sign in page, perform one of the following steps:
   - If you have a Microsoft account, enter your login and password and click **Sign in**.
   - If you do not have a Microsoft account, click **Sign up** and create an account.
6. Select the appropriate settings from the Country and Language boxes, and then click **Continue**.
7. On the My Account page, click **Install**.
8. On the Welcome page, click **Next**.
9. On the First things first page, select the appropriate option, and click **Accept**.
10. On the Sign in page, perform one of the following steps:
    - If you want to sign in, click **Sign in**.
    - If you do not want to sign in at this time, click **No thanks, maybe later**.
11. On the Meet SkyDrive page, click **Next**.
12. On the We're getting things ready page, perform one of the following steps:

- If you want to see information about the new features in Office 2013, click **Take a look**.
- If you just want to proceed with the activation, click **No thanks**.

13. Wait for the activation to complete. When the activation is complete, the You're good to go page appears.
14. When the activation is complete, click **All done!**.
    Office 2013 is now installed and activated.

Next steps

Proceed to Installing Microsoft Visual C++ 2008 Redistributable on page 199.

Installing Microsoft Visual C++ 2008 Redistributable

Before you begin

If you have installed previous pre-release versions of Microsoft Visual C++ 2008 SP1 (such as Beta 1 or Community Technical Preview (CTP) builds), you must uninstall these versions via **Add/Remove Programs** in Control Panel before installing the final released version.

About this task

Use this procedure to install Microsoft Visual C++ 2008 Redistributable on the Document Conversion Server prior to installing the Document Conversion Server software.

Procedure

1. On the Windows server, navigate to the base directory of the Microsoft Visual C++ 2008 Redistributable software (that is, where the file **vcredist_x86.exe** is located).
2. Right-click the file **vcredist_x86.exe** and select **Run as administrator**.
3. In the Installation window, click **Next**.
4. Click the check box to accept the license terms, and then click **Install**.
5. When the installation is complete, click **Close** to close the Installation window.

Next steps

Proceed to Disabling macros in Microsoft Office on page 200.

Disabling macros in Microsoft Office

If macros are enabled on Microsoft Office documents, Avaya recommends that all macros be disabled for Microsoft Office Excel, PowerPoint, and Word to protect the Windows server running the Document Conversion Server software.

About this task

Use the following procedure to disable macros in the Trust Center for each Microsoft application being used by the Document Conversion Server.

Procedure

1. On the Windows server, open the application, for example, Microsoft Excel, PowerPoint, or Word.
2. Click the **Microsoft Office** icon.
3. Depending on the application, click one of the following:
   - Excel Options
   - PowerPoint Options
   - Word Options
4. In the Options navigation pane, click **Trust Center**.
5. Click **Trust Center Settings**.
6. Click **Disable all macros without notification.**
7. Click **OK**.
8. Click **OK** to close the Options window.

Next steps

Proceed to Installing the Document Conversion Server on page 200.

Installing the Document Conversion Server

Before you begin

Important:

Avaya recommends that you copy the Document Conversion Server software directly from the Application Bundle DVD-ROM or the PLDS Web site. If you copy the software to the

Document Conversion Server using a method that differs from the recommended approach, perform the following steps:

1. Right-click the zip file, click **Properties**.
2. On the **General** tab, in the Security section, click **Unblock**.
3. Click **Apply**.
4. Click **OK**.

About this task

Use the following procedure to install the Document Conversion Server.

Procedure

1. Insert the Application Bundle DVD-ROM on the Windows server.
2. Obtain the Document Conversion Server software from the core directory `/dcs/dcs_<version><date-time>.zip`. For example, dcs_MCP_17.0.0.1–2013–09–2200.zip.
3. Copy the zip file to `c:\` and extract the files.
4. Remove the read-only attribute on the dcs directory and apply these changes to the sub-directories.
5. Navigate to `c:\dcs`, type **`Setup DCS.bat`**, and press **Enter**.

Note:

If you encounter a problem determining Java and Microsoft Office installation, see the *Maintaining and Troubleshooting Avaya Aura® Conferencing* document.

Next steps

Proceed to Restricting access to the Document Conversion Server on page 201.

Restricting access to the Document Conversion Server

Before you begin

- If using hostnames instead of IP addresses, ensure that the FDQNs are DNS translatable.
- The addresses and hostnames in this list must belong to the servers where the Web Conferencing Management Server (WCMS) instances are running.

About this task

The Document Conversion Server is configured to allow all conversion requests from any Web Conferencing client by default. Use this procedure to configure an access key to restrict access

to the Document Conversion Server to only Web Conferencing installations with a specific key or hostname.

Procedure

1. Locate the Document Conversion Server configuration file **Config.php** in `<installed directory>/dcs/htdocs/app/Config.php`.
2. To restrict by access key, edit the access_key setting to a specific shared key, for example, **`self::$setting['access_key'] = "123456";`**.
3. To restrict by hostname, edit the access_host setting to a specific shared hostname, for example, **`self::$setting['access_host'] = array("127.0.0.1", "1.2.3.4");`**.

Note:

The access key in the Document Conversion Server configuration file must match the access key specified in the Document Conversion Server external node in Element Manager.

Result

You have restricted access to the Document Conversion Server for Web conferencing installations with a specific access key or hostname.

Next steps

Proceed to Configuring SSL/TLS on the Document Conversion Server on page 202.

Configuring SSL/TLS on the Document Conversion Server

Before you begin

You have obtained the following:

- A TLS (SSL) certificate from a trusted Certificate Authority, for example, Verisign or Entrust. This certificate is used against the host name/DNS of the Windows server.
- An SSL certificate, a private .key file, and a certificate chain file (.crt file).

Important:

Passphrase protection must be removed from the private key file. See Removing the passphrase key file on page 569.

For more information about obtaining SSL certificates from a trusted Certificate Authority, see the appendix for Using OpenSSL for Certificate Signing Requests.

Note:

The http/https ports must be opened on the Document Conversion Server for the client to access the server. The firewall settings must be adjusted or the firewall must be turned off.

About this task

Use the following procedure to configure TLS on the Document Conversion Server.

Procedure

1. In the root folder of the DCS installation directory, create a directory called certs.
2. Copy the SSL certificate file, the private .key file, and the certificate chain file (.crt) to the certs directory.
3. Stop the Document Conversion Server.
4. Save a backup to `<DCS installation directory>/dcs/conf/httpd.conf`.
5. Edit `<DCS installation directory>/dcs/conf/httpd.conf` as follows:
   a. Change the Listen directive at the beginning of the file to port 8443.
   b. Remove the **#** comment tag for **`#ServerName example.com:8443`**, and replace the DNS name for the certificate, the URL, and the port (this is the same as the Listen port).

      Note:

      This must match the Common Name (CN) field of the Subject Domain Name (DN) for the installed certificate.

   c. Remove the **#** comment tag for **`#LoadModule ssl_module modules/mod_ssl.so`** and append section <ifModule ssl_module>.

```
<ifModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
SSLEngine on
SSLCertificateFile "<path to certs directory>/<cert_name>.crt"
SSLCertificateKeyFile "<path to certs directory>/<cert_key>.key"
SSLCertificateChainFile "<path to certs directory>/
<cert_chain_file>.crt"
</IfModule>
```

   Where <path to certs directory> is the absolute path to the certs directory as created in Step 1. All three SSL files are part of the absolute path. The SSLCertificateKeyFile must be without passphrase; otherwise, Apache does not work with password-encrypted keys.

d. Type `<DCS installation directory>/dcs/Start DCS.bat` and press **Enter** to start the Document Conversion Server.

6. Verify that SSL is working. In your browser address field, type `https://<dns name>:<ssl port>/`, and press **Enter**.
   If you installed the SSL certificate successfully, the browser opens without security errors.

Next steps

Proceed to Starting and stopping the Document Conversion Server on page 204.

Starting and stopping the Document Conversion Server

About this task

Use the following commands to start or stop the Document Conversion Server.

Procedure

1. To start the Document Conversion Server, type `<DCS installation directory>/dcs/Start DCS.bat` and press **Enter**.

   Important:

   You must keep the command window open, otherwise the Document Conversion Server stops.

2. To stop the Document Conversion Server, perform one of the following steps:

   - Close the command window that opened when the Document Conversion Server started

     OR

   - Press **Control+C**, type **y**, and press **Enter** to stop.

Next steps

Proceed to Configuring the Document Conversion Server to start automatically on page 205.

Configuring the Document Conversion Server to start automatically

About this task

Use the following procedure to configure the Document Conversion Server for an automatic start.

Procedure

1. On the Windows taskbar, click **Start**.
2. Right-click on **All Programs**, and select **Open**.
   The Start menu window appears.
3. On the File menu, click **New** > **Shortcut**.
4. In the **Type the location of the item** field, type `<DCS installation directory>/dcs/Start DCS.bat`.
5. Click **Next**.
6. Click **Finish**.

Next steps

Proceed to Adding the Document Conversion Server on Element Manager on page 205.

Adding the Document Conversion Server on Element Manager

Before you begin

You must know the IP address of the Document Conversion Server.

About this task

Use this procedure to add the Document Conversion Server on Element Manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Addresses**.
2. In the Addresses window, click **Add (+)**.

3. In the Add IPv4 Address dialog box, enter the logical name and IP address for the Document Conversion Server.
4. Click **Apply**.
5. In the navigation pane of Element Manager Console, select **Servers**.
6. In the Servers window, click **Add (+)**.
7. In the Add Server dialog box, complete the following fields:
   - **Short Name**
   - **Long Server Name**
   - **IPv4 Internal OAM (Default) Address**: Enter the IP address you specified in Step 3.
   - **Operating System**: Select **windows**.
8. Click **Apply**.

Next steps

Proceed to Configuring the Document Conversion Server on Element Manager on page 206.

Configuring the Document Conversion Server on Element Manager

Before you begin

You have added a server for the Document Conversion Server on Element Manager. This server has a Windows operating system and an IPv4 Internal OAM (default) address. The IPv4 Internal OAM (default) address must be resolved by the DNS server to FQDN, which is the common name of the certificate for the Document Conversion Server.

About this task

Use the following procedure to configure the Document Conversion Server on Element Manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Document Conversion Servers**.
2. In the Document Conversion Servers window, click **Add (+)**.
3. In the Add Document Conversion Server dialog box, complete the following fields:
   - **Short name**: Type a short name, for example, DCS.

- **Long Name**: Type a long name, for example, DocumentConversionServer.
- **Server**: Select the server for the Document Conversion Server.
- **Protocol**: Select **HTTPS**.
- **Port**: Specify the HTTPS port number that you configured in the procedure for configuring SSL/TLS on the Document Conversion Server.
- **Relative URL**: Type a relative URL value.
- **Access Key**: Enter an alphanumeric value.

4. Click **Apply**.

Result

The Document Conversion Server appears in the list of Document Conversion Servers.

Optional: Disabling SSL/TLS on the Document Conversion Server

About this task

Use the following procedure to disable TLS (if required).

Note:

Avaya recommends that TLS always be enabled.

Procedure

1. Stop the Document Conversion Server by pressing **Control+C**, type **y**, and press **Enter** to stop.
2. Save a backup to `<DCS installation directory>\dcs\conf\httpd.conf`.
3. Edit the file `<DCS installation directory>\dcs\conf\httpd.conf` as follows:
   a. Change the Listen directive at the beginning of the file to port 8080.
   b. Update the port number against the FQDN/DNS name of the Document Conversion Server.
   c. Prefix the **#** comment tag to **`LoadModule ssl_module modules/mod_ssl.so`**
   d. Start the Document Conversion Server, type `<DCS installation directory>\dcs\Start DCS.bat` and press **Enter**.

4. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Web Conferencing** > **Document Conversion Servers**.
5. In the Document Conversion Servers window, click **Edit (-/+)**.
6. In the Edit Document Conversion Server dialog box, modify the protocol and port settings.
7. Click **Apply**.

Next steps

Deploy and start the remaining network elements.

Chapter 12: Deploying and starting the remaining Network Elements

Starting Server Monitors

About this task

The monitor service reports the following critical resource information about the server:

- CPU usage
- physical memory usage
- network I/O usage
- file system disk usage

Use this procedure to start the monitor service for each server in your configuration.

Procedure

1. In the navigation pane of Element Manager Console, select **Servers > <*Server name*> > Monitor**.
2. In the Server Monitor window, click **Start Monitor**.
   The following message appears at the bottom of the window: “The server monitor is running.”
3. Wait for the RAM, Disk, CPU, and Interface areas to become populated with data.

   Note:

   It is normal for alarms to be raised and then cleared as the system initializes. If any server monitoring alarms are not cleared, contact the Avaya support Web site at http://support.avaya.com to open a service request.
4. Repeat steps 1 through 3 for every server displayed in the Servers folder in Element Manager Console.

Next steps

Start the database monitors.

Starting Database Monitors

About this task

The monitor service reports the data replication status for the mcpdb database.

Procedure

1. In the navigation pane of the Element Manager Console, click **Feature Server Elements > Database > mcpdb > Monitor**.
2. In the mcpdb Monitor window, click the row containing **0** in the Instance Number column.
3. Click **Monitor**.
   The mcpdb_0 Database Instance Monitor window appears.
4. Click **Start Monitor**.
   The message `database instance monitor is running` appears at the bottom of the window.
5. Wait for the General Information and Database Process Status areas to update.

   Note:

   It is normal for alarms to be raised and then cleared as the system initializes. If any monitoring alarms are not cleared, contact the Avaya support Web site at http://support.avaya.com to open a service request.
6. Close the mcpdb _0 Database Instance Monitor window.
7. Repeat steps 2 through 6 for instance number 1 (if configured).
8. When finished, close the mcpdb Monitor window.

Deploying and starting secondary Element Manager Network Element

Element Manager is a component of Element Manager Console that manages all the network elements. For Avaya Aura® Conferencing to be operational, the Element Manager must be deployed and started.

Note:

If the Element Manager is not running, logs and alarms are spooled but conferencing services are available.

About this task

Use the following procedure to start and deploy Element Manager instance 1 for co-resident with redundancy and standalone with redundancy deployment layouts. If you have a co-resident simplex or a standalone simplex deployment type, you can skip this procedure and proceed to deploying and starting an Accounting Manager Network Element.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > NE Maintenance**.
2. In the Element Manager Maintenance dialog box, select the row for ID 1.
3. Click **Deploy**.
   The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.
4. Click **Start**.
   The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

   Check the state transitions for the following fields:

Field	Status
Maint	None
Admin	Online
Link	Up
Oper	Active or Hot Standby

Next steps

Deploy and start the accounting manager network elements.

Deploying and starting an Accounting Manager Network Element

Accounting Manager is a component of Element Manager Console that manages all the billing and accounting details.

About this task

Use the following procedure to deploy and start an Accounting Manager instance.

Procedure

1. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Accounting Managers** > **AM1** > **NE Maintenance**.
2. In the Accounting Manager Maintenance dialog box, select the row for ID 0.
3. Click **Deploy**.
   The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.
4. Click **Start**.
   The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

   Check the state transitions for the following fields:

Field	Status
Maint	None
Admin	Online
Link	Up
Oper	Active or Hot Standby

5. In the Accounting Manager Maintenance dialog box, select the row for ID 1, for non-simplex deployments.

   Note:

   If you have a co-resident simplex or standalone simplex deployment type, skip the remaining steps and proceed to deploying and starting a Provisioning Manager Network Element.

6. Click **Deploy**.

The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.

7. Click **Start**.
   The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

   Check the state transitions for the following fields:

Field	Status
Maint	None
Admin	Online
Link	Up
Oper	Active or Hot Standby

Next steps

Deploy and start the Provisioning Manager Network Elements.

Deploying and starting a Provisioning Manager Network Element

Provisioning Manager is a component of the Element Manager Console that manages configurational procedures.

About this task

Use the following procedure to deploy and start a Provisioning Manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Provisioning Managers** > <*Provisioning Manager name*> > **NE Maintenance** .
   Where *Provisioning Manager name* is Prov1.
2. In the Prov1 NE Maintenance dialog box, select the row for ID 0.
3. Click **Deploy**.
   The dialog box displays the status of the following fields:

Field	Status
Admin	Offline
Link	Down
Oper	Unavailable

4. Click **Start**.
   The dialog box displays the updated status of the following fields:

Field	Status
Admin	Online
Link	Up
Oper	Active

5. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Provisioning Managers** > <*Provisioning Manager name*> > **NE Maintenance** .
   Where *Provisioning Manager name* is Prov2.
6. In the Prov2 NE Maintenance dialog box, select the row for ID 0.
7. Click **Deploy**.
   The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.
8. Click **Start**.
   The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

   Check the state transitions for the following fields:

Field	Status
Maint	None
Admin	Online
Link	Up
Oper	Active

Next steps

Proceed to deploying and starting an Application Server Network Element.

Deploying and starting an Application Server Network Element

For co-resident with redundancy and standalone with redundancy configurations, you can configure failover capability.

About this task

Use the following procedure to deploy and start an Application Server Network Element.

Procedure

1. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Application Servers** > **AS1** > **NE Maintenance**.
2. In the Application Server Maintenance dialog box, select the row for ID 0.
3. Click **Deploy**.
   The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.
4. Click **Start**.
   The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

   Check the state transitions for the following fields:

Field	Status
Maint	None
Admin	Online
Link	Up
Oper	Active or Hot Standby

5. In the Application Server Maintenance dialog box, select the row for ID 1.

   Note:

   If you have a co-resident simplex or standalone simplex deployment, you can skip steps 5 through 7.

6. Click **Deploy**.
   The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.

7. Click **Start**.
   The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

   Check the state transitions for the following fields:

Field	Status
Maint	None
Admin	Online
Link	Up
Oper	Active or Hot Standby

Next steps

Proceed to enabling replication on the Avaya Media Server if you have two or more Avaya Media Servers in one Media Server cluster.

Enabling replication on the Avaya Media Server

If you have two or more Avaya Media Servers in one Media Server cluster, you must enable replication.

About this task

Use the following procedure to enable replication on the Avaya Media Server.

Procedure

1. On the Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Media Server Clusters** > <*Media Server cluster name*>.
2. Click **Replication Settings**.
3. In the Replication Settings dialog box, complete the following fields:
   - **Enable Replication Account**: Select the check box.
   - **User Name**: Type the User Name. Must be 6 to 8 characters in length.
   - **Password**: Type a password. Use the password rules as defined for Element Manager.
   - **Confirm**: Type the password again to confirm.

4. Click **Apply**.

Next steps

Proceed to Deploying and starting the Avaya Media Server Network Element.

Deploying and starting the Avaya Media Server Network Element

Each Avaya Media Server instance must be started for the instance and the cluster to which it is attached to be functional.

About this task

Use the following procedure to deploy and start an Avaya Media Server Network Element instance.

Procedure

1. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers** > <*Media Server name*> >**NE Maintenance**.
2. In the Media Server Maintenance dialog box, select the row for ID 0.
3. Click **Deploy**.
   The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.
4. Click **Start**.
   The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

   Check the state transitions for the following fields:

Field	Status
Maint	None
Admin	Online
Link	Up
Oper	Active

5. Repeat steps 2 through 4 for each additional Avaya Media Server.

Result

The deployment of Avaya Media Server Network Element is complete.

Next steps

Proceed to Deploying and starting the Web Conferencing Network Elements.

Deploying and starting the Web conferencing Network Elements

About this task

Use the following procedure to deploy and start the Web conferencing Network Elements.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Servers > <*Web conferencing server name*> > NE Maintenance**.
2. In the Web Conferencing Server Maintenance dialog box, select the row for ID 0.
3. Click **Deploy**.
   The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.
4. Click **Start**.
   The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

   Check the state transitions for the following fields:

Field	Status
Maint	None
Admin	Online
Link	Up
Oper	Active

Next steps

Proceed to Deploying and starting the Web Conferencing Management Network Elements.

Deploying and starting the Web conferencing management Network Elements

About this task

Use the following procedure to deploy and start the Web Conferencing Management Server network elements.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Management Servers** > <*Web conferencing management server name*> > **NE Maintenance**.
2. In the Web Conferencing Management Server Maintenance dialog box, select the row for ID 0.
3. Click **Deploy**.
   The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.
4. Click **Start**.
   The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

   Check the state transitions for the following fields:

Field	Status
Maint	None
Admin	Online
Link	Up
Oper	Active

Deploying and starting Personal Agent Network Elements

About this task

Use the following procedure to deploy and start the Personal Agent Network Elements.

Note:

If you have a co-resident with redundancy and co-resident simplex deployment, you can skip this procedure.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Personal Agent Managers** > <*Personal Agent name*> > **NE Maintenance**.
2. In the PA1 NE maintenance dialog box, select the row for ID 0.
3. Click **Deploy**.
   The dialog box displays the status of the following fields:

Field	Status
Admin	Offline
Link	Down
Oper	Unavailable

4. Click **Start**.
   The dialog box displays the updated status of the following fields:

Field	Status
Admin	Online
Link	Up
Oper	Active

Note:

If you have a standalone simplex deployment, skip the remaining steps.

5. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Personal Agent Managers** > **PA2**.
6. In the PA2 NE Maintenance dialog box, select the row for ID 0.
7. Click **Deploy**.
   The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.
8. Click **Start**.
   The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

Check the state transitions for the following fields:

Field	Status
Maint	None
Admin	Online
Link	Up
Oper	Active

Next steps

Proceed to verifying local access to the Provisioning Client.

Verifying local/emergency access to the Provisioning Client

Administrators usually log on to Provisioning Client through System Manager using single sign-on (SSO). However, in situations where single sign-on is not available, such as a network issue, you can use local/emergency access.

Before you begin

You must know the following:

- The IP address of EMServer1
- The IP address of EMServer2: for co-resident with redundancy and standalone with redundancy deployments only
- The FQDN of the Provisioning Server

Warning:

During local/emergency access, the administrator must be aware of the following:

- Additional expert mode privileges are granted which allow you to directly modify data which is usually controlled by System Manager.
- Where the expert mode warning appears, any changes made to these pages can cause synchronization issues between System Manager and Provisioning Client.

About this task

Use this procedure to verify local/emergency access to the Provisioning Client for Avaya Aura® Conferencing on EMServer1 and EMServer2.

Procedure

1. On your PC, open the browser.

2. In the Address box, enter the following address:
   `https://<FQDN>:8443/prov`
   where <*FQDN*> is the FQDN of EMServer1.
3. Press **Enter**.
4. Click **Continue to this website**.
   The Provisioning Client Login window appears.

   Note:

   If the Provisioning Client page does not appear, contact the Avaya support Web site at http://support.avaya.com to open a service request.
5. In the Username box on the Provisioning Client Login window, enter `admin`.
6. In the Password box, enter `admin`.
7. Click **Login**.
   The Welcome to the Provisioning Client page appears.
8. Click Logout.
   Complete the following steps if your deployment model supports a secondary Provisioning Manager.
9. In the Address box of the Web browser, enter the following address:
   `https://<FQDN>:8443/prov`
   where <*FQDN*> is the FQDN of EMServer2.
10. Press **Enter**.
11. Click **Continue to this website**.
    The Provisioning Client Login window appears.
12. In the Username box on the Provisioning Client Login window, enter `admin`.
13. In the Password box, enter `admin`.
14. Click **Login**.
    The Welcome to the Provisioning Client page appears.
15. Click **Logout**.

Next steps

Verify local access to Collaboration Agent.

Verifying local access to Collaboration Agent

Before you begin

You must know the IP address of:

- EMServer1
- EMServer2: for co-resident with redundancy and standalone with redundancy deployments only

About this task

Use this procedure to verify that you can access the Collaboration Agent Login window locally on EMServer1 and EMServer2.

Important:

You must provision at least one System Manager domain on the Avaya Aura® Conferencing system before you can access the Collaboration Agent.

Procedure

1. On your PC, open the browser.
2. In the Address field, enter the following address:
   `https://<FQDN>/aacpa`
   where <*FQDN*> is the FQDN of EMServer1.
3. Press **Enter**.
   The Avaya Aura® Conferencing Collaboration Agent Login window appears.

   Note:

   If the Avaya Aura® Conferencing Collaboration Agent Login window does not appear, contact the Avaya support Web site at http://support.avaya.com to open a service request.
4. Close the Avaya Aura® Conferencing Collaboration Agent Login window.
5. In the Address field of the Web browser, enter the following address:
   `https://<FQDN>/aacpa`
   where <*FQDN*> is the FQDN of EMServer2.
6. Press **Enter**.
   The Avaya Aura® Conferencing Collaboration Agent Login window appears.
7. If you have a standalone simplex deployment, in the Address field of the Web browser complete the following or skip to the next step.
   `https://<FQDN>/aacpa`

where <*FQDN*> is the FQDN of PA1.

8. Press **Enter**.
   The Avaya Aura® Conferencing Collaboration Agent Login window appears.
9. If you have a standalone redundancy deployment, in the Address field of the Web browser complete the following:
   `https://<FQDN>/aacpa`

   where <*FQDN*> is the FQDN of PA2.
10. Press **Enter**.
    The Avaya Aura® Conferencing Collaboration Agent Login window appears.

Next steps

Verify the status of all system components.

Verifying the status of all system components

About this task

Use this procedure to verify:

- all components are running
- there are no alarms present

Procedure

1. On the management PC, open the browser.
2. In the Address box, enter the following address:`https://<FDQN>:12121`
   where <*FQDN*> is the Element Manager FQDN. (This is the server running Element Manager Console.)
3. Press **Enter**.
   A Web page appears displaying the FQDN you entered and the link **Launch Element Manager Console**.
4. Click **Launch Element Manager Console**.
5. From the IPv4 Service Address box on the Element Manager Console window, select the FQDN of the server running Element Manager console.
6. Click **Connect**.
   A connection is established to the active element manager (EM) instance.
7. In the UserID box on the Element Manager Console window, enter `admin`.
8. In the Current Password box, enter `admin`.

9. Click **Ok**.
   The Element Manager Console window appears.
10. Look at the alarm bar at the top of the window and verify the following items:
    - The alarm bar is green.
    - The Total Alarms, Critical, Major, Minor, and Warning fields display **0**.

    Note:

    If the alarm bar is not green, and there are alarms, contact the Avaya support Web site at http://support.avaya.com to open a service request.
11. Right-click the mouse on the alarm bar, and select **Logical View**.
12. In the Logical View window, expand each folder, and verify that component has a green icon preceding it.

    Note:

    If all of the folder components do not have a green icon, contact the Avaya support Web site at http://support.avaya.com to open a service request.
13. When finished, close the Logical View window.

Chapter 13: Configuring single sign-on for Element Manager Console and Provisioning Client

Introduction

System Manager is a central management system that delivers a set of shared management services and a common console across multiple products. With single sign-on (SSO) enabled for Avaya Aura® Conferencing, you can administer all the components using System Manager. This chapter provides the procedures to configure SSO, configure System Manager to recognize each network element, and configure the administrator PC.

Configuring time on System Manager and network elements

About this task

To use single sign-on (SSO), System Manager and all the network elements must have synchronized clocks. A clock skew of a few seconds results in SSO to fail. If the Home portlet is missing menus or functions, logon access to the Element Manager Console or Provisioning Client can fail.

Note:

Ensure your servers use the Network Time Protocol (NTP) time sources.

Procedure

1. Log on to the System Platform Console.
2. In the navigation pane, click **Server Management** > **Date/Time Configuration**.
3. On the Server Management Date/Time Configuration page, verify that you are using NTP server in the Manage Time Servers area. If only **Local Clock** displays, add at least one NTP server and in the Added Servers field, and click **start ntpd**. Use the

Primary Clock Source and **Secondary Clock Source** values, and check the **Local Time** value.

Warning:

Clicking start ntpd causes the system platform and server to restart.

4. Open an SSH connection and log into EMServer1 as `ntsysadm` to verify the time on the server.
5. Type `date`, and press **Enter**.
6. Compare the time on the System Platform Console with the time on the application server. If the time difference between the System Platform Console and the application server is greater than 60 seconds, perform the following steps:
   a. Verify that the NTP is configured on the application server.
   b. On the application server, run the ntpConfig tool.
   c. Type `c` to configure.
   d. Use the **Primary Clock Source** and **Secondary Clock Source** values
   e. Type `date`, and press **Enter**.
   f. Compare the time on the System Platform console with the time on EMServer1. If the time difference between the System Platform Console and the application server is still greater than 60 seconds, perform Steps G through K to correct the date and time manually on the application server by forcing the NTP time update.
   g. At the command prompt, enter `su –` to log in as root.
   h. After you log in as root, type `service ntpd stop`, and press **Enter** to stop the ntpd service.
   i. Run `/usr/sbin/ntpdate <Primary Clock Source IP address>` to update the system time.
   j. Type `date`, and press **Enter** to verify that the date and time have been adjusted.
   k. Type `service ntpd start`, and press **Enter** to start the ntpd service.
7. Repeat Steps 5 and 6 for each application server.

Next steps

Proceed to configuring network element FQDNs in System Manager.

Configuring the application server network elements on System Manager

About this task

Details of each Network Element must be added in the System Manager inventory so that it is possible to launch the Network Elements directly from System Manager. To configure details of each Element Manager, use the following procedure.

Note:

System Manager must have only PROVs from one Avaya Aura® Conferencing system in your inventory. If you have another Avaya Aura® Conferencing system, and you enter the PROV elements in the System Manager inventory, you can encounter problems. System Manager always sends conferencing profile data to one PROV. The data is sent to the first available PROV in the inventory.

Note:

To use single sign-on (SSO), the System Manager FQDN, Element Manager FQDN, and Provisioning Client FQDN (if required) must belong to the same root domain.

Procedure

1. Log on to System Manager as admin.
2. On the System Manager console, click **Inventory**.
3. In the navigation pane, click **Manage Elements**.
4. On the Manage Elements page, click **New**.
5. In the **General** section on the New Elements page, select **Conferencing** from the **Type** list.
   The page refreshes and additional fields appear.
6. In the **General** section on the New Conferencing page, complete the following fields:
   - **Name**: Type `AAC-EM`.
   - **Node**: Type the FQDN of the Element Manager Service IP address.
7. Click **Access Point**.
8. In the Access Point section, click **New**.
9. In the Access Point Details section, complete the following fields:
   - **Name**: Type the FQDN of the Element Manager Service IP address.
   - **Access Point Type**: Select **EMURL**.

- **Protocol**: Select **https**.
- **Host**: Type the FQDN of the Element Manager Service IP address.
- **Port**: Type `12121`.
- **Path**: Type `sso`.
- **Order**: Type `0`.

10. Click **Save**.
11. Click **Commit**.
    The addition of Element Manager on System Manager is now complete.
12. For Provisioning Manager, perform the following steps:
    a. On the Manage Elements page, click **New**.
    b. On the New Elements page, complete the following fields:
       - **Name**: Type `AAC-PROV`.
       - **Type**: Select **Conferencing**.
       - **Node**: Type the FQDN of the EMServer1.
    c. Click **Access Point**.
    d. In the Access Point area, click **New**.
    e. In the Access Point Details area, complete the following details:
       - **Name**: Type the IP address of EMServer1.
       - **Access Point Type**: Select **EMURL**.
       - **Protocol**: Select **https**.
       - **Host**: Type the FQDN of the EMServer1.
       - **Port**: Type `8443`.
       - **Path**: Type `prov/sso`.
       - **Order**: Type `0`.
    f. Click **Save**.
    g. Click **Commit**.
       The addition of Provisioning Client on System Manager is now complete.

Next steps

Proceed to Launching Element Manager Console and Provisioning Client from System Manager.

Launching Element Manager Console and Provisioning client from System Manager

After single sign-on is enabled, you can launch network elements directly from System Manager.

Note:

System Manager administrators have permissions for controlling access to Conferencing and Element Manager and Provisioning Client elements. By default, administrators with either Network Administrator or System Administrator roles have read, write, and expert mode permissions. You can change role assignments and configure permissions for access to various elements. On System Manager home page, click **Users** > **Administrators**.

Warning:

If you have Expert mode privileges, you see an Expert mode warning on certain Provisioning Client pages. This mean that the data on this page is normally controlled by System Manager. Only make changes on these pages to fix synchronization issues with System Manager.

About this task

Use the following procedure to launch the Element Manager Console and Provisioning Client from System Manager.

Procedure

1. Log on to System Manager.
2. On the System Manager console, click **Elements** > **Conferencing**.
3. On the Conferencing Dashboard page, in the **Name** column, select the name of Element Manager Console.
4. From the IPv4 Service Address box on the Element Manager Console window, select the IP address of the server running Element Manager Console.
5. Click **Connect**.
   The Element Manager Console window appears.
6. From the Element Manager Console menu bar, select **File** > **Exit** to exit Element Manager Console.
7. On the Conferencing Dashboard page, in the **Name** column, select the name of Element Manager Console. Click the name of the Provisioning Client you want to access.
   The Welcome to the Provisioning Client page appears.

8. On the Provisioning Client page, click **Logout**.

Result

The Element Manager Console and Provisioning client can now be launched from System Manager.

Chapter 14: Configuring routing between System Manager and Avaya Aura® Conferencing

Configuring the route to Avaya Aura® Conferencing on System Manager

About this task

Use the following procedure to configure the route to Avaya Aura® Conferencing from System Manager.

Procedure

1. Log in to System Manager.
2. On the System Manager console, click **Elements** > **Routing**.
3. In the navigation pane, click **SIP Entities**.
4. On the SIP Entities page, click **New**.
5. Complete the following fields:
   - **Name**: Enter a unique name from 3 to 64 characters for this SIP entity.
   - **FQDN or IP Address**: Type the FQDN or IP address of the AS1 signaling service.
   - **Type**: Select **Conferencing**.

     The screen refreshes to display the following:
   - **Adaptation**: Select from the list.
   - **Location**: Select your location.
   - **Time Zone**: Select a time zone from the list.
   - **Override Port & Transport with DNS SRV**: Select the check box to enable it.
   - **SIP Timer B/F (in seconds)**: Type a value between 1 to 32, default is 4.

- **Credential name**: Type a name.
- **Call Detail Recording**: Select from the list.
- **SIP Link Monitoring**: Select **Use Session Manager Configuration**.
- **Supports Call Admission Control**: Select the check box to enable it.
- **Shared Bandwidth Manager**: Select the check box to enable it.
- **Primary Session Manager Bandwidth Association**: Select your Session Manager entity.
- **Backup Session Manager Bandwidth Association**

6. Click **Commit**.
7. In the navigation pane, click **Entity Links**.
8. On the Entity Links page, click **New**.
9. Complete the following fields:
   - **Name**: Enter a name for this link.
   - **SIP Entity 1**: Select the Aura Session Manager entity.
   - **Protocol**: Select **TCP**.

     OR

     Select **TLS**.

     Note:

     If you selected TLS, you must assign a certificate for the Application Server, see Assigning a certificate to the Application Server on page 173.
   - **Port**: Enter `5060` for TCP or `5061` for TLS.
   - **SIP Entity 2**: Select the Avaya Aura® Conferencing SIP entity you previously created.
   - **Port**: Enter `5060` for TCP or `5061` for TLS.
   - **Connection Policy**: Select **Trusted**.

   Note:

   If TLS is selected for SIP Entity 1 then it must also be selected for SIP Entity 2.
10. Click **Commit**.
11. In the navigation pane, click **Routing Policies**.
12. On the Routing Policies page, click **New**.
13. In the Name box on the Routing Policies page, enter a name for this routing policy.

14. In the SIP Entity as Destination area, click **Select**.
15. On the SIP Entity List page, select the Avaya Aura® Conferencing SIP entity.
16. Click **Select**.
17. Click **Commit**.
18. In the navigation pane, click **Dial Patterns**.
19. On the Dial Patterns page, click **New**.
20. In the Pattern box on the Dial Pattern Details page, type the routing/pilot number that is part of the dialing number to join MeetMe conferences.
21. In the Min box, type the number of digits that match the pattern number. This is the minimum number of digits in the dialing number.
22. In the Max box, type the number of digits that match the pattern number. This is the maximum number of digits in the dialing number.
23. In the Originating Location and Routing Policies area, click **Add**.
24. In the Originating Location area, select your location.
25. In the Routing Policies area, select the routing policy that you previously created for Avaya Aura® Conferencing.
26. Click **Select**.
27. Click **Commit**.

Result

You have configured the routing policy so that when you dial a number that contains the pattern you specified, your call goes to the Avaya Aura® Conferencing Application Server.

Next steps

Proceed to configuring the TLS route to Session Manager from the Element Manager, if TLS is configured; otherwise, proceed to the next chapter.

Configuring TLS route to Session Manager from the Element Manager

Before you begin

You have configured TLS in the previous procedure.

About this task

Use the following procedure to configure the Application Server route to the Session Manager to use TLS.

Procedure

1. Log on to System Manager.
2. On the System Manager page, click **Elements** > **Conferencing**.
3. On the Conferencing Dashboard page, in the Name column, select the name of Element Manager Console.
4. Click **Connect**.
5. In the navigation pane of Element Manager Console, click **Avaya Aura Core** > **Session Manager**.
6. In the Session Manager window, select the Session Manager to configure.
7. Click **Edit (-/+).**
8. In the Edit Session Manager dialog box, in the **Enable SIP TLS Port** field, select the check box to enable TLS and verify that the SIP TLS Port is the same as what is configured on the System Manager in the procedure for Configuring the route to Avaya Aura Conferencing on System Manager on page 233.
9. Close the Session Manager window.
10. On the **File** menu, click **Exit** to exit Element Manager Console.

Chapter 15: Provisioning system settings and users for Avaya Aura® Conferencing

Adding MeetMe, Adhoc, and Event service URIs in Provisioning Client

Service URI is the dialing access number for participants to join an Avaya Aura® Conferencing MeetMe conference. The Service URI number matches the routing dial pattern that you previously configured on the Dial Pattern Details page in Configuring the route to on on page 233. The Service URI is the user name part of the SIP URI string.

About this task

Use the following procedure to add a conference URI.

Procedure

1. Log in to System Manager.
2. On the System Manager console, click **Elements** > **Conferencing**.
3. In the Name column on the Conferencing Dashboard, click the Provisioning Client.
   A new browser window appears and displays the Avaya Aura® Provisioning Client.
4. In the Provisioning Client window, select **System Management > Routing > Service URI**.
5. On the Service URI tab, complete the following for a MeetMe conference:
   This number must match the routing pattern that you previously configured in System Manager.
   - **Service URI**: Type an access number for a MeetMe conference.
   - **Locale**: Select a location from the list. The locale specifies the default locale of prompts that are used if your SIP client does not provide your locale.
   - **Conference Type**: Select **MeetMe** from the list.

6. Click **Save**.
7. On the Service URI tab, complete the following for an Adhoc conference:

   This number must match the routing pattern that you configured in System Manager.

   - **Service URI**: Type an access number for an Adhoc conference.
   - **Locale**: Select a location from the list. The locale specifies the default locale of prompts that are used if your SIP client does not provide your locale.
   - **Conference Type**: Select **Adhoc** from the list.
8. Click **Save**.
9. On the Service URI tab, complete the following for an Event conference:

   This number must match the routing pattern that you previously configured in System Manager.

   - **Service URI**: Type an access number for an Event conference. This number must match the routing pattern that you configured in System Manager.
   - **Locale**: Select a location from the list. The locale specifies the default locale of prompts that are used if your SIP client does not provide your locale.
   - **Conference Type**: Select **Event** from the list.
10. Click **Save**.
11. Repeat Steps 8 through 16 to add additional conference access numbers.

Next steps

Configure display numbers in Provisioning Client.

Creating a user template

About this task

Use the following procedure to create a new user with predefined settings.

Procedure

1. Log on to System Manager as admin.
2. On the System Manager console, click **Elements** > **Conferencing**.
3. In the Name column on the Conferencing Dashboard, click Provisioning Client
4. In the Provisioning Client window, select **User Management** > **User Template**.
5. Complete the following:

- **Name**: Type the name of User Template being created.
- **Conference class of service**: Select the conference class of service from the list.
- **Enable Video**: Select the check box to enable video for a particular user of the Multimedia Conferencing service.
- **Priority**: Select a priority from the list.

Note:

The priority is determined by the quality of service required for this user. For example, the higher the priority setting, the better the service. The default value is medium.

6. Click **Save**.

Creating a conference class of service user template

A conference class of service defines configuration details of a user conference. Class of service templates define the video class of service, the number of conference participants, and whether dial out is allowed for a particular group of users who have that template assigned. Avaya Aura® Conferencing provides the following preconfigured conference classes of service that cannot be deleted or modified:

Table 42: Default conference classes of service

Name	Video Class of Service	Allow dial out/Adhoc	Maximum users
executive	ultra_hi_bandwidth_d	yes	300
desktop_user	hi_bandwidth_d	yes	50
mobile_high	medium_bandwidth_c	yes	50
mobile_low	low_bandwidth_c	yes	50
guest_user	none	no	10

Note:

You can skip this procedure if you want to use one of default conference classes of service

About this task

Use the following procedure to create a conference class of service user template.

Procedure

1. Log on to System Manager as admin.
2. On the System Manager console, click **Elements** > **Conferencing**.
3. In the Name column on the Conferencing Dashboard, click the Provisioning Client.
4. In the Name column on the Conferencing Dashboard, click the Provisioning Client.
5. In the Provisioning Client window, select **System Management** > **Conference Class of Service**.
6. Complete the following fields:
   - **Name**: Type the name of Conference Class being created.
   - **Maximum number of participants**: Type a value between 1 and 3,000 to indicate the allowed number of participants on a chairperson bridge.
   - **Event Conference**: Select this check box if you are creating a large event conference.
   - **Allow dial out to participants**: Select this check box to allow the chairperson to invite participants to the conference.
   - **Video class**: Select a video class from the list. The parameters for each video class are shown in the table on the window.
7. Click **Save**.

Next steps

Proceed to creating a video class of service user template.

Creating a video class of service user template

A video class of service defines the video settings for a user conference.

Note:

You can skip this procedure if you want to use one of the default video classes.

About this task

Use the following procedure to create a video class of service user template.

Procedure

1. Log on to System Manager as admin.

Comments? infodev@avaya.com

2. On the System Manager console, click **Elements** > **Conferencing**.
3. In the Name column on the Conferencing Dashboard, click the Provisioning Client.
4. In the Provisioning Client window, select **System Management** > **Video Class of Service**.
5. Complete the following fields:
   - **Name**: Type the name of Video Class being created.
   - **Maximum average bandwidth per participant (kbps)**: Type a value.
   - **SVC Class**: Select from the list. The parameters for each SVC class are shown in the table on the window.

     Note:

     The parameters are automatically calculated when you modify the value in the field for Maximum average bandwidth per participant (kbps).
6. Click **Save**.

Next steps

Proceed to configuring display numbers in Provisioning Client.

Configuring display numbers in Provisioning Client

You can configure display numbers from Provisioning Client to manage the access numbers that are displayed in Collaboration Agent.

About this task

Use the following procedure to configure display numbers in Provisioning Client.

Procedure

1. Log in to System Manager.
2. On the System Manager console, click **Elements** > **Conferencing**.
3. In the Name column on the Conferencing Dashboard, click the Provisioning Client.
   A new browser window appears and displays the Avaya Aura® Provisioning Client.
4. In the Provisioning Client window, select **System Management > Routing > Service URI**.
5. Click the **Display Numbers** tab.

6. In the **Display Number** field, type a number.
7. In the **Description** field, type a description (maximum 50 characters).
8. Click **Save**.

Result

The number and description appears in Collaboration Agent instead of the Service URI.

Deleting display numbers in Provisioning Client

About this task

Use the following procedure to delete display numbers from Provisioning Client.

Procedure

1. Log in to System Manager.
2. On the System Manager console, click **Elements** > **Conferencing**.
3. In the Name column on the Conferencing Dashboard, click on the Provisioning Client you want to access.
   A new browser window appears and displays the Provisioning Client page.
4. In the Provisioning Client window, select **System Management > Routing > Service URI**.
5. Click the **Display Numbers** tab.
6. Navigate to the display number you want to remove and under the Delete column, click **Delete**.
   The message **Display number deleted successfully** appears.
7. Click **Logout** to exit Provisioning Client.

Adding a location

About this task

For any Location you have configured on System Manager, you must add it manually to Provisioning Client. Use the following procedure to add a location that is being serviced.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Locations**.
2. Click **Add Location**.
3. In the Location Name box, enter the name of the location.

   Important:

   The name is case-sensitive name and must match the location name in System Manager.
4. In the Location Description box, enter any pertinent information about the location.
5. Click **Save**.
6. Repeat Steps 2 through 5 for each location in System Manager.

Next steps

Assign media server clusters to locations.

Assigning media server clusters to locations

About this task

Use the following procedure to assign a media server cluster to serve conference calls for a particular location.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Server Serving Locations** tab.
3. From the Media Server Cluster box, select the media server cluster you want to associate with a location.
4. In the Add locations area, select the check box of the location(s) to which you want to associate the selected media server cluster.
5. Click **Save**.
6. Repeat Steps 3 through 5 to assign other media server clusters.

Next steps

Assign media server clusters to a physical location.

Assigning media server clusters to a physical location

About this task

A media server cluster must be assigned a physical location for communication with other network elements. Use the following procedure to assign a particular media server cluster to a location.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Server Cluster Physical Location** tab.
3. From the Select by box, select **Location**.
4. From the Select Physical Location box, select the location to which you want to assign a media server cluster.
5. From the Available Media Server Clusters box, select the appropriate media server cluster, and then click **Copy**. If you want to assign all available media server clusters, click **Copy all**.
6. Click **Save**.
7. Repeat Steps 3 through 6 for each location.

Next steps

Add the System Manager domain in Provisioning Client.

Making Avaya Aura® Conferencing aware of System Manager domains

In order for Avaya Aura® Conferencing to operate successfully within the Avaya Aura® solution stack, System Manager must make Avaya Aura® Conferencing aware of all SIP domains. In other words, there must be a synchronization between System Manager and Avaya Aura® Conferencing.

When you assign a conference profile to a user, by way of System Manager, and this user has a communication address which does not exist in Avaya Aura® Conferencing, System Manager

pushes the user to Avaya Aura® Conferencing and creates the SIP domain on Avaya Aura® Conferencing. However, you may want to add a SIP domain to System Manager and not assign any users to it. In this case, you will require another mechanism for pushing the SIP domain to Avaya Aura® Conferencing.

In all new releases of System Manager, you can configure automatic synchronization. This means that System Manager pushes all new SIP domains to Avaya Aura® Conferencing automatically. Currently, this feature only pushes new SIP domains to Avaya Aura® Conferencing. It does not delete SIP domains. So, if you remove a SIP domain from System Manager, you must also manually remove it from Avaya Aura® Conferencing. If you do not have a new release of System Manager, you must manually add new SIP domains to Avaya Aura® Conferencing, using the Provisioning Client interface.

Note:

Automatic synchronization is supported from System Manager 6.3.5 Service Pack 5 and 6.3.8 Feature Pack 4. If you have an older version, you must manually add new SIP domains using the Provisioning Client interface.

Related topics:

Enabling the automatic synchronization of domains on page 245
Adding System Manager domains in Provisioning Client on page 246

Enabling the automatic synchronization of domains

About this task

Use this task to configure automatic synchronization of SIP domains between System Manager and Avaya Aura® Conferencing.

Procedure

1. Ensure that the Avaya Aura® Conferencing Provisioning Client network element has been added to the System Manager inventory.

   For more information, see Configuring the application server network elements on System Manager on page 229.
2. Log on to System Manager and navigate to **Elements** > **Conferencing**.
3. Click **Sync** in the left hand menu.
4. Click **Synchronize Domains** to synchronize new domains.
   System Manager displays a list of pushed domains. If the synchronization is not successful, System Manager displays an error message.

Adding System Manager domains in Provisioning Client

About this task

You must manually add all the System Manager domains into Provisioning Client.

Procedure

1. In the Provisioning Client window, select **System Management > User Domains**.
2. In the System Manager Domain box, enter the name of the domain you want to add.
3. Click **Add**.
4. Repeat Steps 2 and 3 for each System Manager domain.

Result

Adding System Manager domains in Provisioning Client is complete.

Assigning the conferencing profile to new System Manager users

To use Avaya Aura® Conferencing, a System Manager user must be assigned the conferencing profile. After you assign the conferencing profile to the System Manager user, the user is added into the Avaya Aura® Conferencing database and is available for editing in Provisioning Client.

Avaya Aura® Conferencing SIP users using SIP services require a Session Manager profile to be assigned.

The conferencing profile specifies conferencing parameters, such as participant and moderator collaboration codes and pass codes, location, and conferencing user data template for a user.

Before you begin

Ascertain if the new user you are adding is using a SIP endpoint or a non-SIP endpoint as this determines how to configure the Communication Profile.

About this task

Use the following procedure to assign the conferencing profile to a new System Manager user.

Note:

If you are using the LDAP directory integration feature, do not perform this feature. See Configuring LDAP directory-synchronized users on System Manager on page 328.

Procedure

1. On the System Manager console, click **Users** > **User Management**.
2. In the navigation pane, click **User Management** > **Manage Users**.
3. On the User Management page, click **New**.
   The New User Profile page appears.
4. On the **Identity** tab, complete the required information, and then click **Commit & Continue**.
5. On the **Communication Profile** tab, complete the required information.
   a. **Name**: Type a name.
   b. **Default**: Select this check box.
   c. Complete the **Communication Address** section to add your E.164 or private enterprise numbering plan.
   d. Complete the **Session Manager Profile** section.
   e. Complete the following profiles as required for your users:
      - **CallPilot Messaging Profile**
      - **CM Endpoint Profile**
      - **CS 1000 Endpoint Profile**
      - **Messaging Profile**
      - **IP Office Endpoint Profile**
      - **Presence Profile**
   f. Complete the **Conferencing Profile** section, proceed to Step 6 on page 247.
6. On the **Communication Profile** tab, select the **Conferencing Profile** check box.
   The Conferencing Profile section expands.
7. Complete the following fields:
   - **Select Auto-generated Code Length**: Modify the PIN length from 6 to 8 characters, default is 6.
   - **Auto Generate Participant Collaboration Code**: Select this check box if you want the system to automatically generate the collaboration codes for the participant.
   - **Participant Collaboration Code**: If you want to assign a specific participant collaboration code for this user, make sure the **Auto Generate Participant Collaboration Code** check box is not selected, and type the conference

participant collaboration code for this user in the **Participant Collaboration Code** box.

- **Auto Generate Moderator Collaboration Code**: Select this check box if you want the system to automatically generate the collaboration codes for the moderator.
- **Auto Generate Participant Pass Code**: Select this check box if you want the system to automatically generate the pass codes for the participant.

Note:

Pass codes are like a second level of security. Participants must enter pass codes after they enter the collaboration code, in order to access the conference. Moderators must send the code to the participants.

- **Auto Generate Moderator Pass Code**: Select this check box if you want the system to automatically generate the pass codes for the moderator.
- **Location**: Select a location from the list. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users.

Note:

For SIP users, the location value is obtained from the Home Location field in the Session Manager profile (if an appropriate value was not selected in the Location field in the Conferencing Profile).

- **Template**: Select the Avaya Aura® Conferencing template you want to assign to this user. The settings for the selected template display. If you are running System Manager 6.3.3 or earlier, you can click the Get Templates button. This button is no longer displayed on System Manager 6.3.4 and later.

8. Click **Commit & Continue**.
9. Repeat Steps 1 on page 247 through 8 on page 248 for each new user you want to add to System Manager and assign the conferencing profile.

Result

Avaya Aura® Conferencing is assigned to a new System Manager user.

Assigning the conferencing profile to existing System Manager users

To use Avaya Aura® Conferencing, a System Manager user must be assigned the conferencing profile. The conferencing profile specifies conferencing parameters, such as participant and moderator collaboration codes and pass codes, location, and conferencing user data template for a user. After you assign the conferencing profile to the System Manager user, the user is

added into the Avaya Aura® Conferencing database and is available for editing in Provisioning Client.

Avaya Aura® Conferencing SIP users using SIP services require a Session Manager profile to be assigned.

Before you begin

- Ascertain if the user you are modifying is using a SIP endpoint or a non-SIP endpoint as this determines how to configure the Communication Profile.
- Ensure a Communication Profile has already been configured in System Manager for the existing user.

About this task

Use the following procedure to assign the conferencing profile to an existing System Manager user.

Note:

If you are using the LDAP directory integration feature, do not perform this feature. See Configuring LDAP directory-synchronized users on System Manager on page 328.

Procedure

1. On the System Manager console, click **Users** > **User Management**.
2. In the navigation pane, click **Manage Users**.
3. Select the check box for the user you want to assign the conferencing profile, and click **Edit**.
4. On the **Communication Profile** tab, select the **Conferencing Profile** check box. The Conferencing Profile section expands.
5. Complete the following fields:
   - **Select Auto-generated Code Length**: Modify the PIN length from 6 to 8 characters, default is 6.
   - **Auto Generate Participant Collaboration Code**: Select this check box if you want the system to automatically generate the collaboration codes for the participant.
   - **Participant Collaboration Code**: If you want to assign a specific participant collaboration code for this user, make sure the **Auto Generate Participant Collaboration Code** check box is not selected, and type the conference participant collaboration code for this user in the **Participant Collaboration Code** box.
   - **Auto Generate Moderator Collaboration Code**: Select this check box if you want the system to automatically generate the collaboration codes for the moderator.

- **Auto Generate Participant Pass Code**: Select this check box if you want the system to automatically generate the pass codes for the participant.

  Note:

  Pass codes are like a second level of security. Participants must enter pass codes after they enter the collaboration code, in order to access the conference. Moderators must send the code to the participants.

- **Auto Generate Moderator Pass Code**: Select this check box if you want the system to automatically generate the pass codes for the moderator.
- **Location**: Select a location from the list. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users.

  Note:

  For SIP users, the location value is obtained from the Home Location field in the Session Manager profile (if an appropriate value was not selected in the Location field in the Conferencing Profile).

- **Template**: Select the Avaya Aura® Conferencing template you want to assign to this user. The settings for the selected template display. If you are running System Manager 6.3.3 or earlier, you can click the Get Templates button. This button is no longer displayed on System Manager 6.3.4 and later.

6. Click **Commit & Continue**.
7. Repeat Steps 1 on page 249 through 6 on page 250 to assign the conferencing profile for every existing System Manager user.

Assigning the conferencing profile to a group of System Manager users

To use Avaya Aura® Conferencing, a System Manager user must be assigned the conferencing profile. The conferencing profile specifies conferencing parameter such as moderator and participant collaboration codes and pass codes, location, and conferencing user data template for a user.

Avaya Aura® Conferencing SIP users using SIP services require a Session Manager profile to be assigned.

About this task

Use the following procedure to assign the conferencing profile to a group of System Manager users.

Note:

Avaya recommends using this procedure when assigning conferencing profiles to a large group of System Manager users.

Note:

If you are using the LDAP directory integration feature, do not perform this feature. See Configuring LDAP directory-synchronized users on System Manager on page 328.

Procedure

1. On the System Manager console, click **Users** > **User Management**.
2. In the navigation pane, click **Manage Users** and ensure there is at least one user on this page.
3. In the **Communication Address** section, verify that at least one communication address is assigned.
4. In the **Session Manager Profile** section, verify that at least one Session Manager profile is assigned.
5. Log on to the System Manager as admin through ssh.
6. Run the following commands:
   - For System Manager 6.3:

     ```
     cd $MGMT_HOME/bulkadministration/exportutility
     ```
     and

     ```
     bash exportUpmUsers.sh
     ```
   - For System Manager 6.2:

     ```
     cd $MGMT_HOME/upm/bulkexport/exportutility
     ```
     and

     ```
     bash exportUpmUsers.sh
     ```

   Job:<filename> is created.
7. Copy the <filename>.zip, as shown in the previous step to your PC.
   - For System Manager 6.3, <filename>.zip is located in `$MGMT_HOME/bulkadministration/export`.
   - For System Manager 6.2, <filename>.zip is located in `$MGMT_HOME/upm/bulkexport`.
8. View `$AVAYA_LOG/mgmt/um_bulkexport/bulkexportTraceLog.log` file to check for error messages.
9. Extract the xml file(s) from <filename>.zip on your PC.
10. In the xml file(s), remove all users who are not affected.

11. In the xml file(s), locate the following information:

```
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:ns3="http://xml.avaya.com/schema/import1"
xmlns:ns4="http://xml.avaya.com/schema/deltaImport"
xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">
```

12. In the xml file(s), replace the information specified in Step 11 with the following information:

```
<tns:deltaUserList xmlns:ns3="http://xml.avaya.com/schema/import1"
xmlns:tns="http://xml.avaya.com/schema/deltaImport"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport
userdeltaimport.xsd ">
```

13. In the xml file(s), perform the following steps:
    a. Replace all instances of `<tns:user>` with `<tns:userDelta>`.
    b. Replace all instances of `</tns:user>` with `</tns:userDelta>`.
    c. Replace all instances of `<tns:users>` with `<tns:deltaUserList>`.
    d. Replace all instances of `</tns:users>` with `</tns:deltaUserList>`.
14. In the xml file(s), add the following xml segments between the lines `<commProfileList>` and `</commProfileList>` for users who have a conferencing profile:

```
<commProfile xsi:type="ns2:MmcsCommProfileType" xmlns:ns2="http://
xml.avaya.com/schema/import_mmcs">
<commProfileType>mmcsCommProfile</commProfileType>
<ns2:template>template</ns2:template>
<ns2:securityCode>123456</ns2:securityCode>
<ns2:moderatorPin>654321</ns2:moderatorPin>
<ns2:eventConfCode>222</ns2:eventConfCode>
<ns2:location>location</ns2:location>
<ns2:autoGeneratedCodeLength>6</ns2:autoGeneratedCodeLength>
</commProfile>
```

15. To create a conferencing profile from an existing template, copy the template and add the xml segments from the preceding step to the conferencing profile xml file.
16. Verify that all SIP users have values for `primarySM` and `homeLocation`.
17. Verify that all users have at least one handle in `commProfileSet > handleList`.
18. Complete the conferencing profile xml values:

    Where:

    - *template*: is an Avaya Aura® Conferencing user template name.
    - *securityCode*: is a Participant collaboration code. This is required if the autoGeneratedCodeLength parameter is not configured.
    - *moderatorPin*: is a Moderator collaboration code. This is required if the autoGeneratedCodeLength parameter is not configured.
    - *eventConfCode*: is a Presenter security code. This is required if the autoGeneratedCodeLength parameter is not configured.

- *autoGeneratedCodeLength*: indicates if security codes must be auto generated and the required length for auto generated codes.
- *location*: is an Avaya Aura® Conferencing user Location. The location is mandatory for non-SIP users without a configured Session Manager profile and optional for SIP users.

Note:

For SIP users, the value for the Avaya Aura® Conferencing user location is obtained from the Home Location parameter in the Session Manager profile (if the Location parameter in the Conferencing Profile is not configured).

19. Log on to System Manager as admin.
20. On the System Manager console, click **Bulk Import and Export**.
21. On the Import and export page, click **Import**.
22. On the Import page, click **User Management**.
23. On the Import - User and global settings page, click **Users**.
24. On the Import users page, click **Browse** to select the edited xml file.
25. In the General section on the Import users page, set Select import type to **Partial**.
26. Click **Import** to start the job.
27. In the **Manage job** section, click **Refresh** to view the status of your job.
    The status updates to indicate SUCCESSFUL or FAILED.

Note:

In case of a failure, under the **Job name** column, click the job number to see the error message.

Verifying access to the MeetMe conference

Before you begin

You must have Avaya Flare® Experience for Windows installed and configured on a PC. To install and configure Avaya Flare® Experience for Windows, see *Implementing Avaya Flare® Experience for Windows*.

About this task

Use this procedure to verify that you can access the MeetMe confererence URI.

Procedure

1. Start Avaya Flare® Experience for Windows.
2. Click **Settings**.
3. In navigation pane in the General Settings dialog box, click **Dialing Rules**.
4. On the Dialing Rules page, clear the **Apply Dialing Rules for outgoing calls** check box to prevent dialing rules from being applied to the number dialed to access the MeetMe conference.
5. In the navigation pane, click **Conference**.
6. In the Conference Factory URI box on the Conference page, type the Adhoc URI you entered in Provisioning Client.
7. Click **OK**.
8. In the Extension box, enter a valid communication profile name that is administered on System Manager.
9. In the Password box, enter the password for the communications profile.
10. Click **Log in**.
11. Click **Call**.
12. On the dialpad, enter the MeetMe number you configured in Provisioning Client.
13. On the dialpad, click **Call**.
    You hear the Avaya introduction and are prompted to enter your conference access code followed by the pound (#) key.
14. Click **Keypad**.
15. On the keypad, enter a valid moderator PIN and press the pound (#) key.
    The MeetMe conference starts.

Associating Web conferencing resources with a location in Provisioning Client

Before you begin

Web conferencing server resources (that is, Web Conferencing Server and Document Conversion Server) must be configured on the Element Manager Console.

About this task

Perform this procedure to associate Web conferencing resources with a location. You can associate multiple locations with the Web Conferencing Server resources.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Web Conferencing Server Resources**.
2. From the Location box, select the location to which you want associate Web Conferencing Server resources.
3. From the Primary Web Conferencing Server box, select the primary Web Conferencing Server for the selected location.
4. From the Secondary Web Conferencing Server box, select the secondary Web Conferencing Server for the selected location (optional).
5. From the Document Conversion Server box, select the Document Conversion Server for the selected location.
6. Click **Save**.
7. Repeat this procedure for every location you previously defined.

Configuring a Web conferencing host

This task is particularly significant if you plan to deploy the Avaya Aura® Conference Manager Add-in for Microsoft Outlook®. You will require the Web conferencing host name during the configuration of the Avaya Aura® Conference Manager Add-in for Microsoft Outlook®.

About this task

Use the following procedure to configure a Web conferencing host name.

Procedure

1. In the Provisioning Client window, select **System Management** > **Routing** > **Web Conferencing Host**.
2. In the Host Name field, enter a host name.

   Depending on the deployment type, you should enter either:

   - The fully qualified domain name (FQDN) of the Provisioning Manager network element/Personal Agent network element.
   - The FQDN of the load balancer.
3. Click **Save**.

Related topics:

Deploying the Avaya Aura Conference Manager Add-in for Microsoft Outlook on page 401

Implementing a ClickOnce deployment on page 402
Implementing a centralized software deployment on page 403

Configuring an operator

An operator has the following abilities:

- search conferences in Collaboration Agent by user name and participant code
- log on to a conference using the moderator code
- has moderator privileges during a conference

About this task

Use the following procedure to configure a user as an operator of a conference.

Procedure

1. In the Provisioning Client window, select **User Management** > **Conferencing User.**
2. In the **Select Login name** field, type a logon name, and click **>>**.
3. Select the **Enable operator control** check box to enable, and click **Save**.

Configuring the system operator

Before you begin

You can only specify one URI for the operator.

About this task

Use this procedure to specify the URI that is contacted when a participant requests the operator during a conference.

Procedure

1. In the Provisioning Client window, select **System Management** > **System Default Settings**.
2. In the **Operator** field, enter the URI of the operator. If a participant requests the operator during a conference, this URI is contacted.
3. Click **Save**.

Configuring Event conferencing

About this task

Use the following procedure to configure a large event conference.

Procedure

1. In the Provisioning Client window, select **User Management** > **User Template**.
2. In the User Template window, complete the following fields:
   - **Name**: Type a name.
   - **Conference class of service**: Select an event name from the list, for example, Event_1000 or Event_2000.
   - **Enable Video**: Select the check box to enable.
   - **Priority**: Select a priority type from the list.
3. Click **Save**.
4. In the Provisioning Client window, select **System Management** > **Routing** > **Media Server Resources**.
5. Click the **Media Server Serving Locations** tab.
6. In the Add locations section, clear the check boxes for the locations where event conferencing is to be used.
7. Click **Save**.
8. Click the **Media Server Cluster Physical Location** tab.
9. In the **Select by** field, select **Location** from the list.
10. In the **Select Physical Location** field, select the location for where the equipment is located.
11. Click the **Media Server Clusters for Event Conferences** tab.
12. In the **Available Media Server Clusters** list, select the **Media Server Cluster**, and click **Copy** to move it to the **Select Media Server Clusters** list.
13. Click **Save**.
14. If the Event conferencing Service URI is not already added, see Adding MeetMe Adhoc and Event service URIs in Provisioning Client on page 237.

Next steps

Proceed to configuring media server cascading.

Configuring Avaya Media Server cascading

Traffic can be minimized between Avaya Media Servers if a conference has users on different Avaya Media Servers. Only one channel is used between Avaya Media Servers.

Before you begin

More than one Media Server cluster must be configured in Element Manager. See Adding additional Avaya Media Server hosts on page 177.

About this task

Use the following procedure to configure Avaya Media Server cascading.

Procedure

1. In the Provisioning Client window, select **System Management** > **System Default Settings**.
2. On the **System Default Settings** tab, select the **Allow media cascading** check box to enable.
3. Click **Save**.
4. In the Provisioning Client window, select **System Management** > **Routing** > **Media Server Resources**.
5. Click the **Media Server Serving Locations** tab.
6. In the Media Server cluster box, select a Media Server cluster from the list.
7. In the Add locations section, select a location check box to assign a location for the Media Server cluster.
8. Click **Save**.
9. Repeat Steps 6 through 8 for each Media Server cluster.
10. Click the **Media Server Cluster Physical Location** tab.
11. In the Select by field, select **Location** from the list.
12. In the Select Physical Location field, select a location from the list.
13. Click **Save**.
14. Click the **Media Stream Cascading** tab.
15. In the Select location field, select a location from the list.
16. Select the check box to enable **Cascading is allowed when this location is hosting the conference**.
17. Click **Save**.

18. Repeat Steps 15 through 17 for each location.
19. Click the **Hosting Locations** tab.
20. In the Select Hosting Location field, select a hosting location as the host for all other locations.
21. Click **Copy all** to move the locations in the Hostable Locations field to the Hosted Locations field.
22. Click **Save**.

Next steps

Proceed to configuring bandwidth management.

Related topics:

Configuring the codecs for the cascading trunks on page 259

Configuring the codecs for the cascading trunks

About this task

Use this task to specify a G.711, G.722, or G.726 audio codec for the cascading trunks in your deployment. If you are using cascading trunks in your deployment, you can also specify the packet time for the audio codec. If you are not using cascading trunks in your deployment, the packet time is hardcoded to 20 milliseconds.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Cascading Trunk Codec Settings**.
2. On the **Cascading Trunk Codec Settings** dialog, re-order the list of audio codecs in accordance with your preferences.
3. Specify the packet time for the audio codec from the **Default PTimes for all codecs** drop-down list.
4. Click **Ok**.

Related topics:

Cascading Trunk Codec Settings field descriptions on page 260

Cascading Trunk Codec Settings field descriptions

Name	Description
Enabled	The Enabled panel lists the audio codecs that are available. You can select each item in this list.
Default PTimes for all codecs	Specify a packet time for the audio codec. By default, the packet time is set to 10 milliseconds.

Button	Description
Up	Moves the selected audio codec to a higher location on the list.
Down	Moves the selected audio codec to a lower location on the list.
Ok	Click **Ok** to apply your changes.
Cancel	Click **Cancel** to disregard your changes.

Configuring a regional cascading location

Before you begin

- You must be logged into Provisioning Client.
- Cascaded locations (that is, locations that cascade through a cascading location) must have a good-quality WAN link.
- Cascaded locations do not need to have media servers configured.
- A cascaded location can be assigned to only one cascading location (that is, the location that provides media cascading).
- A cascaded location and cascading location pair cannot be assigned as a hosting location and hosted location pair (and vice versa).
- A cascading location can be the same as the hosting location for a particular location.
- Cascading must be enabled for the Avaya Aura® Conferencing system, the user location, the cascading location, and the hosting location if you want to use regional cascading.

About this task

Use this procedure to configure a regional cascading location, which provides media cascading to the remote locations you specify. The users at the specified locations will be able to call into

the regional cascading location instead of the joining the conference directly via the hosting media server. Regional cascading locations enable you to optimize WAN bandwidth usage.

Note:

Cascading must be allowed (enabled) for the Avaya Aura® Conferencing system, the user location, the cascading location, and the hosting location if you want to use regional cascading.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Cascading Locations** tab.
3. From the Select Cascading Location box, select the location that will provide media cascading for other locations.
4. From the Locations that have no Cascading Location assigned list box, select the location(s) that you want to assign to the selected cascading location, and then click **Copy**. If you want to assign all locations, click **Copy all**. For more information see, Media Cascading Locations tab field descriptions on page 261.
5. Click **Save**.

Related topics:

Media Cascading Locations tab field descriptions on page 261

Media Cascading Locations tab field descriptions

Name	Description
Select Cascading Location	Select the location that will provide media cascading for other locations.
Locations that have no Cascading Location assigned	Displays the locations that you can assign to the selected cascading location. From this list box, you can select the location(s) that you want to assign to the selected cascading location.
Locations that cascade throug	Displays the locations that you want to assign to the selected cascading location.

Button	Description
Copy all	Moves all of the locations displayed in the Locations that have no Cascading Location

Button	Description
	assigned list box into the Locations that cascade through list box.
Copy	Moves the selected location in the Locations that have no Cascading Location assigned list box into the Locations that cascade through list box.
Remove	Moves the selected location in the Locations that have no Cascading Location assigned list box into the Locations that cascade through list box.
Remove All	Moves all of the locations displayed in the Locations that cascade through list box into the Locations that have no Cascading Location assigned list box.

Configuring bandwidth management

Bandwidth for conferences can be managed in accordance with configured thresholds and user priority. With proactive bandwidth optimization, you can reduce bandwidth usage and reduce costs while managing the quality of multimedia sessions.

About this task

Use the following procedure to configure bandwidth management.

Procedure

1. In the Provisioning Client window, select **System Management** > **System Default Settings**.
2. Select the **Allow bandwidth management** check box to enable.
3. Click **Save**.
4. In the Provisioning Client window, select **System Management** > **Bandwidth Optimization**.
5. In the Select location field, select a location from the list.
6. In the High threshold field, type a value. The range is 75 to 100. If 100 is selected, bandwidth optimization is disabled for all new and existing sessions.
7. In the Critical threshold field, type a value. The range is 75 to 100. If 100 is selected, bandwidth optimization is disabled for all new sessions. The value must be greater than the High threshold value.

8. Click **Save**.
9. Select **User Management** > **Conferencing User**.
10. In the **Select login name** field, type a login name, for example, jsmith@yourcompany.com, and click **>>**.
11. In the **Priority** field, select one of the following:
    - Business critical
    - High
    - Medium
    - Low
12. In the **Class of service** field, assign the conference class of service for this user.
    For more information about the default classes of service, see Creating a conference class of service user template on page 239.
13. Select the **Enable Video** check box to enable video for this user.
14. Click **Save**.

Chapter 16: Configuring Audio SRTP

This section describe how to configure Audio SRTP with Avaya Aura® Conferencing. This feature enables users to conduct “secure” audio conferences if all participants in the conference are using SRTP audio.

Endpoints supported with Audio SRTP

The following endpoints support Audio SRTP:

- Avaya 9600 Series IP Deskphones 96x1 H.323 Release 6.2
- Avaya 9600 Series IP Deskphones 96x1 H.323 Release 6.3
- Avaya 9600 Series IP Deskphones 96x1 SIP Release 6.2
- Avaya 9600 Series IP Deskphones 96x1 SIP Release 6.3
- Avaya Flare Experience Release 1.1 for Windows
- Avaya Flare Experience Release 1.1 for iPad Devices
- Avaya one-X Communicator Release 6.1
- Avaya one-X Communicator Release 6.1.1
- Avaya one-X Communicator Release 6.1.6

Audio SRTP configuration tasks

You must perform the following tasks to use Audio SRTP with Avaya Aura® Conferencing.

#	Task	Description	Notes	✔
1	Configure TLS to secure the connection between Session Manager and Avaya Aura® Conferencing. Ensure that **Enable SIP TLS Port** is selected in the Transport Information area in the Add/Edit Session Manager dialog box.	See Configuring TLS route to Session Manager from the Element Manager on page 235.		

#	Task	Description	Notes	✔
2	Configure TLS for Avaya Media Server connections. For each Avaya Media Server, ensure that **Enable SIP TLS** is selected in the Transport area in the Add/Edit Media Server dialog box.	See Assigning certificates to the Avaya Media Servers on page 174.		
3	Configure the SRTP settings for audio on Avaya Aura® Conferencing.	See Administering the Audio SRTP settings for Avaya Aura Conferencing on page 266.		
4	Configure Communication Manager to support Audio SRTP with Avaya Aura® Conferencing.	See Modifying Communication Manager settings for Audio SRTP on page 270.		

Administering the Audio SRTP settings for Avaya Aura Conferencing

About this task

Use this procedure to configure the SRTP settings for audio for Avaya Aura® Conferencing.

Here are the recommended Audio SRTP settings when configuring Avaya Aura® Conferencing in the Aura Solution:

- Security Policy - **BEST EFFORT**
- Encrypt RTCP - Disabled (that is, check box is not selected)
- Video Allowed For Security Enforced Calls - Enabled (that is, check box is selected)
- Enforce SIPS for Security Enforced Calls - Enabled
- Use SIP for Best Effort Offers - This setting is not used.
- Mode - AES_CM_128_HMAC_SHA1_80:
  - Priority - **1**
  - Send Lifetime - Disabled

- SRTP Master Key Lifetime - **31**
- Key Derive Rate - **0**
- Master Key Index Length - **0**

• Mode - AES_CM_128_HMAC_SHA1_32:

- Priority - **1**
- Send Lifetime - Disabled (that is, check box is not selected)
- SRTP Master Key Lifetime - **31**
- Key Derive Rate - **0**
- Master Key Index Length - **0**

Procedure

1. In the navigation pane of Element Manager Console, select **Security > SRTP Settings**.
2. In the SRTP Settings dialog box, configure each setting. For more information, see SRTP Settings dialog box field descriptions on page 267.
3. When finished, click **Apply**.

Related topics:

SRTP Settings dialog box field descriptions on page 267

SRTP Settings dialog box field descriptions

Name	Description
Security Policy	Select the type of media security policy you want to use. The security policy you specify dictates the type of audio media Avaya Aura® Conferencing will include in offer SDPs and how Avaya Aura® Conferencing generates answer SDP during SDP negotiation. Choices are: • **BEST EFFORT** When this option is selected, Avaya Aura® Conferencing will generate requests using SIPS and will offer both RTP and SRTP audio using capability negotiation. If the request fails because SIPS is not supported by the endpoint, Avaya Aura® Conferencing will retry the request using SIP and RTP. Avaya Aura® Conferencing will accept and negotiate RTP-only audio offers, SRTP-only audio offers, and RTP/SRTP best effort audio offers. SRTP will be negotiated where allowed when a compatible SRTP crypto suite is offered. RTP will be negotiated for RTP-only offers and for RTP/

Name	Description
	SRTP best effort audio offers when a compatible SRTP crypto suite is not offered. • **SECURITY DISABLED** When this option is selected, Avaya Aura® Conferencing will support only RTP audio. Avaya Aura® Conferencing will accept and generate RTP audio offers/answers. Avaya Aura® Conferencing will negotiate to RTP audio when it receives a request that contains an SDP offer with RTP audio or best-effort audio. Avaya Aura® Conferencing will reject requests that contain an SDP offer with only SRTP audio by replying with a 480 Temporarily Unavailable response. A local treatment will be played to the end user. • **SECURITY ENFORCED** When this option is selected, Avaya Aura® Conferencing will support only SRTP audio. Avaya Aura® Conferencing will negotiate to SRTP audio when it receives a request that contains an SDP offer with SRTP audio or best-effort audio and a compatible crypto suite. Avaya Aura® Conferencing will reject requests that contain an SDP offer with only RTP audio by replying with a 480 Temporarily Unavailable response. A local treatment will be played to the end user. **Note:** The SECURITY ENFORCED option does not guarantee signaling security. To ensure full encryption, you must configure TLS for the Avaya Aura® Conferencing Application Server network element.
Encrypt RTCP	Select this check box to indicate that Avaya Aura® Conferencing supports encrypted SRTCP messages. When not selected, Avaya Aura® Conferencing does not support sending or receiving encrypted SRTCP messages. Avaya Aura® Conferencing will include the UNENCRYPTED_SRTCP session parameter in both its offers and answers, and unencrypted SRTCP will be used in both directions. When selected, Avaya Aura® Conferencing supports sending and receiving encrypted SRTCP messages. Avaya Aura® Conferencing will not include the UNENCRYPTED_SRTCP session parameter in its offers. However, if the UNENCRYPTED_SRTCP session parameter is received in an offer when this setting is selected, Avaya Aura® Conferencing will echo the UNENCRYPTED_SRTCP session parameter in its answer, and unencrypted SRTCP will be used in both directions.
Video Allowed For Security Enforced Calls	Select this check box if you want Avaya Aura® Conferencing to send secure audio and unsecure video, if possible. If this check box is not selected, Avaya Aura® Conferencing will disable the video port for calls with secure audio.

Name	Description
Enforce SIPS for Security Enforced Calls	Select this check box if you want to require incoming calls to use SIPS signaling to negotiate secure media for the call. In addition, Avaya Aura® Conferencing generated requests with SRTP-only audio offers will use SIPS signaling.
Use SIPS For Best Effort Offers	This setting is not used. Avaya Aura® Conferencing uses SIPS when generating a request with both RTP and SRTP (for example, Security Polity is BEST EFFORT). If the request fails because SIPS is not supported by the endpoint, Avaya Aura® Conferencing will retry the request with SIP and RTP.
Mode	Select the encryption mode(s) you want to use. This is commonly referred to as the “crypto suite.“ Choices are **AES_CM_128_HMAC_SHA1_80** and **AES_CM_128_HMAC_SHA1_32**.
Priority	Select the priority for the associated mode. Choices are **0** to **9**. If you want to disable the encryption mode, select **0**. A non-zero value indicates the priority that should be applied to the crypto suite during media negotiation. **1** is the highest priority; **9** is the lowest priority.
Send Lifetime	Select this check box to indicate that Avaya Aura® Conferencing should include the Master Key Lifetime specified by the SRTP Master Key Lifetime option (below) in the key parameter of the SRTP crypto attribute during SRTP media negotiation. When not selected, the Master Key Lifetime field is not included in the key parameter of the SRTP crypto attribute during SRTP media negotiation. In this case, the default lifetime for the crypto suite is used for media negotiation.
SRTP Master Key Lifetime	Specify the maximum number of SRTP packets that will use a particular master key. Choices are **1** to **31**.
Key Derive Rate	Specify how frequently a new session key is derived from an SRTP master key. Choices are **0** to **24**.
Master Key Index Length	Specify the size of the Master Key Index/Identifier (MKI) field in the actual SRTP packets. Choices are **0** to **4**. An MKI is used to identify the master key from which the session key that authenticates the particular packet was derived. When set to **0**, Avaya Aura® Conferencing will not include an MKI value and its associated length in the key parameter of the SRTP crypto attribute during SRTP media negotiation, and an MKI field will not be included in the actual SRTP packets. When the Master Key Index Length is set to a value greater than **0**, Avaya Aura® Conferencing will include an MKI value, and its associated length in the key parameter of the SRTP crypto attribute during SRTP media negotiation and an MKI field will be included in the actual SRTP packets.

Modifying Communication Manager settings for Audio SRTP

About this task

Use the following procedure to modify Communication Manager settings to support Audio SRTP. These settings are recommendations for “best effort.”

Procedure

1. Log on to System Manager as admin.
2. On the System Manager console, click **Elements >** Communication Manager.
3. In the navigation pane, click **Parameters > System Parameters – Customer Options**.
4. On the System Parameters – Customer Options page, select the appropriate device, and click **View**.
5. Click **Next Page** to go to page 4.
6. On page 4, verify **Media Encryption Over IP** is set to **Y**.

   Note:

   If **Media Encryption Over IP** is set to **N**, contact Avaya support.
7. In the navigation pane, click **Parameters > System Parameters – Features**.
8. On the System Parameters – Features page, select the appropriate device, and click **New**.
9. Click **Prev Page** to go to page 19.
10. In the IP Parameters section, set **Initial INVITE with SDP for secure calls** to **Y**.
11. Press **Enter** to save your changes.
12. In the navigation pane, click **Network > Signaling Groups**.
13. Click the check box of the appropriate signaling group, and click **Edit**.
14. On Page 1, set **Enforce SIPS URI for SRTP** to **Y**.
15. Press **Enter** to save your changes.
16. Log off System Manager.
17. Open your Web browser and in the Address bar, type the IP address for the Communication Manager System Management Interface (SMI).
18. At the Logon ID prompt, type your Logon ID, and click **Logon**.
19. Type your password, and click **Logon**.

20. On the Administration menu, click **Native Configuration Manager**.
21. In the Server Login window, type your Logon ID, and click **OK**.
22. Type your password, and click **OK**.
23. In the Command field, type `change system-parameters ip-options`, and click **Send**.
24. On the IP-options system parameters page, click **NEXT PAGE** to navigate to page 2.
25. In the **Override ip-codec-set for SIP direct-media connections** field, type **y**.
26. Click **Enter**.
27. In the Command field, type `change ip-codec-set #`, where `#` is the IP codec set you want to modify, and click **Send**.
28. In the Media Encryption section on page 1 of IP Codec Set, perform the following steps:
    a. In field 1, type `1-srtp-aescm128-hmac80`.
    b. In field 2, type `2-srtp-aescm128-hmac32`.
    c. In field 3, type `none`.
29. Click **Enter**.
30. Repeat Steps 27 through 29 for each IP codec set.
31. When finished, close the Native Configuration Manager window.
32. In the Communication Manager system Management Interface (SMI) window, click **Logoff**.
33. Click **Log Off**.

Chapter 17: Configuring the recording feature

Avaya Aura® Conferencing captures audio and web collaboration within a conference. Avaya Aura® Conferencing does not record video and it does not record standalone web conferences (SWC). Standalone web conferences are conferences that do not have an Avaya Aura® Conferencing audio component. Instead, their audio component is provided by an external source, such as a direct call between two parties.

Avaya Aura® Conferencing supports the following recording deployments:

- Co-resident deployment. See Checklist for configuring Recording in a co-resident deployment on page 274.
- Dedicated Recording server deployment. See Checklist for configuring Recording in a dedicated Recording server deployment on page 273.

Avaya Aura® Conferencing does not implement a quota system. So, for example, the recordings of a single user could take up all of the available storage space. Avaya Aura® Conferencing does not encrypt recordings on the hard drive. Recordings are stored and played back without encryption. Users cannot edit recordings and they cannot search for a phrase within a recording.

Checklist for configuring recording in a dedicated recording server deployment

The following checklist provides a high-level view of the tasks involved in configuring the Recording feature in a dedicated Recording server deployment.

#	Task	Description	Notes	✔
1	Add and configure a media server dedicated for Recording via Element Manager Console.	See Adding a media server dedicated for recording on page 275.		
2	Assign locations to the Recording media	See Configuring the Recording media server cluster for		

#	Task	Description	Notes	✔
	server cluster via Provisioning Client.	locations on page 281.		
3	Create and assign a certificate for the dedicated Recording server.	See Creating a certificate for a dedicated Recording server on page 278.		
4	Configure the system-wide Recording setting via Provisioning Client.	See Configuring the system-wide Recording setting on page 281.		
5	Configure the Recording feature for users via Provisioning Client.	See Configuring the Recording feature for a user on page 282.		
6	Configure the Recording backup server.	See Configuring the Recording backup server on page 286.		

Checklist for configuring recording in a co-resident deployment

The following checklist provides a high-level view of the tasks involved in configuring the Recording feature in a co-resident deployment.

#	Task	Description	Notes	✔
1	Configure the Recording media server cluster via Element Manager Console.	See Configuring Recording for a media server cluster in a co-resident deployment on page 279.		
2	Configure the system-wide Recording setting via Provisioning Client.	See Configuring the system-wide Recording setting on page 281.		

#	Task	Description	Notes	✔
3	Assign a Recording media server cluster to locations.	See Assign a Recording media server cluster to locations on page 280.		
4	Configure the Recording feature for users via Provisioning Client.	See Modifying a single user on page 282.		
5	Configure the Recording backup server.	See Configuring the Recording backup server on page 286.		

Dedicated recording server deployment only

In this context, a dedicated recording server deployment is also known as a standalone deployment.

The steps involved in configuring recording for a dedicated recording server deployment are much the same as the steps involved in configuring recording for a co-resident deployment. However, the following procedures only apply to dedicated recording server deployments.

Related topics:

Adding a media server dedicated for recording on page 275

Creating a certificate for the dedicated Recording server on page 278

Adding a media server dedicated for recording

About this task

Use this procedure to add a media server that will be dedicated for recording.

Note:

During this procedure, you will create a new media server cluster. A media server cluster supports a maximum of eight media servers:

- one primary
- one secondary
- six standard servers

Procedure

1. In the navigation pane of Element Manager Console, select **Addresses**.
2. In the Addresses window, click **Add (+)**.
3. In the Add IPv4 Address dialog box, enter the logical name and IP address for the media server.
4. Click **Apply**.
5. In the navigation pane of Element Manager Console, select **Servers**.
6. In the Servers window, click **Add (+)**.
7. In the Add Server dialog box, complete the following fields:
   - **Short Name**
   - **Long Server Name**
   - **Internal OAM (Default) Address**: Enter the IP address you specified in Step 3.
   - **Operating System**: Select **linux**.
   - **Host Name**: Enter the short name or FQDN of the server.
8. Click **Apply**.
9. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers**.
10. In the Media Servers window, click **Add (+)**.
11. In the Add Media Server dialog box, complete the following fields:
    - **Short Name**
    - **Long Name**
    - **Base Port**: Type 49000.
    - **Enable SIP TCP**: Select this check box to enable.

      OR

      Enable SIP TLS: Select this check box to enable.
    - **SIP Certificate**: If SIP TLS is enabled, select the certificate you want to use for SIP TLS. For more information, see the chapter for Configuring Transport Layer Security.

    Note:

    Accept the default for all other fields.
12. Click **Apply**.

Comments? infodev@avaya.com

13. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers** > **<media server you specified in Step 3> Instance**.
14. In the Media Server Instance window, click **Add (+)**.
15. In the Add Media Server Instance dialog box, complete the following fields:
    - **Server**: Select the media server you created in Step 3.
    - **Load or Patch**: Select the software load.
    - **Engineering**: Select the configuration that corresponds to your hardware type and layout.
16. Click **Apply**.
17. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters**.
18. In the Media Server Clusters window, click **Add (+)**.
19. In the Add Media Server Cluster dialog box, complete the following fields:
    - **Short Name**
    - **Long Name**
    - **Primary Server**: Select the Avaya Media Server network element. This list contains only the media server network elements that do not belong to any cluster. You must specify a primary server.
    - **Secondary Server**: If this cluster has two or more Avaya Media Servers, you must specify a secondary server. Otherwise, leave this field blank.
    - **Role**: Select **RECORDING ONLY**.
20. Click **Apply**.
21. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers** > **MediaServer2** >**NE Maintenance**.
22. In the Media Server Maintenance dialog box, select the row for ID 0.
23. Click **Deploy**.
    The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.
24. Click **Start**.
    The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

    Check the state transitions for the following fields:

Field	Status
Maint	None
Admin	Online
Link	Up
Oper	Active

25. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters**.
26. In the Media Server Clusters window, select **MediaServer1**, and click **Edit (+/-)**.
27. In the Edit Media Server Cluster dialog box, make sure the Role box is set to **CONFERENCING ONLY** .

Creating a certificate for the dedicated Recording server

Before you begin

You must know the enrollment password as completed in Obtaining enrollment password from System Manager on page 165.

About this task

Use this procedure to create a new certificate for the dedicated Recording server.

Procedure

1. In the navigation pane of Element Manager Console, click **Security** > **Certificate Management** > **Enrollment Request**.
2. In the Certificate Enrollment window, complete the following fields:
   - **Logical Name**: Type a logical name for the certificate to be assigned to the dedicated Recording server (for example, AMS2Cert).
   - **Bit length**: Select 1024, 2048, or 4096 from the list. If your security policy does not specify bit length, select **1024**.
   - **Common name**: Type the IP address.
   - **Enrollment password**: This password must match the current Enrollment Password that is configured on System Manager.
3. Click **Submit**.
   The certificate is automatically installed on the Element Manager Keystore.
4. In the navigation pane of the Element Manager Console, select **Feature Server Elements**, **Media Servers and Clusters**, **Media Servers**.

5. In the Media Servers window, select the dedicate Recording server.
6. Click **Edit (-/+)**.
7. In the Edit Media Server dialog box, complete the following fields:
   - **SIP Certificate**: Select the certificate you created from the list. This list corresponds to the logical names in the Keystore (for example, AMS2Cert).
   - **SOAP Certificate**: Select the certificate you requested from the list. This list corresponds to the logical names in the Keystore (for example, AMS2Cert).
8. Click **Apply**.

Co-resident deployments only

The steps involved in configuring recording for a co-resident deployment are much the same as the steps involved in configuring recording for a dedicated recording server deployment. However, the following procedure only applies to co-resident deployments.

Related topics:

Configuring recording for a media server cluster in a co-resident deployment on page 279

Configuring recording for a media server cluster in a co-resident deployment

About this task

Use this procedure to assign the Conferencing and Recording Role to a media server cluster in a co-resident deployment. This task applies to co-resident deployments which provide redundancy and co-resident deployments that do not provide redundancy. These non-redundant deployments are called simplex deployments. Avaya Aura® Conferencing provides redundancy using additional servers and a load balancer. In a redundant deployment, the main media server and additional secondary/back-up media servers are in a single cluster.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters**.
2. In the Media Server Clusters window, select the media server cluster, and click **Edit (+/-)**.
3. From the Role box in the Edit Media Server Cluster dialog box, select **CONFERENCING AND RECORDING**.

4. Click **Apply**.

Both deployments

The following procedures apply to dedicated recording server and co-resident deployments.

Related topics:

Assign a Recording media server cluster to locations on page 280
Configuring the Recording media server cluster for locations on page 281
Configuring the system-wide Recording setting on page 281
Configuring the recording feature for users on page 282
Configuring the Recording backup server on page 286

Assign a Recording media server cluster to locations

About this task

Use this procedure to assign a Recording media server cluster to locations.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Server Cluster for Recording** tab.
3. From the Select by box, select **Media Server Cluster**.
4. From the Select Recording Media Server Cluster box, select the appropriate Recording media server cluster.
5. In the Select Locations area, select the check box for each location you want to assign to the selected Recording media server cluster.
6. Click **Save**.

Configuring the Recording media server cluster for locations

About this task

Use this procedure to configure and assign a Recording media server cluster to locations.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Server Cluster Physical Location** tab.
3. From the Select by box, select **Location**.
4. From the Select Physical Location box, select the location to which you want to assign the Recording media server cluster.
5. From the Available Media Server Clusters box, select the Recording media server cluster (MediaServerCluster2), and then click **Copy**.
6. Click **Save**.
7. Click the **Media Server Cluster for Recording** tab.
8. From the Select by box, select **Media Server Cluster**.
9. From the Select Recording Media Server Cluster box, select the Recording media server cluster you created (MediaServerCluster2).
10. In the Select Locations area, select the check box for each location you want to assign to the selected Recording media server cluster.
11. Click **Save**.

Configuring the system-wide Recording setting

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to enable the system-wide setting for the Recording feature. The Recording feature enables users to record audio and web collaboration sessions. When the Recording feature is enabled for the system, you can then enable the Recording feature on a per user basis.

Procedure

1. In the Provisioning Client window, select **System Management > System Default Settings**.
2. On the System Default Settings tab, select (check) the **Allow recording** check box.
3. Click **Save**.

Configuring the recording feature for users

You can configure a single user at one time or you can configure multiple users at one time. In a typical deployment scenario, it is likely that you will enable recording for configure multiple users at one time.

Related topics:

Modifying a single user on page 282
Modifying multiple users at one time on page 283

Modifying a single user

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to configure the Recording feature for a user.

Note:

If you want to configure the Recording feature for multiple users at one time, you can use the Bulk Provisioning feature (**User Management > Bulk Provisioning**) in Provisioning Client.

Procedure

1. In the Provisioning Client window, select **User Management > Search Users**.
2. On the Advanced Search tab, click **Search** to view all provisioned users.
3. In the Login Name column, click on the Login Name of the user to whom you want to assign the Recording feature.
4. On the User page, click the **Actions** tab.
5. On the Actions tab, click **Conferencing**.

6. On the Conferencing User page, select (check) the **Enable Recording** check box.
7. Click **Save**.
8. Repeat Steps 2 through 7 for each user.

Modifying multiple users at one time

Before you begin

- You must be logged into Provisioning Client.
- Your login must have Expert mode privileges to perform this procedure.

Warning:

Any changes you make may cause the Provisioning Client data to become out of sync with the data in Avaya Aura® System Manager. You should only modify data to fix sync issues that cannot be resolved from the System Manager interface.

About this task

Use this procedure to modify the conference class of service, video (enable/disable) setting, and recording (enable/disable) setting for multiple users at one time (that is, bulk provisioning). In this procedure, you will identify the list of users you want to modify by specifying search criteria.

Procedure

1. In the Provisioning Client window, select **User Management > Bulk Provisioning**.
2. From the Field box, select the user criterion you want to search.
3. From the Operation box, select the search operation you want to perform.
4. In the Value box, specify the appropriate search information for the users.
5. Click **Add Criteria**.
6. Repeat Steps 2 through 5 to specify any other search criteria.
7. When finished specifying your search criteria, click **Search**.
   The user's who match your search criteria are displayed.
8. Click the check box for each user you want to modify.
9. In the Actions area, select the check box for each setting you want to modify for all of the selected users, and then select the appropriate value. See Bulk Provisioning page field descriptions on page 284.

10. Click **Assign**.

Related topics:

Bulk Provisioning page field descriptions on page 284

Bulk Provisioning page field descriptions

Name	Description
Field	Displays the field you want to search in the user data. Your choices are: • **Login Name** • **Communication Address Handle** • **Communication Address Domain** • **Last Name** • **First Name** • **Profile name** • **Video Enabled** • **Recording Enabled** • **Video Class** • **Directory Sync Status** There are three possible values for this field. - Pending (sync error or out of filter scope) - Synced from directory - Local user
Operation	Display the search operation you want to perform. Your choices are: • **Starts with** • **Contains** • **Equals**
Value	Displays the data you want to find in the specified user field.

Button	Description
Add Criteria	Adds the information you specified in the Field, Operation, and Value boxes into the search criteria list box.
Edit	Enables you to modify the selected search criterion .
Remove	Deletes the selected search criterion.
Remove all	Deletes all of the search criteria.
Search	Searches the user data using the displayed search criteria.

Name	Description
Directory Distinguished Name column	Displays an element which operates in conjunction with the search scope. It is the tree from which you would like to synchronize users. It is important to note that the domain part of the distinguished name is automatically based on the selected domain and cannot be changed. For example: `cn=Users,dc=example,dc=com display`.
Login name column	Displays the System Manager login name of each user.
Communication Profile	Displays the administered System Manager communications profile for each user.
Last Name	Displays the last name of each user.
First Name	Displays the first name of each user.

Name	Description
Conference Profile	Specify the conference class of service you want to assign to the selected users.
Enable Video	Specify whether video will be enabled or disabled for the selected users.
Enable Recording	Specify whether the Recording feature will be enabled or disabled for the selected users.
Delete User	Specify whether you would like to delete all selected users.

Configuring the Recording backup server

Before you begin

- The backup server must support the ssh protocol.
- You must have a user login (for example, admin) that can access the backup server and has read and write permissions for the backup folder.

About this task

Use this procedure to configure the server that will store backup files from the Recording server.

Procedure

1. Log on to the primary media server in the cluster as `ntsysadm` through ssh or directly on the server console.
2. Enter **`su -`** to log on as root.
3. At the prompt `password`, type the root password, and press **Enter**.
4. Type `configRecordingBackup.pl -backupuser <remote user ID> -backupip <IP address of backup server>`, and press **Enter**.
5. To verify that the configuration was successfully, type `ssh -i /admin/recording/bkrstr-recording_id_rsa <admin@remote server>`, and press **Enter** .
   You should be logged on to the backup server without being prompted for a password.
6. Repeat steps 1–5 for each recording media server cluster.
7. In the navigation pane of Element Manager Console, select **Addresses**.
8. In the Addresses window, click **Add (+)**.
9. In the Add IPv4 Address dialog box, complete the following fields:
   - **Logical Name**: Type the logical name for the backup server.
   - **IPv4 Address**: Type the IP address for the backup server.
10. Click **Apply**.
11. In the navigation pane of Element Manager Console, select **External Nodes**.
12. In the External Nodes window, click **Add (+)**.
13. In the Add External Node dialog box, complete the following fields:
    - **Logical Name**: Type another logical name for the backup server.
    - **IPv4 Address**: Type the IP address for the backup server.

14. Click **Apply**.
15. In the navigation pane of Element Manager Console, select **Recording > Backup Locations**.
16. In the Add Backup Locations dialog box, complete the following fields:
    - **Name**: Type the name of the backup server.
    - **Node**: Select the node for the backup server.
    - **Path**: Type the absolute path under which recordings should be stored on the backup server.
17. Click **Apply**.
18. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <*Cluster name*> > Recording > Backup/Purge Settings**.
    The Backup/Purge Settings dialog box appears.
19. If you want to schedule a backup and/or purge to be performed daily at a specific time:
    a. In the Schedule area, click Daily.
    b. Using the Time boxes, specify the hour and minute (in 24-hour format) at which you want the backup and/or purge to be performed.
    c. In the Actions area, click the check box of the process you want to schedule. If you want to schedule both a backup and a purge, select both the **Backup** check box and the **Purge** check box. If both the **Backup** check box and the **Purge** check box are checked, the purge process will delete only the recordings that have been backed up. If only the **Purge** check box is checked, the purge process will free space by deleting recordings regardless of whether the recordings are backed up.

       Note:

       - The purge process always deletes the oldest records first.
       - The timestamp is reset when recordings are restored to prevent the recordings from being immediately purged in the next purge process.
       - Changing the recording metadata (for example, by changing the title or by changing whether it is shared) will reset the backup flag and cause the file to be backed up again.

    d. From the Location box, select the appropriate setting.
    e. Click **Ok**.
20. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <*Cluster name*> > Recording > Purge Thresholds**.
21. In the Purge Thresholds dialog box, configure the thresholds at which an alarm will be triggered for disk space usage on the Recording media server recordings partition. Using the **Major Threshold** box and the **Critical Threshold** box, you can

set thresholds for major and critical alarms. Once a critical threshold is crossed, the purge job will start deleting the oldest recordings until disk space is freed at or below the value specified in the **Retain** box.

22. When finished, click **Ok**.

Chapter 18: Configuring a load balancer

Introduction to installing and configuring a load balancer

A load balancer is required when there are more than 1,500 users on a Personal Agent Manager (PAMgr) or when there are multiple Personal Agent Managers from a single domain or IP address. The load balancer can be configured within the demilitarized zone (DMZ) or without a DMZ.

Prerequisites

- The load balancer can be installed within or without a DMZ configuration. In a DMZ configuration, if users outside of the Enterprise require Collaboration Agent capabilities, the load balancer must be installed within the DMZ.
- The load balancer must be configured in a redundant model (1+1, active backup) configuration to avoid a single point of failure.
- If you have a firewall, open the required ports. See the documentation that came with your load balancer and this document.
- For installation and network configuration information, see the documentation that came with your load balancer.
- For capacity information about the Personal Agent Manager to determine if load balancing is required, see the *Avaya Aura® Conferencing Planning and Design* document.

Minimum requirements

- 1 Gigabit throughput
- real server support: 10
- high availability option
- layer 7 (HTTPS) load balancing
- SSL offloading

Load balancer without a DMZ

The following figure shows a load balancer that is deployed without a DMZ.

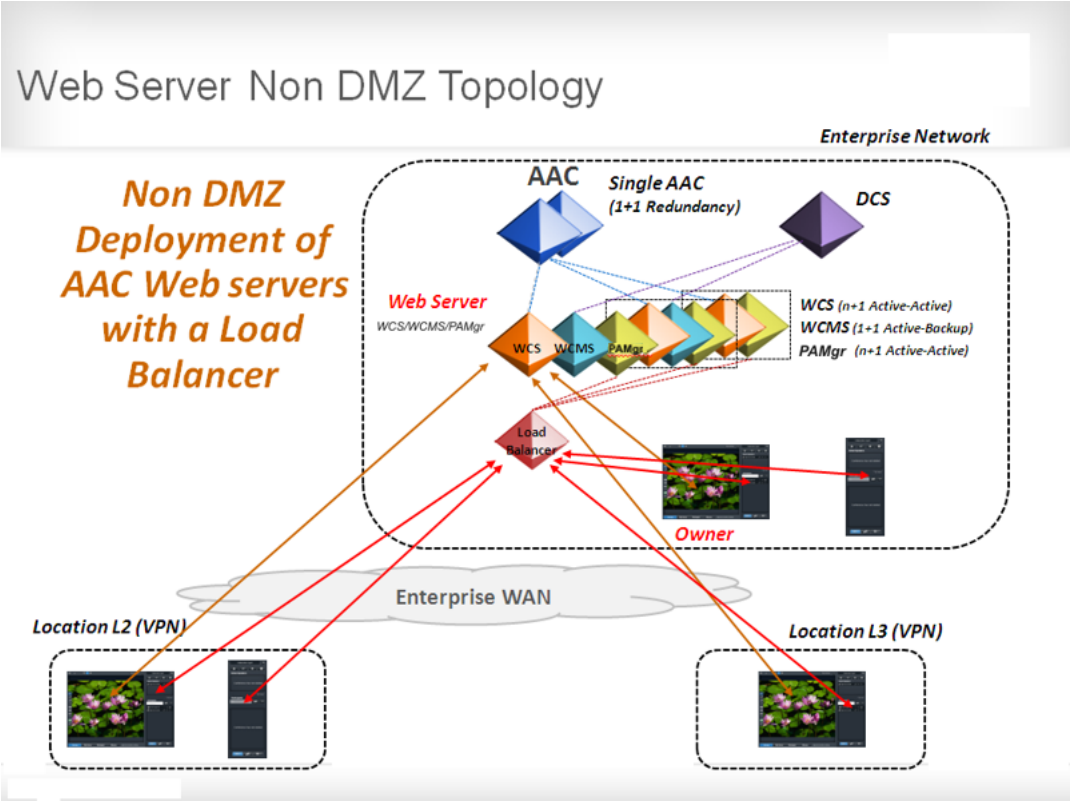


Figure 17: Load balancer deployment without a DMZ

Load balancer within a DMZ

The following figure shows a load balancer that is deployed within a DMZ.

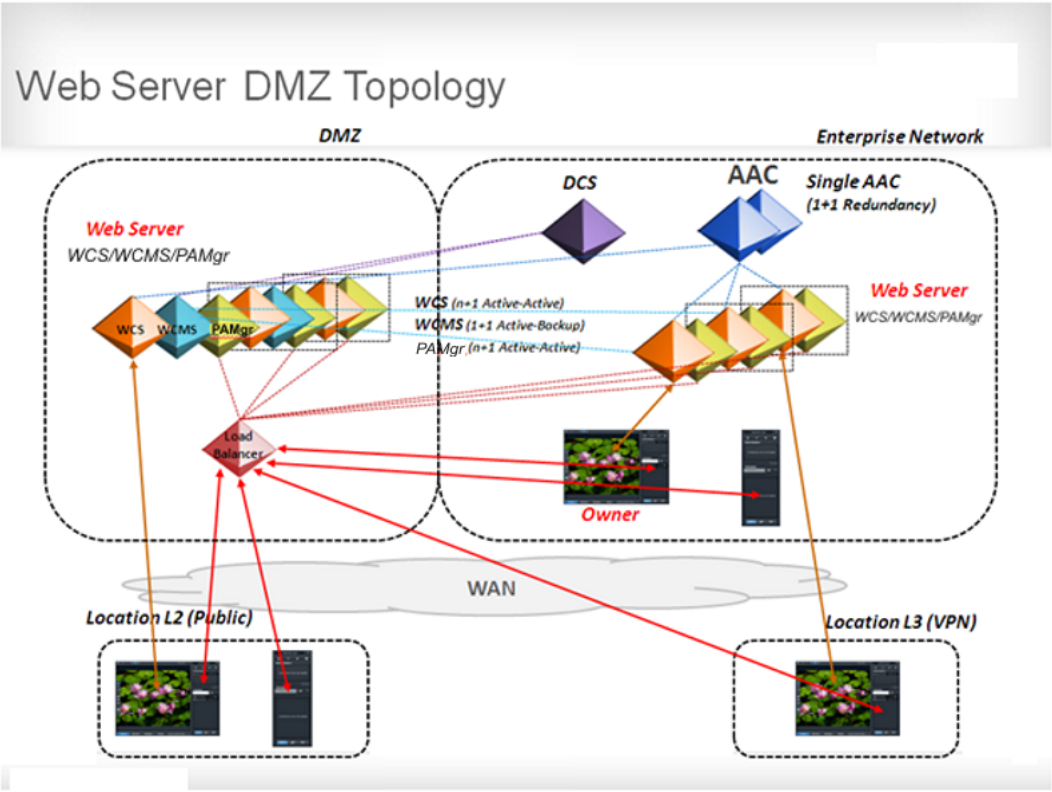


Figure 18: Load balancer deployment within a DMZ

Configuring a load balancer

Before you begin

You have a keyboard and monitor available for connecting to the load balancer.

About this task

Use the following procedure as a general guideline for configuring a load balancer. For more information, see the documentation that came with your load balancer.

Procedure

1. Connect a monitor and keyboard to the load balancer, and configure the WAN IP Address, as necessary for your network.
   - **IP address**
   - **Subnet mask**
   - **Default gateway**
   - **Primary DNS server**

- **Secondary DNS server**

2. Open the required firewall ports if your load balancer is located behind an Enterprise firewall.
   a. Port Direction TCP UDP usage:
      - 22 Out Yes No Technical support services
      - 53 Out Yes Yes Domain Name Service (DNS)
      - 80 Out Yes No IPS and firmware updates
      - 123 Out No Yes Network Time Protocol (NTP)
   b. Include any ports used by Services 1:1 NATs (as required) and any port required to access the virtual IP address of a load-balanced service.
3. Log on to the load balancer by connecting a computer (with a Web browser) to the same network as your load balancer.
   a. Type `http://<IP address of load balancer>:8000`, where :8000 is the default Web interface HTTP port.
   b. Log on to the load balancer as the administrator. For example, Username: admin and Password: admin.
4. Configure the LAN IP address of the load balancer (used in route-path only) and LAN netmask.

   Note:

   In a two-armed Route-Path mode, the LAN IP address acts as the default gateway for the real servers. In a one-armed Route-Path mode, the LAN IP address is used for management.
5. Configure the default host name and default domain name.
   - **Default Host Name**: This is used in system generated emails. For example, aacloadbalancer
   - **Default Domain**: This is used in the sender address for system emails. For example, ca.avaya.com
6. Optional: Configure the Proxy Server.
   - **Server Name/IP**: Enter a server name or IP address of the forward proxy that is required for accessing the internet. This is required to download firmware and other updates.
   - **TPC Port**: Enter **8000**.
   - **Username** and **Password**: Enter a username and password if your proxy requires this.
7. Configure a Layer 7 HTTPS service (one-armed route-path deployment).

Note:

This service accepts the HTTPS requests from the Collaboration Agent clients and directs to the real servers.

8. Add a new service.
   - **Service Name**: This is the new service name to identify the service.
   - **Service Type**: Use **Layer 7 - HTTPS**.
   - **Virtual IP Address**: This is the virtual IP address for the service. This IP address can be found on the WAN interface and becomes the IP address used by the clients to reach the load balanced service. For example, the Personal Agent Manager.
   - **SSL Certificate**: This certificate is the same as the certificate installed on the Personal Agent Manager servers.
   - **Real Server**: This is the IP address for the real servers that hold the application or content. The real servers must be on a separate subnet from the associated virtual IP address.
   - **Port**: This is the port for the given service. If the services uses multiple ports, enter **ALL**.
9. Configure the service to maintain client IP persistency. This is where requests from a single Collaboration Agent client are always directed to a single Personal Agent Manager.

   Note:

   If applicable, you can also configure a persistence time which allows routing to a different Personal Agent Manager when the client has been inactive after a configured time period.
10. Add the real servers under the configured service.

    Note:

    Ensure HTTPS/SSL is enabled on the real servers when adding them into the service.
11. Verify network connectivity by connecting to a system on your network to access the new service. Connect to the virtual IP address using the same method as used for a single server, for example, `https://47.11.47.247:8043/aacpa/`.

Chapter 19: Alarm and log forwarding to System Manager

Enabling alarm forwarding to System Manager

Before you begin

- You must have recorded the System Manager IP address, the Community, and TrapListener Port information from System Manager.
- You have created a logical name for System Manager.
- You have created an external node for System Manager.

About this task

Use the following procedure to enable forwarding of Avaya Aura® Conferencing alarms as SNMP traps to System Manager by configuring and enabling an SNMP manager on Avaya Aura® Conferencing.

Procedure

1. Log on to the Element Manager Console.
2. In the navigation pane, click **OAM Profiles** > **OSS Servers**.
3. Click **Add (+)**.
4. In the Add OSS Server dialog box, complete the following fields:
    - **Name**: Type a name, for example, SmgrOssServer.
    - **Node**: Choose **SmgrExtNode** from the list.
    - **Use External OAM Network**: Do not select this check box.
5. Click **Apply**.
6. In the navigation pane, click **OAM Profiles** > **SNMP Managers**.
7. Click **Add (+)**.
8. In the Add SNMP Manager dialog box, complete the following fields:
    - **Name**: Type a name, for example, SmgrSnmpManager.
    - **Community**: Type the community string as obtained from System Manager.

- **Servers**: Select the server name you created in Step 4, for example, SmgrOssServer.
- **Trap Port**: Type the Trap Listener port number as obtained from System Manager.

9. Click **Apply**.
10. To restart Element Manager, perform the following:
    a. Log on to the server hosting EMServer instance 0 through ssh or the server console. At the logon prompt, type ntappadm or logon to an account with the AA role assigned.
    b. Type `./emStop.pl`, and press **Enter** to stop Element Manager.
    c. Type `./emStart.pl`, and press **Enter** to start Element Manager.
11. If you have a redundant instances of Element Manager, repeat Steps 1 through 10 for each instance.

Disabling alarm forwarding to System Manager

About this task

Use the following procedure to disable Avaya Aura® Conferencing alarm forwarding to System Manager.

Procedure

1. Log on to the Element Manager Console.
2. In the navigation pane, click **OAM Profiles** > **SNMP Managers**.
3. Click **SmgrSnmpManager**, and click **Delete (-)** to delete the SNMP manager.
4. In the navigation pane, click **OAM Profiles** > **OSS Servers**.
5. Click **SmgrOssServer**, and click **Delete (-)** to delete the OSS server.
6. Restart Element Manager, perform the following:
    a. Navigate to **Feature Server Elements** > **Element Manager** > <*Element Manager NE*> > **NE Maintenance**.
    b. Select the EM instance to restart.
    c. Click **Restart**.
7. Log on to the server hosting EMServer instance 0 through ssh or the server console. At the logon prompt, type ntappadm or logon to an account with the AA role assigned.
    a. Type `./emStop.pl`, and press **Enter** to stop Element Manager.

b. Type `./emStart.pl`, and press **Enter** to start Element Manager.

8. If you have a redundant instances of Element Manager, repeat Steps 1 through 7 for each instance.

Checklist for forwarding logs to System Manager

The following checklist provides the high-level steps required to enable forwarding of the Avaya Aura® Conferencing logs to System Manager.

#	Task	Description	Notes	✔
1	Review the prerequisites.	You have the following privileges: • root access to Element Manager server • access to the Element Manager Console • access to System Manager		
2	Generate enrollment password on System Manager and record information for future reference.	See Generating enrollment password on on page 298.		
4	Configure Element Manager logs UDP transport client feed rule for forwarding to System Manager.	See Configuring Element Manager log UDP client feed rule on page 298.		
5	Enable the logAgent to allow Element Manager logs to be forwarded to System Manager. A trust certificate is automatically installed in the SPIRIT agent for	See Enabling log forwarding to on page 300.		

#	Task	Description	Notes	✔
	secure communication.			

Generating enrollment password on System Manager

About this task

Use the following procedure to generate the enrollment password on System Manager.

Procedure

1. Log on to System Manager.
2. On the System Manager console, click **Services** > **Security**.
3. In the navigation pane, click **Certificates**.
4. Click **Enrollment Password**.
5. In the **Password expires in** field, select **4 week(s)**.
6. In the **Password** field, type a new password.

   Record the FQDN or IP address and the enrollment password for future reference.
7. Click **Generate**.
8. Click **Commit**.

Next steps

Proceed to configuring Element Manager log UDP client feed rule.

Configuring Element Manager log UDP client feed rule

Element Manager logs can be sent to System Manager through the UDP transport to `/var/log/mcpacl`. The SPIRIT agent then forwards the logs to System Manager.

About this task

Use this procedure to configure a log UDP client feed rule on Element Manager.

Procedure

1. Log on to the Element Manager Console.
2. In the navigation pane of Element Manager Console, select **Addresses**.
3. In the Addresses window, click **Add (+)** .
4. In the Add IPv4 Address dialog box, complete the following fields:
   - **Logical Name**: Type `Localhost`.
   - **IPv4 Address**: Type `127.0.0.1`.
5. Click **Apply**.
6. In the navigation pane, click **External Nodes**.
7. In the External Nodes window, click **Add (+)** .
8. In the Add External Node dialog box, complete the following fields:
   - **Name**: Type `LocalhostNode`.
   - **IPv4 Address**: Select **Localhost** from the list.
9. Click **Apply**.
10. In the navigation pane, click **OSS Profiles** > **OSS Servers**.
11. In the OSS Servers window, click **Add (+)** .
12. In the Add OSS Server dialog box, complete the following fields:
    - **Name**: Type `LocalhostServer`.
    - **Node**: Select **LocalhostNode** from the list.
    - **Use External OAM Network**: Do not select the check box.
13. Click **Apply**.
14. In the navigation pane, click **OAM Profiles** > **OSS Endpoints**.
15. In the OSS Endpoints window, click **Add (+)** .
16. In the Add OSS Endpoint dialog box, complete the following fields:
    - **Name**: Type `Localhostsyslog`.
    - **Server**: Select **LocalhostServer**.
    - **Port**: Type `514`.
17. Click **Feature Server Elements** > **Element Manager** > **ElementManager** > **Log Processing** > **Log UDP Client Feed Rules**.
18. In the ElementManager Log UDP Client Feed Rules window, click **Add (+)** .
19. In the Add Log UDP Client Feed Rule dialog box, complete the following fields:
    - **Name**: Type `SecurityAuditSyslog`.

- **Log Format**: Select **ACL**.
- **Log Filter**: Select **security**.
- **UDP Client Feed Rule**: Select the Localhostsyslog endpoint from the list on the left, and click **>>** to move to the list on the right.

20. Click **Apply**.
21. In the ElementManager Log UDP Client Feed Rules window, click **Add (+)** .
22. In the Add Log UDP Client Feed Rule dialog box, complete the following fields:
    - **Name**: Type `NonSecurityAuditSyslog`.
    - **Log Format**: Select **ACL**.
    - **Log Filter**: Select **NonSecurity**.
    - **UDP Client Feed Rule**: Select the Localhostsyslog endpoint from the list on the left, and click **>>** to move to the list on the right.
23. Click **Apply**.
24. In the navigation pane, click **Feature Server Elements** > **Element Manager** > **ElementManager** > **Log Processing** > **Log Rule Maintenance**.
25. In the ElementManager Log Processing Rules Maintenance window, click **Add (+)** .
26. Click the **UDP Client Feed** tab.
27. Click the name **SecurityAuditSyslog**, and click **Enable**.
28. Click the name **NonSecurityAuditSyslog**, and click **Enable**.
29. If you have a redundant instances of Element Manager, repeat Steps 17 through 28 for each instance.
30. On the **File** menu, click **Exit** to exit the Element Manager Console.

Result

You have configured a log UDP client feed rule on Element Manager

Next steps

Proceed to enabling log forwarding to System Manager.

Enabling log forwarding to System Manager

About this task

Use the following procedure to enable log forwarding to System Manager.

Procedure

1. Log on to the Element Manager server as the root user.
2. Type **logAgent enable <smgr-host> <smgr-port> <e-password>**, and press **Enter**.

   where:

   - smgr-host is the FQDN or IP address of System Manager.
   - smgr-port is the https port of System Manager.
   - e-password is the enrollment password (unexpired).
3. If you have a redundant instances of Element Manager, repeat Steps 1 and 2 for each instance.

Disabling log forwarding to System Manager

About this task

Use the following procedure to disable log forwarding to System Manager.

Procedure

1. Log on to the Element Manager server as the root user.
2. Type `logAgent disable`, and press **Enter**.
3. Log on to the Element Manager Console as admin.
4. In the navigation pane, click **Feature Server Elements** > **Element Manager** > **ElementManager** > **Log Processing** > **Log Rules Maintenance**.
5. Click the **UDP Client Feed** tab.
6. Click the line for SecurityAuditSyslog, and click **Disable**.
7. Click the line for NonSecurityAuditSyslog, and click **Disable**.
8. On the **File** menu, click **Exit** to exit the Element Manager Console.

Chapter 20: Secure Access Link Gateway

Secure Access Link Gateway overview

With Avaya Aura® Conferencing, the Secure Access Link (SAL) provides remote access to the Avaya Aura® Conferencing servers through SSH, to the Provisioning Manager using HTTPS, and to the Element Manager Graphical User Interface (GUI). SAL can also be configured to receive SNMP alarms from Avaya Aura® Conferencing.

Depending on the deployment layout, either the integrated System Manager SAL gateway or an external standalone SAL gateway can be used to manage the Avaya Aura® Conferencing solution. The System Manager integrated SAL gateway can be used to manage a maximum of 10 individual or a combination of instances of Session Managers and Avaya Aura® Conferencing elements. For deployments that exceed 10 Session Managers or Avaya Aura® Conferencing elements, an external SAL gateway must be used.

Enabling alarm forwarding to the SAL gateway

Before you begin

- You have recorded the Secure Access Link (SAL) gateway IP address, the Community, and TrapListener Port information from the SAL gateway.
- You have created a logical name for the SAL gateway IP address.
- You have created an external node for the SAL gateway

Note:

This is required in Step 4 of the following procedure.

About this task

Use the following procedure to enable forwarding of Avaya Aura® Conferencing alarms as SNMP traps to the SAL gateway by configuring and enabling an SNMP manager on Avaya Aura® Conferencing.

Procedure

1. Log on to the Element Manager Console.

2. In the navigation pane, select **OAM Profiles** > **OSS Servers**.
3. Click **Add (+)**.
4. In the **Add OSS Server** dialog box, complete the following fields:
   - **Name**: Type a name, for example, SALgwOssServer.
   - **Node**: Choose the external node that was previously created.
   - **Use External OAM Network**: Do not select this check box.
5. Click **Apply**.
6. In the navigation pane, click **OAM Profiles** > **SNMP Managers**.
7. Click **Add (+)**.
8. In the **Add SNMP Manager** dialog box, complete the following fields:
   - **Name**: Type a name, for example, SALgwSnmpManager.
   - **Community**: Type the community string as obtained from the SAL gateway.
   - **Servers**: Select the server name you created in Step 4, for example, SALgwOssServer.
   - **Trap Port**: Type the Trap Listener port number as obtained from SAL gateway.
9. Click **Apply**.
10. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Element Manager** > **Element Manager** > **Alarm Processing** > **SNMP Managers**.
11. Click **Add (+)**.
12. Select the SNMP manager you added in Step 8, for example, SALgwSnmpManager.
13. Click **Delete (-)**.
14. Click **Apply**.
15. To restart Element Manager, perform the following:
    a. Log on to the server hosting EMServer instance 0 through ssh or the server console. At the logon prompt, type `ntappadm` or logon to an account with the AA role assigned.
    b. Type `./emStop.pl`, and press **Enter** to stop Element Manager.
    c. Type `./emStart.pl`, and press **Enter** to start Element Manager.

Disabling alarm forwarding to the SAL gateway

About this task

Use the following procedure to disable Avaya Aura® Conferencing alarm forwarding to the Secure Access Link (SAL) gateway.

Procedure

1. Log on to the Element Manager Console.
2. In the navigation pane, click **Feature Server Elements** > **Element Manager** > **Element Manager** > **Alarm Processing** > **SNMP Managers**.
3. Click **SALgwSnmpManager**, and click **Delete (-)**.
4. In the navigation pane, click **OAM Profiles** > **SNMP Managers**.
5. Click **SALgwSnmpManager**, and click **Delete (-)** to delete the SNMP manager.
6. In the navigation pane, click **OAM Profiles** > **OSS Servers**.
7. Click **SALgwOssServer**, and click **Delete (-)** to delete the OSS server.

Chapter 21: Configuring Communication Manager system parameters

Checklist for Communication Manager parameter settings

Avaya Aura® Conferencing requires specific settings be enabled for Communication Manager.

The following checklist identifies the parameters required for configuring the Communication Manager using the System Manager for Avaya Aura® Conferencing. For more information about configuring the following parameters, see *Administering Avaya Aura® System Manager*.

#	Task	Description	Notes	✔
1	Verify or modify the following feature-related system parameters: • Multimedia Call Handling (Basic) • Multimedia Call Handling (Enhanced) • Multimedia IP SIP Trunking • Direct IP-IP Audio Connections • IP Audio Hairpinning • SIP Endpoint Managed Transfer	See Modifying system parameters on page 308.		
2	Verify or modify the following for Signaling groups: • Direct IP-IP Audio Connections • Initial IP-IP Direct Media	See Modifying Signaling Groups on page 309.		

#	Task	Description	Notes	✔
	• IP Audio Hairpinning • DTMF over IP			
3	View or modify the following IP options system parameters: • Intra-System IP DTMF Transmission Mode • Override ip-codec-set for SIP direct-media connections	See Modifying IP options system parameters on page 310.		
4	View or modify the following settings for each IP codec set: • Allow Direct-IP Multimedia • Maximum Call Rate for Direct-IP Multimedia • Maximum Call Rate for Priority Direct-IP Multimedia	See Modifying IP codec sets on page 311.		

Modifying Communication Manager system parameters

About this task

Use the following procedure to verify or modify the system parameters.

Procedure

1. Log on to System Manager as admin.
2. On the System Manager console, click **Elements >** Communication Manager.
3. In the navigation pane, click **Parameters > System Parameters – Customer Options**.
4. On the System Parameters – Customer Options screen, select the appropriate device, and click **View**.
5. Click **Next Page** to go to page 4.
6. On page 4, verify the following:

- **Multimedia Call Handling (Basic)** is set to **Y**.
- **Multimedia Call Handling (Enhanced)** is set to **Y**.
- **Multimedia IP SIP Trunking** is set to **Y**.

Note:

If these system parameters are not set correctly, contact Avaya support.

7. In the navigation pane, click **Parameters > System Parameters – Features**.
8. On the System Parameters – Features screen, click **New**.
9. Click **Prev Page** to go to page 19.
10. In the IP Parameters section, verify or change the following:
    - **Direct IP-IP Audio Connections** to **Y**.
    - **IP Audio Hairpinning** to **N**.
    - **SIP Endpoint Managed Transfer** to **Y**.
11. Press **Enter** to save your changes.

Result

You have verified or changed the IP parameters.

Modifying Signaling Groups

About this task

Use the following procedure to verify or modify the SIP direct media parameters.

Procedure

1. Log on to System Manager as admin.
2. On the System Manager console, click **Elements > Communication Manager**.
3. In the navigation pane, click **Network > Signaling Groups**.
4. Click the check box of the appropriate signaling group, and then click **Edit**.
5. Verify or modify **Direct IP-IP Audio Connections** to **Y**.
6. Verify or modify **Initial IP-IP Direct Media** to **Y**.
7. Verify or modify **IP Audio Hairpinning** to **N**.
8. Verify or modify **DTMF over IP** to **rtp-payload**.

9. Repeat Steps 4 on page 309 to 8 on page 309 for the other group number, for example 128.

Optional: Modifying IP network region for private numbering

About this task

Use the following procedure to verify or modify private numbering. This procedure is optional if region 1 already exists.

Procedure

1. Log on to System Manager as admin.
2. On the System Manager console, click **Elements** > **Communication Manager**.
3. In the navigation pane, click **Network** > **IP Network Regions**.
4. Click the option button for the appropriate region, and then click **Edit**.

Result

The private numbering is verified or modified.

Modifying IP options system parameters

Before you begin

You must use the *init* Login ID for this procedure.

About this task

Use the following procedure to view or modify the IP options system parameters.

Procedure

1. Open your Web browser and in the Address bar, type the IP address for the Communication Manager System Management Interface (SMI).
2. At the Logon ID prompt, type `init`, and click **Logon**.
3. Type your password, and click **Logon**.
4. On the Administration menu, click **Native Configuration Manager**.

5. In the Server Login window, type your Logon ID, and click **OK**.
6. Type your password, and click **OK**.
7. In the Command field, type `change system-parameters ip-options`, and click **Send**.
8. On the IP-options system parameters page, click **NEXT PAGE** to navigate to page 2.
9. In the **Intra-System IP DTMF Transmission Mode** field, select **rtp-payload**.
10. Click **NEXT PAGE** twice to navigate to page 4.
11. In the **Override ip-codec-set for SIP direct-media connections** field, type **y**.
12. Click **Enter**.
13. Close the Native Configuration Manager window.
14. In the Communication Manager system Management Interface (SMI) window, click **Logoff**.
15. Click **Log Off**.

Modifying IP codec sets

About this task

Use the following procedure to view or modify the IP codec sets for Communication Manager.

Procedure

1. Open your Web browser and in the Address bar, type the IP address for the Communication Manager System Management Interface (SMI).
2. At the Logon ID prompt, type your Logon ID, and click **Logon**.
3. Type your password, and click **Logon**.
4. On the Administration menu, click **Native Configuration Manager**.
5. In the Server Login window, type your Logon ID, and click **OK**.
6. Type your password, and click **OK**.
7. In the Command field, type `change ip-codec-set #`, where `#` is the IP codec set you want to modify, and click **Send**.
8. On the IP Codec Set page, click **NEXT PAGE** to navigate to page 2.
9. In the **Allow Direct-IP Multimedia** field, type **y**.

10. In the **Maximum Call Rate for Direct-IP Multimedia** field, type **15360**. This setting is necessary for video.
11. In the **Maximum Call Rate for Priority Direct-IP Multimedia** field, type **15360**. This setting is necessary for video.
12. Click **Enter**.
13. Repeat Steps 7 through 12 for each IP codec set.
14. When finished, close the Native Configuration Manager window.
15. In the Communication Manager system Management Interface (SMI) window, click **Logoff**.
16. Click **Log Off**.

Chapter 22: Integrating Avaya Aura® Conferencing with LDAP directory servers

This chapter describes the procedures to configure Avaya Aura® Conferencing to synchronize its database with LDAP directory servers. The LDAP directory integration feature enables an enterprise administrator to regularly synchronize the Avaya Aura® Conferencing database with LDAP directories. When Avaya Aura® Conferencing is integrated with LDAP directory servers, the conferencing subscriber data is managed in the LDAP directory. When a user logs into Avaya Aura® Conferencing via Collaboration Agent or a mobile client, the user will be authenticated directly against the password in the LDAP directory.

Note:

Avaya Aura® Conferencing supports any directory server that supports LDAP (for example, Microsoft® Active Directory 2003 and 2008 and OpenLDAP).

Pre-deployment checklist for LDAP integration

The following checklist provides the high level steps and considerations prior to beginning your integration of Avaya Aura Conferencing with LDAP directory servers.

#	Task	Notes	✔
1	Obtain the list of directory domains (including child domains or sub-domains) from which enterprise users will be added as Avaya Aura® Conferencing users. Examples of directory domains are `avaya.com`, `ca.avaya.com`, and `avaya.uk`.		
2	Obtain the list of LDAP directory servers in each domain. For each directory server, you must have: • IP address • port		

#	Task	Notes	✔
	• connection credentials (user distinguished name and password) of a user with read access to the directory servers in the domain • A maximum of two redundant servers for synchronization • As many redundant servers as required for authentication. These servers can be the same redundant servers used for synchronization.		
3	Obtain the list of physical sites in which the Avaya Aura® Conferencing network elements are deployed to determine the list of authentication servers the network elements will try. Examples of physical sites are `Enterprise Intranet` and `Enterprise DMZ`.		

LDAP integration tasks

You must perform the following tasks to integrate Avaya Aura® Conferencing with LDAP directory servers.

#	Task	Description	Notes	✔
1	Review the prerequisites.	See Pre-deployment checklist for LDAP integration on page 313.		
2	Add each physical site in which Avaya Aura® Conferencing network elements are deployed, and assign these sites to the appropriate servers.	See Configuring the physical sites on page 316.		
3	Add the IP address, add an external node, and configure the port	See Configuring the IP addresses and		

#	Task	Description	Notes	✔
	for each directory server.	ports for the directory servers on page 317.		
4	Add the directory domains that contain the enterprise users you want to add as Avaya Aura® Conferencing users.	See Adding the directory domains on page 319.		
5	Configure the connection, synchronization, and authentication settings for the directory domains you added.	See Configuring directory servers on page 319.		
6	Configure the directory synchronization service.	See Configuring the directory synchronization service on page 321.		
7	Configure the timeout settings for directory authentication.	See Configuring the directory authentication service on page 325.		
8	Configure the directory access passcode settings for each directory domain.	See Configuring the directory access passcode settings on page 326.		
9	If you added multiple directory domains in Step 4, configure those additional directory domains.	See Configuring multiple directory domains on page 328.		
10	Provision manually on Avaya Aura® System Manager each user that is synchronized from the LDAP directory.	See Configuring LDAP directory-synchronized users on System Manager on page 328.		
11	If you are using TLS to connect to the Active Directory server, retrieve the CA certificate from the	See Retrieving the CA certificate from the Active Directory server on page 330.		

#	Task	Description	Notes	✔
	Active Directory server.			

Configuring the physical sites

Before you begin

You must have the list of physical sites in which the Avaya Aura® Conferencing network elements are deployed.

About this task

Use this procedure to add each physical site in which the Avaya Aura® Conferencing network elements are deployed and assign these sites to the appropriate servers.

Procedure

1. In the navigation pane of Element Manager Console, select **Physical Sites**.
2. In the Physical Sites window, click **Add (+)**.
3. In the Add Site dialog box, complete the following fields:
   - **Name**: Enter a short name for the site (for example, `EnterIntranet`).
   - **Long Name**: Enter the full name for the site (for example, `EnterpriseIntranet`).
4. Click **Apply**.
5. Repeat Steps 2 through 4 for each physical site you want to configure.
6. In the navigation pane of Element Manager Console, select **Servers**.
7. In the Servers window, select **EMServer1**, and then click **Edit (-/+)**.
8. From the Physical Site box in the Edit Server dialog box, select the appropriate site you added in Steps 2 through 4.
9. Click **Apply**.
10. Repeat Steps 7 through 9 for each server displayed in the Servers window.
11. Click **Apply**.

Comments? infodev@avaya.com

Configuring the IP addresses and ports for the directory servers

Before you begin

For each directory server, you must know:

- the IP address
- whether the directory server is configured for secure access
- the port number

About this task

Use this procedure to add the IP address, add an external node, and configure the port for each directory server.

Procedure

1. In the navigation pane of Element Manager Console, select **Addresses**.
2. In the Addresses window, click **Add (+)**.
3. In the Add IPv4 Address dialog box, complete the following fields:
   - **Logical Name**: Type the logical name for the directory server (for example, `LDAP1`).
   - **IPv4 Address**: Type the IP address for the directory server.
4. Click **Apply**.
5. Repeat Steps 2 through 4 for each directory server.
6. In the navigation pane of Element Manager Console, select **External Nodes**.
7. In the External Nodes window, click **Add (+)**.
8. In the Add External Node dialog box, complete the following fields:
   - **Name**: Type a name for the directory server (for example, `LDAP1Node`).
   - **IPv4 Address**: Select the appropriate directory server address you added in Steps 2 through 4.
9. Click **Apply**.
10. Repeat Steps 7 through 9 for each directory server address you added in Steps 2 through 4.
11. In the navigation pane of Element Manager Console, select **Directory Access Servers**.
12. In the Directory Access Servers window, click **Add (+)**.

13. In the Add Directory Access Server dialog box, complete the following fields:
    - **Short Name**: Type the short name of the directory server (for example, `LDAP1`).
    - **Long Name**: Type the long name of the directory server (for example, `LDAPServer1`).
    - **Node**: Select the directory server node you added previously (for example, **LDAP1Node**).
    - **Enable TLS Port**: If the directory server is configured for secure access, select this check box. When this check box is selected, port 636 will be used by default. To change the port, enter the port you want to use.
    - **Enable TCP Port**: If the directory server is configured for non-secure access, select this check box. When this check box is selected, port 389 will be used by default. To change the port, enter the port you want to use.
14. Click **Apply**.
15. Repeat Steps 11 through 13 for each directory server node you added in Steps 7 through 9.

Note:

If an LDAP directory server is configured with a TLS certificate that is signed by a non-System Manager Certificate Authority, you must export a copy of the Certificate Authority certificate and place the certificate in **Security > Truststore** in Element Manager Console. See Retrieving the CA certificate from the Active Directory server on page 330.

Optionally, if any of the directory servers are configured for mutual/client authentication, you must set the respective certificate/key in **Security > Keystore** in Element Manager Console to **Directory Server certificate** for the following network elements:

- Application Server
- Provisioning Manager
- Personal Agent Manager

To change the certificate/key to **Directory Server certificate** for these network elements, see Assigning the Directory Server Certificate for the network elements on page 331.

Adding the directory domains

Before you begin

You must know the directory domains (including child domains or sub-domains) from which enterprise users will be added as Avaya Aura® Conferencing users.

About this task

Use the following procedure to add the directory domains that contain the enterprise users you want to add as Avaya Aura® Conferencing users.

Procedure

1. In the Provisioning Client window, select **System Management > User Domains**.
2. In the User Domain box, enter the directory domain you want to add.
3. Click **Add**.
   The directory domain appears at the bottom of the User Domain list.
4. Repeat Steps 2 and 3 for each directory domain you want to add.

Configuring directory servers

Before you begin

You must know the distinguished name and password of a user with read access to the directory servers in each domain (for example, `cn=administrator,cn=Users,dc=ca,dc=canada,dc=com`).

About this task

Use the following procedure to configure the connection, synchronization, and authentication settings for the directory domains you added.

Procedure

1. In the Provisioning Client window, select **System Management > Directory Access Services > Directory Servers**.
2. Click the **Connection Credentials** tab.
3. From the Select domain box, select the directory domain you want to configure. The Select domain box displays all the directory domains you have added.

4. In the Connection Principal box, enter the distinguished name of a user with read access to the directory servers in the selected domain (for example, `cn=administrator,cn=Users,dc=ca,dc=canada,dc=com`).
5. In the Connection Password box, enter the password of the user you entered in Step 4.
6. Click **Save**.
7. Click the **Synchronization Servers** tab.
8. From the Select domain box, select the directory domain you want to configure.
9. From the Primary Server box, select the primary server used for synchronization.
10. Perform one of the following steps:
    - If there is a redundant server, select the redundant server from the Secondary Server box.
    - If there is not a redundant server, select **Not Selected** from the Secondary Server box.
11. Click **Save**.
12. Click the **Authentication Servers** tab.
13. From the Select domain box, select the directory domain you want to configure.
14. From the Physical Site box, select the physical site of the Application Server or Provisioning Manager server. (Both of these servers usually reside together on your intranet.)
15. From the Authentication Server box, select the directory server that the Provisioning Manager server should try first for authentication for the domain.
16. Click **Add**.
    The information you entered appears at the top of the table.
17. Repeat Steps 14 through 16 for all other directory servers that the Provisioning Manager server can try for authentication for the domain.

    Note:

    The order in which the information is displayed in the table indicates the order in which the authentication servers are queried. Be sure to prioritize the list of authentication servers for each physical site based on availability or network access.
18. From the Physical Site box, select the physical site of Personal Agent Manager. (This site can reside in the DMZ.)
19. From the Authentication Server box, select the directory server that the Personal Agent Manager network element should try first for authentication for the domain.
20. Click **Add**.
    The information you entered appears at the top of the table.

21. Repeat Steps 19 and 20 for all other directory servers that the Personal Agent Manager network element can try for authentication for the domain.

    Note:

    The order in which the information is displayed in the table indicates the order in which the authentication servers are queried. Be sure to prioritize the list of authentication servers for each physical site based on availability or network access.

22. Repeat Steps 18 through 21 for all other Personal Agent Manager servers in the Avaya Aura Conferencing deployment.

    Note:

    Be sure to prioritize the list of authentication servers for each physical site based on availability or network access.

Configuring the directory synchronization service

Before you begin

You must have the following information:

- the Provisioning Manager you want to perform the synchronization
- the directory distinguished name from which users must be synchronized for the domain
- the directory attribute of the directory user that you want to map to the login name for Avaya Aura® Conferencing
- the directory attributes that you want to map to the Avaya Aura® Conferencing fields

About this task

Use the following procedure to:

- configure the directory synchronization service settings
- test the connection and schema settings
- configure directory filters for a specific user domain
- perform a synchronization
- schedule a synchronization to be performed

Procedure

1. In the Provisioning Client window, select **System Management > Directory Access Services > Synchronization Service**.

2. Click the **Sync Configuration** tab.
3. From the Select Provision manager for sync box, select the Provisioning Manager network element that you want to perform the synchronization.
4. In the Connection Timeout (milliseconds) box, enter the connection timeout in milliseconds for synchronization. If the directory synchronization client cannot establish a connection within the period you specify, the client aborts the synchronization attempt.

   Note:

   If you enter 0, the connection timeout is handled by TCP protocol.
5. In the Read Timeout (milliseconds) box, enter the read timeout in milliseconds for synchronization. If the directory synchronization client does not receive a read response within the period you specify, the client aborts the read attempt.

   Note:

   If you enter 0, there is not timeout, and the system will wait for the read operation to complete.
6. Click **Save**.
7. Click the **Sync Schema** tab.
8. From the Select domain box, select the directory domain you want to configure.
9. In the Directory distinguished name box, enter the directory distinguished name (base distinguished name or root distinguished name) from which the users must be synchronized for the domain (for example, `cn=Users,dc=ca,dc=avaya,dc=com`).
10. In the Login name box, enter the directory attribute of the directory user that you want to map to the login name for Avaya Aura Conferencing.
11. Enter all other directory attributes that you want to map to the Avaya Aura Conferencing fields displayed on this page.

    You must specify the following fields:

    - First name
    - Last name
    - Communication address handle

      The Communication address handle is a communication address without a domain. For example, if the communication address is *12345@yourcompany.com*, the handle is *12345*. If you map the email field from the directory to this field, you may receive the wrong communication address after the synchronization. For example, you may receive data with the domain repeated twice (*12345@yourcompany.com@yourcompany.com*). The domain is added automatically to the communication address handle during synchronization.

Note:

Make sure you map the following fields to unique fields in the directory:

- Moderator access code
- Participant access code
- Moderator passcode
- Participant passcode

12. When finished, click **Save**.
13. Click the **Query Test Tool** tab and test the connection and schema settings.

    Using Query Test Tool tab, you can test the connection and schema settings at any time. To test the LDAP query, you must specify an LDAP filter. For example, you may try the filter “cn=*”. This filter will query all users under the base distinguished name you specified in the schema.
14. Click the **Sync Filter & Defaults** tab.

    Using the Sync Filter & Defaults tab, you can configure directory filters for a specific user domain.

    You must define one filter for each group of users you want to synchronize from the directory server. For example, if you want to synchronize users with the job title “engineer,” you may define the filter “title=engineer.” You can set a specific template for these users. Then, you may define a filter and default for managers. For example, this filter could be “title=manager” with a more advanced template “executive_passcodes.”

    Note:

    Keep in mind the following:

    - Synchronization will not occur unless at least one filter is configured.
    - A filter with an empty filter value is equivalent to “query all users”.

    The syntax of the filter string is defined by RFC 2254, The String Representation of LDAP Search Filters. This RFC may be used as a reference for constructing more complex filter strings.

    A filter is a UTF-8 formatted string that has the following syntax:

    (*attribute operator value*)

    or

    (*operator(filter1)(filter2)*)

    where *filter1* and *filter2* have the syntax displayed on the first line, and the operator is a string operator. The *attribute* corresponds to an LDAP attribute that exists in the directory, and value corresponds to the actual data value that is requested for the attribute. An example filter is `(&(ou=Austin)(sn=Miller))`. This filter

returns all users whose last name is “Miller” and also have the organization unit “Austin.”

An attribute specified in the filter can be any attribute that exists in the LDAP directory, and it is not required to be one of the attributes (specified in translation schema) that is imported by Provisioning Manager. The attribute is used only on the LDAP server to select data, and the corresponding entries will have a subset of their data imported (based on the translation schema).

15. To configure a directory filter for a user domain, perform the following steps:
    a. From the Select domain box, select the directory domain you want to configure.
    b. In the Name box, enter the name for this filter.
    c. In the Filter box, enter the string representation of an LDAP search filter.
    d. If you want to use a specific template, select the appropriate template from the Template box.
    e. If you want to use a specific location, select the appropriate location from the Location box.
    f. If you want to use a specific locale, select the appropriate locale from the Local box.
    g. If you want to use a specific time zone, select the appropriate time zone from the Time zone box.
    h. In the Communication profile box, enter the appropriate communication profile (for example, `Primary`).
    i. Click **Save**.
    The new filter appears at the bottom of the table.

    Note:

    The order in which the filters are displayed in the table indicates the order in which the filters are run.

16. Repeat Step 15 if you want to create another filter.
17. Click the **Sync Scheduler** tab.
18. If you want to perform a synchronization now, click **Sync Now**.
19. If you want to schedule a synchronization for a specific time and at a specific frequency (daily, weekly, and/or monthly), perform the following steps:
    a. Click the **Enable scheduled sync** check box.
    b. In the Time boxes, specify the time of day you want to run the synchronization.
    c. If you want to schedule the synchronization to run on specific days of the week, select **Day of Week** from the Type box, and then click the check box of the appropriate day(s).

d. If you want to schedule the synchronization to run on a specific day of the month, select **Day of Month** from the Type box, and then select the appropriate day from the Perform sync every month at the following day box.

Note:

If the day number you specify exceeds the last day of a month, the synchronization will run on the last day of the month. For example, if you select **31**, the synchronization will run on the last day of the month in months that have less than 31 days.

e. When finished, click **Save**.

Configuring the directory authentication service

About this task

Use the following procedure to configure the following settings for the directory authentication service:

- connection timeout
- read timeout

Note:

Set these values based on the network and required user experience. Users logging into Collaboration Agent will experience the total amount of time configured here as the total amount of wait time before their login fails due to connection/read issues to the directory.

Procedure

1. In the Provisioning Client window, select **System Management > Directory Access Services > Authentication Service**.
2. Click the **Auth Configuration** tab.
3. In the Connection Timeout (milliseconds) box, enter the connection timeout in milliseconds for authentication. If the directory authentication client cannot establish a connection within the period you specify, the client aborts the connection attempt.

   Note:

   If you enter 0, the connection timeout is handled by TCP protocol.
4. In the Read Timeout (milliseconds) box, enter the read timeout in milliseconds for authentication. If the directory authentication client does not receive a response within the period you specify, the client aborts the read attempt.

Note:

If you enter 0, there is no timeout, and the system will wait for the authentication operation to complete.

5. Click **Save**.

Configuring the directory access passcode settings

Before you begin

If you want to store encrypted passcodes on the LDAP server and in the Avaya Aura® Conferencing, see Passcodes encryption on page 327.

About this task

Use the following procedure to configure the following directory access passcode settings for a domain:

- data source
- encoding method
- authentication key
- authentication action

Note:

- Changes to the encoding method and authentication key may cause encrypted passcodes stored in the external directory to become out of sync with the method Avaya Aura Conferencing will use to decrypt the passcodes. Any changes you make to these values may require you to update encrypted passcode values in the external directory and then synchronize these values to Avaya Aura® Conferencing.
- Changing the data source from the Avaya Aura Confencing database to LDAP will override passcodes with the values from the directory server during the next synchronization.

Passcode validation is enabled when the Conference Profile has passcodes enabled. Users enter the moderator or participant passcode (if required) after the participant collaboration code. The passcode is validated by either the LDAP server or the local Avaya Aura Conferencing database when the user logs into the audio/video conference or Web Collaboration Agent.

Procedure

1. In the Provisioning Client window, select **System Management > Directory Access Services > Authentication Service**.

Comments? infodev@avaya.com

2. Click the **Auth Passcode** tab.
3. From the Select domain box, select the domain you want to configure.
4. From the Data Source box, select the source you want to use to validate passcodes for users when they log into an audio/video conference or Web Collaboration Agent. Your choices are **LDAP** and **AAC Database**.
5. From the Encoding Method box, select the encoding method you want to use for passcode authentication.
6. In the Authentication Key box, enter the authentication key that you want to use to decrypt passcodes.

   The authentication key uses an AES cypher with a key length of either 128 bits or 256 bits. The key should be provided in hexadecimal format. A 128 bits key will have 32 hexadecimal characters. A 256 bits key will have 64 hexadecimal characters. Passcodes are stored encrypted on the LDAP server (if the data source is LDAP). To validate the passcodes during login, the system decrypts the value from the LDAP server and compares that value with the value entered by the user during login. You may enter the value 0123456789ABCDEF0123456789ABCDEF from the example in Passcodes encryption on page 327 or your own key in the Authentication Key box. For more information, see Passcodes encryption on page 327.
7. In the Confirm Authentication Key box, re-enter the authentication key string.
8. From the Authentication Action box, select the action you want performed when LDAP is unavailable for authentication. Your choices are **Authenticate with AAC Database** and **Block Admission**.
9. Click **Save**.
10. Repeat Steps 3 through 9 for each domain.

Passcodes encryption

For additional security, Avaya Aura® Conferencing supports encrypted passcodes stored as base64 text strings on the LDAP server and the Avaya Aura® Conferencing database. The Advanced Encryption Standard (AES) is the only supported encryption algorithm using Cipher-block Chaining (CBC) mode with key sizes of either 128 or 256 bits. PKCS5 is used for padding.

Avaya Aura® Conferencing decrypts passcodes by first base64 decoding the passcode value. Then, it removes the first 16 bytes of the result and uses this value as the initialization vector (IV) along with the provisioned key to decrypt the remaining bytes, representing the cipher text.

Passcodes are decrypted as needed. Passcodes only use the available provisioned key and cipher during the decryption process.

Avaya Aura® Conferencing will only decrypt passcodes based on the above criteria.

Configuring multiple directory domains

About this task

Use the following procedure to configure additional directory domains (if you added multiple directory domains).

Procedure

1. Configure the directory servers for another directory domain you added. See Configuring directory servers on page 319.
2. Configure the directory synchronization service for the directory domain you configured in Step 1. See Configuring the directory synchronization service on page 321.
3. Configure the directory authentication service. See Configuring the directory authentication service on page 325.
4. Configure the directory access passcode settings. See Configuring the directory access passcode settings on page 326.
5. Repeat Steps 1 through 4 for the remaining directory domains you added.

Configuring LDAP directory-synchronized users on System Manager

About this task

Use the following procedure to provision manually on Avaya Aura® System Manager each user that you want synchronized from the LDAP directory.

Procedure

1. Log into Avaya Aura® System Manager.
2. On the System Manager console, click **Users** > **User Management**.

3. In the navigation pane, click **User Management** > **Manage Users**.
4. On the User Management page, click **New**.
   The New User Profile page appears.
5. On the **Identity** tab, complete the required information. When entering this information, perform the following steps:
   - Make sure the data you enter in the Last Name box matches the data in the schema you mapped to “Last name” on the Sync Schema tab in Provisioning Client (Step 11 in Configuring the directory synchronization service on page 321).
   - Make sure the data you enter in the First Name box matches the data in the schema you mapped to “First name” on the Synch Schema tab in Provisioning Client (Step 11 in Configuring the directory synchronization service on page 321).
6. When finished, click **Commit & Continue**.
7. On the **Communication Profile** tab, complete the required information:
   a. **Name**: Type a name.
   b. **Default**: Select this check box.
   c. Complete the **Communication Address** section to add the user’s communication address.

      Note:

      The user’s communication address consists of a handle and a domain (for example, 5522@avaya.com). When entering this information:

      - Make sure the data you enter for the handle matches the data in the schema you mapped to “Communication address handle” on the **Sync Schema** tab in Provisioning Client (Step 11 in Configuring the directory synchronization service on page 321).
      - Make sure the data you enter for the domain matches the domain you selected on the **Sync Schema** tab in Provisioning Client (Step 8 in Configuring the directory synchronization service on page 321).

   d. Complete the **Session Manager Profile** section.
   e. Complete the following profiles as required for your users:
      - **CallPilot Messaging Profile**
      - **CM Endpoint Profile**
      - **CS 1000 Endpoint Profile**
      - **Messaging Profile**
      - **B5800 Branch Gateway Endpoint profile**

      Note:

      Do not assign the Conferencing Profile to the user. The user will be synchronized into Avaya Aura Conferencing. If you assign the Conferencing

Profile, you will receive errors either when saving the user on System Manager or during a subsequent LDAP synchronization because two sources will be trying to modify the same user data in Avaya Aura Conferencing.

8. Click **Commit & Continue**.
9. Repeat Steps 4 through 8 for each new user you want to add to System Manager.

Retrieving the CA certificate from the Active Directory server

About this task

Use the following procedure to retrieve the CA certificate from the Active Directory server.

Note:

Perform this procedure only if you are using TLS to connect to the Active Directory server.

Procedure

1. Log into the Active Directory server as administratior.
2. Open the Certificates console:
   a. Click **Start**.
   b. Type `MMC` and press the ENTER key.
   c. If prompted by the User Account Control, make sure the action you want to perform is displayed, and click **Yes**.
3. In the MMC console window, click **File**, and then click **Add/Remove Snap-in**.
4. In Add or Remove Snap-ins under Available Snap-ins, click **Certificates**, and then click **Add**.
5. In Certificates snap-in, select **Computer account**, and then click **Next**.
6. Perform one of the following steps:
   - If you are managing the LDAP server requiring the certificate, select **Local**.
   - If you are not managing the LDAP server requiring the certificate, select **Another computer**, click **Browse**, and select the LDAP server requiring the certificate.
7. Click **OK**.

8. Click **Finish**.
9. In Add or Remove Snap-ins, click **OK**.
10. In the console tree, expand Certificates (<computer>).
11. Go to **Personal**.
12. Go to **Certificates**.
13. Select a topmost certificate.
14. Right-click the certificate, and select **All Tasks > Export**.
15. In the Export dialog box:
    - Do not export private key.
    - Select **User base64 encoding format**.
16. Save to a file. Use a filename similar to ADserver_CA_base64.cer.

Assigning the Directory Server Certificate for the network elements

About this task

Use this procedure to set the certificate/key from the keystore for any directory servers configured for mutual/client authentication to Directory Server Certificate for the following network elements:

- Application Server
- Provisioning Manager
- Personal Agent Manager

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Provisioning Managers**.
2. In the Provisioning Managers window, select the first Provisioning Manager (for example, **PROV1**).
3. Click **Edit (-/+)**.
4. From the Directory Server Certificate box in the Edit dialog box, select the appropriate certificate.
5. Click **Apply**.

6. Repeat Steps 2 through 5 for any additional Provisioning Managers.
7. In the navigation pane of Element Manager Console, select **Feature Server Elements > Application Servers**.
8. In the Application Servers window, select the first Application Server (for example, **AS1**).
9. Click **Edit (-/+)**.
10. From the Directory Server Certificate box in the Edit dialog box, select the appropriate certificate.
11. Click **Apply**.
12. Repeat Steps 8 through 11 for any additional Application Servers.
13. In the navigation pane of Element Manager Console, select **Feature Server Elements > Personal Agent Managers**.
14. In the Personal Agent Managers window, select the first Personal Agent Manager (for example, **PA1**).
15. Click **Edit (-/+)**.
16. From the Directory Server Certificate box in the Edit dialog box, select the appropriate certificate.
17. Click **Apply**.
18. Repeat Steps 14 through 17 for any additional Personal Agent Managers.

Chapter 23: Deploying Audio/Video in Collaboration Agent

Pre-deployment checklist for Audio/Video in Collaboration Agent

The following checklist provides the high level steps and considerations prior to beginning your installation of Audio/Video in Collaboration Agent.

#	Task	Description	Notes	✔
1	Ensure that Avaya Aura® Conferencing 7.2 is installed and operating properly prior to installing Audio/Video in Collaboration Agent.			
2	Obtain the following information for the Avaya Aura® Conferencing system: • IP address of each Provisioning Manager that will host the Management Portal Client and its supporting files • IP address of each Personal Agent Manager that will host the Audio/ Video in Collaboration			

#	Task	Description	Notes	✔
	Agent client and its supporting files • Avaya Aura® Conferencing service domain • Avaya Aura® Conferencing MeetMe Conference service name • Avaya Aura® Conferencing Event Conference service name			
3	If you plan to control access to Audio/ Feature in Collaboration Agent, determine the service network topology (as IP address ranges). Provisioning Manager will control access to this feature by IP address range.			
4	Obtain the IP address of the System Manager that will be used to establish a SIP trunk for each Flash Media Gateway, and add a SIP entity for each Flash Media Gateway in the System Manager.			
5	Determine the dedicated IP address and FQDN for each server that will host a Flash Media Gateway instance.			

#	Task	Description	Notes	✔
	For systems with more than one Flash Media Gateway, identify which Flash Media Gateway instance will also host the simplex Management Server. For systems with more than two Flash Media Gateways, identify which Flash Media Gateway instances will perform the Load Balancer function. You can have a maximum of two Flash Media Gateways performing the Load Balancer function.			
6	If secure communication links are required, obtain security certificates from a public Certificate Authority.			
7	Identify the target server that will host the Audio/Video Management Server for the system.			
8	Ensure that the enterprise firewall is configured to support delivery of Audio/ Video in Collaboration Agent capabilities. If you are using a DMZ deployment,	Contact your network specialist or administrator if you have a standalone with redundancy or standalone simplex deployment and require a DMZ configuration. For more information, see Enterprise DMZ deployment on page 62. For the complete *Port Matrix: Avaya Aura® Conferencing* document, go to http://support.avaya.com.		

#	Task	Description	Notes	✔
	consider the following: • Ensure you have configured the required servers, routers, and firewalls. • Ensure the required port modifications are made.			
9	Make sure the server on which you will install Audio/Video in Collaboration Agent is supported.			
10	Obtain the Avaya Aura® Conferencing disks for Linux and software installation, and patches: • AAC platform DVD-ROM • Application Bundle DVD-ROM • Platform patches DVD-ROM To install Audio/ Video for Collaboration Agent, you must have the following software: • AccWeb-a-b-c.i386.rpm.bin (This is the server software.) • AccWeb-clients-d-e.zip (This is the Management Portal software.) • AacpaOtv-client-f-g.zip (This is the			

#	Task	Description	Notes	✔
	client software that will be integrated with Collaboration Agent.)			

Checklist for installing Audio/Video in Collaboration Agent

The following checklist provides a high-level view of the tasks involved in installing Audio/Video in Collaboration Agent.

#	Task	Description	Notes	✔
1	Ensure you have gathered the information required to install Audio/Video in Collaboration Agent.	See Pre-deployment checklist for Audio/ Video in Collaboration Agent on page 333.		
2	Open the appropriate ports between the Internet, DMZ, and enterprise networks.	See Configuring ports for Audio/Video in Collaboration Agent on page 339.		
3	Install the hardware (if required).	See “Chapter 5: Installing the hardware.”		
4	If you are using a standalone server for the Flash Media Gateway, perform the following steps: 1. Install the Linux operating system on that server. **Important:** The “Installing the AAC Platform” procedure guides you through the installation process with links	See: • Installing the AAC Platform on page 116 • Verifying the AAC Platform installation on page 129.		

#	Task	Description	Notes	✔
	to individual procedures. Upon completion of each step, return to the next step in the "Installing the AAC Platform" procedure by clicking the link at the end of each individual procedure. 2. Verify that all the required components are operational and error free after completing the Linux operating system installation.			
5	Extract the Audio/Video in Collaboration Agent software loads from the AAC Application Bundle iso image.	See Accessing and extracting the Audio/ Video in Collaboration Agent installation files on page 342.		
6	If you are installing Audio/Video in Collaboration Agent in a coresident deployment with other Avaya Aura® Conferencing components, you must add the IP address of the coresident Flash Media Gateway using the **`mcpModIPv4Subnet`** command.	See Configuring Audio/Video in Collaboration Agent for a coresident deployment on page 343.		
7	Install the Flash Media Gateway server software.	See Installing the Audio/Video in Collaboration Agent server software on page 344.		

#	Task	Description	Notes	✔
8	Install the Management Portal Client software.	See Installing the Audio/Video in Collaboration Agent Management Portal software on page 347.		
9	Configure the Flash Media Gateway.	See Configuring the Flash Media Gateway on page 349.		
10	Add a Flash Media Gateway cluster.	See Adding a Flash Media Gateway cluster on page 351.		
11	Place the Flash Media Gateway in service.	See Starting the Flash Media Gateway on page 353.		
12	Create the configuration file for the Audio/Video in Collaboration Agent client.	See Creating the client configuration file on page 353.		
13	Install the Audio/Video in Collaboration Agent client software.	See Installing the Audio/Video in Collaboration Agent client software on page 355.		
14	Verify that the Audio/Video in Collaboration Agent client software is integrated properly with Collaboration Agent.	See Verifying integration of the multimedia client software with Collaboration Agent on page 356.		
15	Secure Audio/Video in Collaboration Agent.	See Hardening Audio/Video in Collaboration Agent on page 357.		

Configuring ports for Audio/Video in Collaboration Agent

About this task

Use this procedure to configure the ports for Audio/Video in Collaboration Agent.

Procedure

1. Configure the ports between the Internet and the DMZ. See the following table:

   Table 43: Ports between the Internet and the DMZ

Server	Port Name	Description
Personal Agent Manager	Port 443 for HTTPS	This port leads to a secure web page for the user.
Flash Media Gateway **Note:** RTMPT provides the highest level of usability. However, the most secure method is RTMPS. Avaya recommends the use of the RTMPS protocol, except in cases where RTMPS is blocked by personal computer or corporate firewalls. In these cases, the use of RTMPT usually resolves any blockage.	Port 80	This port is for RTMPT, which is a tunneled version of the RTMP protocol for the Audio/Video for Collaboration Agent flash client.
	Port 1935	This port is for RTMP for the user flash client.
	Port 443	This port is for RTMPS, which is a secure SSL version of the RTMP protocol for the user flash client.

2. Configure the ports used inside the DMZ. See the following table:

   Table 44: Ports between the Internet and the DMZ

Server	Port Name	Description
Flash Media Gateway	Port 9444	This port is for the JMX-RMI connection from the Management Server to the Flash Media Gateway.
	Port 9445	This port is for the JMX-RMI connection from the Flash Media Gateway to the Load Balancer server.

Comments? infodev@avaya.com

Server	Port Name	Description
	Ports 5080 and 9999	These ports are internal to the Flash Media Gateway server.

3. Configure the ports between the DMZ and the enterprise.

Table 45: Ports between the Internet and the DMZ

Server	Port Name	Description
Personal Agent Manager	Port 443 for HTTPS	This port leads to a secure web page for the user. This port should be allowed if: • Audio/Video for Collaboration Agent access is required inside the enterprise • Collaboration Agent has the Audio/Video for Collaboration Agent client deployed and is located in the DMZ
Flash Media Gateway	Port 5060	This port is the SIP TCP connection to the SIP proxy (for example, to the Session Border Control application).
	Port 5061	This port is the SIP TLS connection to the SIP proxy (for example, to the Session Border Control application).
	RTP Port range	This is the range of ports used for RTP as configured on the Flash Media Gateway. Two ports are required for each audio session, and four ports are required for each audio/video session. **Note:** The RTP connection is required only between the Flash Media Gateway and the hosting Avaya Media Servers.
	Ports 80, 1935, and 443	These ports are for RTMPT (port 80), RTMP (port 1935), RTMPS (port 443) if: • Audio/Video in Collaboration Agent access is required inside the enterprise • the Flash Media Gateway that provides Audio/Video in

Server	Port Name	Description
		Collaboration Agent is deployed in the DMZ
	Port 9443	This port is for RTMPS for the Flash Media Gateway Management Portal. This port is required if the Management Server is deployed inside the DMZ, which is not recommended.

Accessing and extracting the Audio/Video in Collaboration Agent installation files

Before you begin

Make sure you have the latest version of the Avaya Aura® Conferencing Application Bundle. You can download iso images of this software from PDLS and burn the iso images to DVD-ROM.

About this task

Use this procedure to copy the Avaya Aura® Conferencing Application Bundle iso image to the primary Element Manager server and extract the Audio/Video in Collaboration Agent software. The Audio/Video in Collaboration Agent software consists of the following components:

- AccWeb-a-b-c.i386.rpm.bin

  This is the Flash Media Gateway server software.

- AccWeb-clients-d-e.zip

  This is the Management Portal Client software.

- AacpaOtv-client-f-g.zip

  This is the Audio/Video in Collaboration Agent (AViCA) client software.

Procedure

1. Log on to the primary Element Manager server as a user with the SA role (for example, `ntappadm`) through ssh or directly at the server console.
2. Copy the Avaya Aura® Conferencing Application Bundle iso file to the directory `/var/mcp/extract`on the primary Element Manager server.
3. Access the directory `/var/mcp/extract`.

Comments? infodev@avaya.com

4. Use the command `mcpExtractContent` to extract the content.
   The software is extracted to the directory `/var/mcp/media/avica`. This directory should contain the following files:
   - AccWeb-a-b-c.i386.rpm.bin
   - AccWeb-clients-d-e.zip
   - AacpaOtv-client-f-g.zip

Next steps

Proceed to Installing the Audio/Video in Collaboration Agent server software on page 344.

Configuring Audio/Video in Collaboration Agent for a coresident deployment

Before you begin

You must know the IP address of the co-resident Flash Media Gateway. This is equivalent to the network element instance service address.

About this task

Use this procedure to configure Audio/Video in Collaboration Agent for a coresident deployment.

Procedure

1. Using Element Manager Console, stop all network element instances deployed on the selected server. For more information, see Stopping a Network Element instance on page 472.
2. Log on to the target server as `ntsysadm` through ssh or directly on the server console.
3. At the prompt, type `mcpModIPv4Subnet -name sn0 -addotheraddrs <FMG.CO.RES.IP>` where *<FMG.CO.RES.IP>* is the network element instance service address.
4. Press **Enter**.
5. Using Element Manager Console, start all the network element instances deployed on the selected server. For more information, see Starting a Network Element instance on page 476.

Installing the Audio/Video in Collaboration Agent server software

Before you begin

You must be able to access the Audio/Video in Collaboration Agent server software (AccWeb-a-b-c.i386.rpm.bin).

About this task

Use this procedure to install the Audio/Video in Collaboration Agent server software. You will install this software on the Flash Media Gateway server.

Procedure

1. Log on to the Flash Media Gateway server as `ntsysadm` through ssh or directly on the server console.
2. Enter **`su -`** to log on as root.
3. At the prompt `password`, type the root password, and press **Enter**.
4. Make sure the directory `/var/mcp/media/avica` exists on the Flash Media Gateway server.

   If this directory does not exist, perform the following steps to create the directory:

   a. At the prompt, type `mkdir -m 770 /var/mcp/media/avica` and press **Enter**.
   b. At the prompt, type `chmod ntappadm:ntappgrp /var/mcp/media/avica` and press **Enter**.
5. Copy the file `AccWeb-a-b-c.i386.rpm.bin` from the directory `/var/mcp/media/avica` on the primary Element Manager server into the directory `/var/mcp/media/avica` on the Flash Media Gateway server.
6. Go to the directory `/var/mcp/media/avica` on the Flash Media Gateway server.
7. Type `chmod +x AccWeb-x.x-x.i386.rpm.bin` and press **Enter**.
8. Type `./AccWeb-x.x-x.i386.rpm.bin` and press **Enter**.
   The Avaya Customer Connections Web End User License Agreement (EULA) appears.
9. Read the license agreement.
10. To accept the license agreement and proceed with the installation, type `y`.

The software is installed on the server. During the installation, the software is installed in the directory `/opt/Avaya/AccWeb`, and Red5 Media Server is installed in the directory `/usr/local/red5`.

You are prompted to run the configuration tool.

Note:

In this procedure, you will run the configuration tool now. However, you can manually run the configuration tool at a later time by accessing `/opt/Avaya/AccWeb/bin` and then using the command **`./configure`**.

11. Type `y`, and press **Enter**.
    You are prompted to enter the IP address for the JMX connections.
12. Perform one of the following steps:
    - If you want to use the default, press **Enter**.
    - If you want to use a different IP address, enter the appropriate IP address, and then press **Enter**.
13. When prompted to enter the IP address for the RTMP connections, perform one of the following steps:
    - If you want to use the default, press **Enter**.
    - If you want to use a different IP address, enter the appropriate IP address, and then press **Enter**.
14. When prompted to enter the IP address for the HTTP connections, perform one of the following steps:
    - If you want to use the default, press **Enter**.
    - If you want to use a different IP address, enter the appropriate IP address, and then press **Enter**.
15. When prompted to enable RTMPS, type `y`, and press **Enter**.
16. When prompted to enter the port for RTMPS, perform one of the following steps:
    - If you want to use the default, press **Enter**.
    - If you want to use a different port, enter the appropriate port, and then press **Enter**.
17. When prompted to generate a self-signed certificate for RTMPS, type `y`, and press **Enter**.
18. When prompted to enable RTMP, type `y`, and press **Enter**.
19. When prompted to enter the port for RTMP, perform one of the following steps:
    - If you want to use the default, press **Enter**.

- If you want to use a different port, enter the appropriate port, and then press **Enter**.

20. When prompted to enable RTMPT, type `y`, and press **Enter**.
21. When prompted to enter the port for RTMPT, perform one of the following steps:
    - If you want to use the default, press **Enter**.
    - If you want to use a different port, enter the appropriate port, and then press **Enter**.

    You are prompted to enter the IP address for the Management Client.
22. Perform one of the following steps:
    - If you want to use the default, press **Enter**.
    - If you want to use a different IP address, enter the appropriate IP address, and then press **Enter**.
23. When prompted to enter the port for the Management Client, type `y`, and press **Enter**.
    You are prompted to run the Management Server on this machine.
24. Perform one of the following steps:
    - If this machine is the primary Flash Media Gateway in the cluster or this machine is a standalone Flash Media Gateway Management server co-located with Provisioning Manager if all Flash Media Gateways are in the DMZ, type `y`, and press **Enter**.
    - If this machine is *not* the primary Flash Media Gateway in the cluster or this machine is *not* a standalone Flash Media Gateway Management server co-located with Provisioning Manager if all Flash Media Gateways are in the DMZ, type `n`, and press **Enter**.
25. When prompted to generate a self-signed certificate for RTMPS for the Management Portal, type `y`, and press **Enter**.
26. At the command prompt, type `source /root/.bash_profile` and press **Enter** to apply the environment variables that were added during installation.
27. At the command prompt, type `service red5 start` and press **Enter** to start the server as a Linux service.

Next steps

Proceed to Installing the Audio/Video in Collaboration Agent Management Portal software on page 347.

Installing the Audio/Video in Collaboration Agent Management Portal software

Before you begin

You must be able to access the Audio/Video in Collaboration Agent Management Portal software (AccWeb-clients-d-e.zip).

About this task

Use this procedure to install the Audio/Video in Collaboration Agent server software. You will install this software on the Element Manager server where the Provisioning Manager (PROV) is installed.

Procedure

1. Log on to the Element Manager server where the Provisioning Manager is installed as `ntsysadm` through ssh or directly on the server console.
2. Enter **`su -`** to log on as root.
3. At the prompt `password`, type the root password, and press **Enter**.
4. Make sure the directory `/var/mcp/media/prov_pa_installs` exists on the target server.

   If this directory does not exist, perform the following steps to create the directory:

   a. At the prompt, type `mkdir -m 770 /var/mcp/media/prov_pa_installs` and press **Enter**.
   b. At the prompt, type `chmod ntappadm:ntappgrp /var/mcp/media/prov_pa_installs` and press **Enter**.
5. Make sure the directory `/var/mcp/media/prov_pa_installs/fmgadmin` exists on the target server.

   If this directory does not exist, perform the following steps to create the directory:

   a. At the prompt, type `mkdir -m 770 /var/mcp/media/prov_pa_installs/fmgadmin` and press **Enter**.
   b. At the prompt, type `chmod ntappadm:ntappgrp /var/mcp/media/prov_pa_installs/fmgadmin` and press **Enter**.
6. Copy the file `AccWeb-clients-d-e.zip` from the directory `/var/mcp/media/avica` on the primary Element Manager server into the directory `/var/mcp/media/avica` on the target server.
7. Go to the directory `/var/mcp/media/avica` on the target server.

8. At the prompt, type `unzip AccWeb-clients-d-e.zip admin/* -d fmgtemp/` and press **Enter**.
9. At the prompt, type `cp -R fmgtemp/admin/* /var/mcp/media/prov_pa_installs/fmgadmin/` and press **Enter**.
10. At the prompt, type `chown -R ntappsw:ntappgrp /var/mcp/media/prov_pa_installs/fmgadmin` and press **Enter**.
11. At the prompt, type `chmod -R 770 /var/mcp/media/prov_pa_installs/fmgadmin` and press **Enter**.
12. At the prompt, type `rm -rf fmgtemp` and press **Enter**.
13. Open a web browser and go to `https://<PROV IP address or FQDN>:8443/fmgadmin/index.html` where <PROV IP address or FQDN> is the IP address or FQDN of the server running Provisioning Manager.
    The Log On page for Avaya One Touch Video 3.0 appears. You will use Avaya One Touch Video 3.0 to administer the Audio/Video in Collaboration Agent feature.
14. In the User Name box, enter `admin`.
15. In the Password box, enter `admin01`.
16. Click **Log on**.
    The Security Alert dialog box appears.

    Note:

    The first time you access the Management Portal Client you must set up the certificate in your Truststore.
17. Click **View Certificate**.
18. In the Certificate dialog box, click **Install Certificate**.
19. In the Certificate Import Wizard dialog box, click **Next**.
20. On the Certificate Store page, select **Place all certificates in the following store**, and then click **Browse**.
21. In the Select Certificate Store dialog box, select **Trusted Root Certification Authorities**, and click **OK**.
22. On the Certificate Store page, click **Next**.
23. On the Completing the Certificate Import Wizard page, click **Finish**.
24. In the Security Warning dialog box, click **Yes**.
    The Certificate Import Wizard message box appears, indicating that the certificate import was successful.
25. In the Certificate Import Wizard message box, click **OK**.

Note:

Your initial attempt to access the Management Portal Client will fail. After the certificate is installed, you must refresh your browser window and then try to log in again.

Next steps

Proceed to Configuring the Flash Media Gateway on page 349.

Configuring the Flash Media Gateway

Before you begin

You must be able to access the Audio/Video in Collaboration Agent Management Portal client.

About this task

Use this procedure to configure the Flash Media Gateway.

Note:

Avaya Aura Conferencing supports a maximum of four Flash Media Gateways.

Procedure

1. Open a web browser and go to `https://<PROV IP address or FQDN>:8443/fmgadmin/index.html` where <PROV IP address or FQDN> is the IP address or FQDN of the server running Provisioning Manager.
   The Log On page for Avaya One Touch Video 3.0 appears. You will use Avaya One Touch Video 3.0 to administer the Audio/Video in Collaboration Agent feature.
2. In the User Name box, enter `admin`.
3. In the Password box, enter `admin01`.
4. Click **Log on**.
   The Legal Notice page appears.
5. On the Legal Notice page, read the information provided.
6. To accept the information displayed, click **Accept**.
   The Welcome page appears.
7. On the Welcome page, click **Add New Flash Media Gateway**.
8. In the Name box on the Flash Media Gateway page, enter a name for this Flash Media Gateway.

9. In the Management IP Address box, enter the IP address of this Flash Media Gateway that will connect to the Flash Media Gateway Management Server as specified during installation.
10. In the Management Port box, use the default setting (9444).
11. In the Externally accessible RTMP IP Address box, enter the IP address of this Flash Media Gateway that will service the Flash domain.
12. In the Server ID box, click **Get Next** to assign a unique ID to this Flash Media Gateway.
13. In the IP Address box in the SIP Trunk area, enter the IP address of this Flash Media Gateway that will establish a SIP trunk to the Avaya Aura Session Manager server as specified during installation.
14. In the Port box, use the default setting (5060).
15. Click the **Use Cluster Settings** check box to enable it.
16. In the RTP area at the bottom of the page, click **New**.
17. In the IP Address box in the RTP Bind Interfaces Table Input dialog box, enter the IP address of this Flash Media Gateway that will establish RTP/RTCP connections to the Avaya Media Server as specified during installation.
18. In the Start Port box, enter 40000.
19. In the End Port box, enter 60000.

    Note:

    These Start Port and End Port settings will provide a range of 10000 RTP ports and 10000 RTCP ports.
20. Click **OK**.
21. Click **Save** at the bottom of the page.
22. If you want to configure another Flash Media Gateway, repeat Steps 7 through 21.

    Note:

    Avaya Aura Conferencing supports a maximum of four Flash Media Gateways.

Next steps

Proceed to Adding a Flash Media Gateway cluster on page 351.

Adding a Flash Media Gateway cluster

Before you begin

You must be able to log into the Audio/Video in Collaboration Agent Management Portal client.

About this task

Use this procedure to add a Flash Media Gateway cluster.

Note:

Avaya Aura® Conferencing supports one Flash Media Gateway cluster.

Procedure

1. From the Clusters area in the navigation panel of the Avaya One Touch Video 3.0 application, click **Add New**.
2. In the Name box on the Clusters page, enter a name for this cluster.
3. In the Flash Media Gateways area, click **Add**.
4. From the Name box in the Cluster FMG Table Input dialog box, select the Flash Media Gateway you added.
5. In the Call Capacity box, enter a number that is less than or equal to the licensed capacity of the Flash Media Gateway you selected in Step 4.
6. Click **OK**.
7. In the Load Balancer area, click **Add**.
8. From the FMG Name box in the Cluster Load Balancer Table Input dialog box, select the Flash Media Gateway that will provide the Load Balancer function.
9. In the JMX Bind Interface box, enter the IP address of the Flash Media Gateway you specified in Step 8.
10. In the JMX Bind Port box, enter the appropriate port number. The default is 9445.
11. Click **OK**.
12. In the RTMPS Cipher Settings area, select **SSL_RSA_WITH_3DES_EDE_CBC_SHA** in the Available Ciphers list box.
13. Click **>>**.
    The selected cipher appears in the Selected Ciphers list box.
14. In the SIP Trunk area, enter the IP address of the Avaya Aura® Session Manager in the IP Address box.
15. In the Port box, enter 5060 (the default).

16. In the Agent Call Setting area, enter the service domain for Avaya Aura® Conferencing in the SIP domain box.
17. In the Customer Call Settings area, enter the service domain for Avaya Aura® Conferencing in the (From) SIP Domain box.
18. In the (To) SIP Domain box, enter the service domain for Avaya Aura® Conferencing.
19. In the Routing area, click **New**.
20. In the Route Name box in the Cluster Routing Table Input dialog box, enter the name for the route that will be used for connecting to MeetMe conferencing.
21. In the SIP User Name box, enter the service name for MeetMe conferencing.
22. In the SIP Domain box, enter the service domain for Avaya Aura® Conferencing.
23. Click **OK**.
24. In the Routing area, click **New**.
25. In the Route Name box in the Cluster Routing Table Input dialog box, enter the name for the route that will be used for connecting to Event conferencing.
26. In the SIP User Name box, enter the service name for Event conferencing.
27. In the SIP Domain box, enter the service domain for Avaya Aura® Conferencing.
28. Click **OK**.
29. In the Codecs area, select the appropriate audio codec from the Audio Codecs box.
30. From the Customer Call Audio Codecs box, select the appropriate audio codec.
31. From the Cluster Video Codecs box, select **H264**.
32. In the Profiles area, click **Add Profile**.
33. In the Enter a profile Name dialog box, enter a name for this profile, and click **OK**.
34. Click **Add**.
35. From the Video FPS box, in the Bandwidth Level Table dialog box, select **30**.
36. From the Video Size box, select **AAC_640_360**.
37. From the Video B/W box, select **512**.
38. From the AS B/W box, enter `0`. AS/BW is not supported for Avaya Aura® Conferencing.
39. From the AS Mode box, select **RESERVED**. AS Mode is not supported for Avaya Aura® Conferencing.
40. Click **OK**.

41. Click **Save** at the bottom of the page.

Next steps

Proceed to Starting the Flash Media Gateway on page 353.

Starting the Flash Media Gateway

Before you begin

You must be able to log into the Audio/Video in Collaboration Agent Management Portal software.

About this task

Use this procedure to place the Flash Media Gateway into service.

Procedure

1. From the Flash Media Gateway area in the navigation panel of the Avaya One Touch Video 3.0 application, click **List All**.
2. In the System Status area of the Flash Media Gateway page, select the Flash Media Gateway.
3. Click **Start** to place the selected Flash Media Gateway into service.
4. Repeat Steps 2 and 3 for each Flash Media Gateway.

Next steps

Proceed to Creating the client configuration file on page 353.

Creating the client configuration file

Before you begin

- All of the Flash Media Gateway are licensed and started (in service).
- You are able to log into the Audio/Video in Collaboration Agent Management Portal client.

About this task

Use this procedure to create the configuration file for the Audio/Video in Collaboration Agent client.

Procedure

1. From the Settings area in the navigation panel of the Avaya One Touch Video 3.0 application, click **Customer Configuration**.
   The ACC Web Customer Configuration page appears.
2. From the Cluster box, select the cluster that you created. This is the primary address that the Audio/Video in Collaboration Agent client will use to connect to the Flash Media Gateways.
3. From the Protocol box, select the protocol that the Audio/Video in Collaboration Agent client will use to establish connections across the Flash domain.
4. From the Profile Name box, select the profile that you created.
5. From the Meetme Route Name box, select the MeetMe conferencing route that you created. This is the route that the Audio/Video in Collaboration Agent client will use to connect callers to a MeetMe conference.
6. From the Event Route Name box, select the Event conferencing route that you created. This is the route that the Audio/Video in Collaboration Agent client will use to connect callers to an Event conference.
7. Check the **Audio Available** check box if you want to make the audio capability available to the Audio/Video in Collaboration Agent client using this configuration. This option is available only if licensed.
8. Check the **Video Available** check box if you want to make the video capability available to the Audio/Video in Collaboration Agent client using this configuration. This option is available only if licensed.
9. Check the Default Audio Selected check box if you want to make the audio capability available by default to the Audio/Video in Collaboration Agent client using this configuration.
10. Check the Default Video Selected check box if you want to make the video capability available by default to the Audio/Video in Collaboration Agent client using this configuration.
11. Click **Generate** to create the client configuration file (`AccWebCustomerConfig.xml`).
    The Configuration Text dialog box appears and displays the contents of the `AccWebCustomerConfig.xml`.
12. Click **Save**.
13. Using the Select location for download by dialog box, specify where you want to save the file `AccWebCustomerConfig.xml`, and then click **Save**.
14. Click **Log Off** at the top of the page to log off Avaya One Touch Video 3.0.

Next steps

Proceed to Installing the Audio/Video in Collaboration Agent client software on page 355.

Installing the Audio/Video in Collaboration Agent client software

Before you begin

- You must be able to access the Audio/Video in Collaboration Agent client software (`AacpaOtv-client-f-g.zip`).
- You must be able to access the client configuration file you created (`AccWebCustomerConfig.xml`).

About this task

Use this procedure to install the Audio/Video in Collaboration Agent client software and configuration file you created. You will install this software and configuration file on the Personal Agent Manager server.

Procedure

1. Log on to the Personal Agent Manager server as `ntsysadm` through ssh or directly on the server console.
2. Enter **`su -`** to log on as root.
3. At the prompt `password`, type the root password, and press **Enter**.
4. Make sure the directory `/var/mcp/media/prov_pa_installs` exists on the target server.

   If this directory does not exist, perform the following steps to create the directory:

   a. At the prompt, type `mkdir -m 770 /var/mcp/media/prov_pa_installs` and press **Enter**.
   b. At the prompt, type `chmod ntappadm:ntappgrp /var/mcp/media/prov_pa_installs` and press **Enter**.
5. Make sure the directory `/var/mcp/media/prov_pa_installs/otv` exists on the target server.

   If this directory does not exist, perform the following steps to create the directory:

   a. At the prompt, type `mkdir -m 770 /var/mcp/media/prov_pa_installs/otv` and press **Enter**.
   b. At the prompt, type `chmod ntappadm:ntappgrp /var/mcp/media/prov_pa_installs/otv` and press **Enter**.

6. Copy the file `AacpaOtv-client-f-g.zip` from the directory `/var/mcp/media/avica` on the primary Element Manager server into the directory `/var/mcp/media/avica` on the Personal Agent Manager server.
7. Go to the directory `/var/mcp/media/avica` on the Personal Agent Manager server.
8. Type `unzip AacpaOtv-client-f-g.zip AacpaOtv/* –d fmgtemp/` and press **Enter**.
9. Type `cp –R fmgtemp/AacpaOtv/* /var/mcp/media/prov_pa/installs/otv` and press **Enter**.
10. Type `rm –rf fmgtemp` and press **Enter**.
11. Copy the file `AccWebCustomerConfig.xml` file to the directory `/var/mcp/media/prov_pa_installs/otv/` on the Personal Agent Manager server.
12. At the prompt, type `chown -R ntappsw:ntappgrp /var/mcp/media/prov_pa_installs/otv` and press **Enter**.
13. At the prompt, type `chmod -R 770 /var/mcp/media/prov_pa_installs/otv` and press **Enter**.

Next steps

Proceed to Verifying integration of the multimedia client software with Collaboration Agent on page 356.

Verifying integration of the multimedia client software with Collaboration Agent

About this task

Use this procedure to verify that the Audio/Video in Collaboration Agent client software is integrated with Collaboration Agent.

Procedure

1. Open your web browser and go to `https://<Personal Agent Manager IP address or FQDN>/aacpa`.
   The Avaya Aura Conferencing Collaboration Agent login page appears.
2. Log into Collaboration Agent.
3. Enter a conference.

The Audio/Video in Collaboration Agent popup dialog box should appear, indicating that the Audio/Video in Collaboration Agent client software is integrated properly with Collaboration Agent.

Hardening Audio/Video in Collaboration Agent

The following checklist provides a high-level view of the tasks involved in hardening Audio/Video in Collaboration Agent.

#	Task	Description	Notes	✔
1	Create a certificate for the Flash Media Gateway IP address that is signed by Avaya Aura® System Manager.	See Creating a System Manager-signed certificate for the Flash Media Gateway IP address on page 358.		
2	Create a VeriSign-signed certificate for the Flash Media Gateway FQDN.	See Creating a VeriSign-signed certificate for the Flash Media Gateway on page 359.		
3	Secure the JMX connection between the Flash Media Gateways and the RTMPS connection to the Flash Media Gateway server.	See Securing the JMX connection between the Flash Media Gateways and the RTMPS connection to the Flash Media Gateway Management server on page 360.		
4	Configure a SIP TLS connection from the Flash Media Gateway to the Avaya Aura® Session Manager.	See Configuring a secure SIP TLS connection from the Flash Media Gateway to Avaya Aura Session Manager on page 361.		
5	Configure a secure RTMPS connection between the Flash	See Configuring a secure RTMPS connection between		

#	Task	Description	Notes	✔
	Media Gateways and the Audio/Video in Collaboration Agent clients.	the Flash Media Gateways and the Audio/Video in Collaboration Agent clients on page 362.		

Related topics:

Creating a System Manager- signed certificate for the Flash Media Gateway IP address on page 358

Creating a VeriSign-signed certificate for the Flash Media Gateway on page 359

Securing the JMX connection between the Flash Media Gateways and the RTMPS connection to the Flash Media Gateway Management server on page 360

Configuring a secure SIP TLS connection from the Flash Media Gateway to Avaya Aura Session Manager on page 361

Configuring a secure RTMPS connection between the Flash Media Gateways and the Audio/Video in Collaboration Agent clients on page 362

Creating a System Manager- signed certificate for the Flash Media Gateway IP address

About this task

Use the following procedure to create a certificate for the Flash Media Gateway IP address that is signed by System Manager.

Procedure

1. Log on to System Manager.
2. Click **Services** > **Security**.
3. In the navigation pane, click **Certificates** > **Authority**.
4. In the navigation pane, click **Add End Entity**.
5. In the Add End Entity window, complete the following fields:
   - **End Entity Profile**: Select **INBOUND_OUTBOUND_TLS** from the list.
   - **Username**: Enter the IP address of the Flash Media Gateway.
   - **Password**: Enter any password. You will use this password when creating the certificate.
   - **Confirm Password**: Type the password again.
   - **CN, Common Name (first entry)**: Enter the userID for the specific administrator. For example, admin.

- **Token**: Select **JKS file** from the list.

6. Click **Add End Entity**.
7. In the navigation pane, click **Public Web**.
8. In the navigation pane of the new browser window or tab, click **Create Keystore**.
9. Type the user name and password, and click **OK**.
10. Click **OK**.
11. Click **OK**, and save the *.jks file on your PC.

Creating a VeriSign-signed certificate for the Flash Media Gateway

About this task

Use this procedure to create a VeriSign-signed certificate for the Flash Media Gateway FQDN to make it accessible in the Internet.

Procedure

1. Log on to the Flash Media Gateway server as `ntsysadm` through ssh or directly on the server console.
2. Enter **`su -`** to log on as root.
3. At the prompt `password`, type the root password, and press **Enter**.
4. At the prompt, type `mkdir /var/mcp/fmg/certs/external` and press **Enter**.
5. At the prompt, type `cd /var/mcp/fmg/certs/external` and press **Enter**.
6. Type `openssl genrsa -des3 -out <FMG_FQDN>.key 2048` and press **Enter** to create a private key.

   Note:

   The value 2048 represents the bit length of the key.
7. When prompted, enter a password, and press **Enter**.
8. Type `openssl req -new -key <FMG_FQDN>.key -out <FMG_FQDN>.csr -subj "/C=<country>/O=<company>/ST=<state>/L=<location>/CN=<FMG_FQDN>"` to create a private key.

   An example is `openssl req -new -key FMGServer1@avaya.com.key -out FMGServer1@avaya.com.csr -subj "/C=US/O=Avaya, Inc./ST=Colorado/L=Westminster/CN=FMGServer1@avaya.com"` where `FMGServer1@avaya.com` is the *<FMG_FQDN>*.

9. Press **Enter** to create the private key.
10. Submit the CSR file to VeriSign to get a certificate.
11. Obtain the appropriate VeriSign root and intermediate CA certificates.
12. Put the CA certificates and the Flash Media Gateway certificate returned from VeriSign in the directory `/var/mcp/fmg/certs/external`on the server.
13. Type `cd /var/mcp/fmg/certs/external` and press **Enter**.
14. Type `cat VeriSign_G5_top.crt VeriSign_G3_Int.crt <FMG_FQDN>.cer > <FMG_FQDN>.chain.crt` and press **Enter** to create the certificate chain.
15. Type `openssl pkcs12 -export -out <FMG_FQDN>.pkcs12 -inkey <FMG_FQDN>.key -in <FMG_FQDN>.chain.crt` and press **Enter** to create the PKCS12 keystore that contains the Flash Media Gateway certificate chain and the private key.
16. When prompted, enter the password you entered in Step 1.
17. When prompted, enter the new export password.
18. Type `cp <FMG_FQDN>.pkcs12 ../` and press **Enter** to copy the PKCS12 keystore to the directory `/var/mcp/fmg/certs`.
19. Type `/opt/Avaya/AccWeb/bin/convertP12toJKS` and press **Enter** to convert the PKCS12 keystore to a JKS keystore.
20. Follow the instructions. When prompted for a password, enter the export password you entered in Step 16.
21. Transfer the file `<FMG_FQDN>.jks` from the directory `/var/mcp/fmg/certs` to your PC.

Securing the JMX connection between the Flash Media Gateways and the RTMPS connection to the Flash Media Gateway Management server

About this task

Use this procedure to secure:

- the JMX connection between the Flash Media Gateways
- the RTMPS connection to the Flash Media Gateway Management server

Procedure

1. Log on to the Flash Media Gateway server as `ntsysadm` through ssh or directly on the server console.
2. Enter **`su -`** to log on as root.
3. At the prompt `password`, type the root password, and press **Enter**.
4. Put the *.jks keystore in the directory `/var/mcp/fmg/certs`. You created this *.jks keystore in Creating a System Manager- signed certificate for the Flash Media Gateway IP address on page 358.
5. Go to the directory `/opt/Avaya/AccWeb/bin`.
6. Type `installKeystore` and press **Enter**.
7. Follow the instructions.

   Note:

   Select the option to install the keystore for All Management Interfaces.
8. When finished, type `service red5 restart` and press **Enter** to restart the Audio/Video in Collaboration Agent server software.

Configuring a secure SIP TLS connection from the Flash Media Gateway to Avaya Aura® Session Manager

About this task

Use this procedure to configure a secure SIP TLS connection from the Flash Media Gateway to Avaya Aura® Session Manager.

Procedure

1. Log on to System Manager and create a TLS SIP entity link from Session Manager to each Flash Media Gateway using port 5061.
2. Open a web browser and go to `https://<PROV IP address or FQDN>:8443/fmgadmin/index.html` where <PROV IP address or FQDN> is the IP address or FQDN of the server running Provisioning Manager.
   The Log On page for Avaya One Touch Video 3.0 appears.
3. In the User Name box, enter `admin`.
4. In the Password box, enter `admin01`.
5. Click **Log on**.

The Legal Notice page appears.

6. On the Legal Notice page, read the information provided.
7. To accept the information displayed, click **Accept**.
   The Welcome page appears.
8. From the Flash Media Gateway area in the navigation panel, click **List All**.
9. In the System Status area of the Flash Media Gateway page, select a Flash Media Gateway, and click **Edit**.
10. In the SIP Trunk area, change the port from 5060 to 5061, and click **Save**.
11. Repeat Steps 9 and 10 for each Flash Media Gateway.
12. From the Cluster area in the navigation panel, click **List All**.
13. In the System Status area of the Flash Media Gateway page, select a cluster, and click **Edit**.
14. In the SIP Trunk area, make the following changes:
    - Port: Set to `5061` (or other port that is used for SIP TLS on Session Manager).
    - Enable: Set to **TRUE**.
    - TLS certificate: Click Upload, select the certificate you create in Creating a System Manager- signed certificate for the Flash Media Gateway IP address on page 358 and upload the file.
    - Key Store Password: Enter the password from Step 3 in Creating a System Manager- signed certificate for the Flash Media Gateway IP address on page 358.
15. Click **Save**.
16. Go to the Flash Media Gateway on the Management Portal client and restart all Flash Media Gateways.

Configuring a secure RTMPS connection between the Flash Media Gateways and the Audio/Video in Collaboration Agent clients

About this task

Use this procedure to configure a secure the RTMPS connection between the Flash Media Gateways and the Audio/Video in Collaboration Agent clients.

Procedure

1. Open a web browser and go to `https://<PROV IP address or FQDN>:8443/fmgadmin/index.html` where <PROV IP address or FQDN> is the IP address or FQDN of the server running Provisioning Manager.
   The Log On page for Avaya One Touch Video 3.0 appears.
2. In the User Name box, enter `admin`.
3. In the Password box, enter `admin01`.
4. Click **Log on**.
   The Legal Notice page appears.
5. On the Legal Notice page, read the information provided.
6. To accept the information displayed, click **Accept**.
   The Welcome page appears.
7. From the Flash Media Gateway area in the navigation panel, click **List All**.
8. In the System Status area of the Flash Media Gateway page, select a Flash Media Gateway, and click **Edit**.
9. In the General area, make the following changes:
   - RTMPS Certificate: Click **Upload**, select the certificate you created in Creating a VeriSign-signed certificate for the Flash Media Gateway on page 359, and click **Open**.
   - RTMPS JKS Password: Enter the password from Step x in Creating a VeriSign-signed certificate for the Flash Media Gateway on page 359.
10. Click **Save**.
11. Restart the Flash Media Gateway.
12. Repeat Steps 7 through 11 for each Flash Media Gateway.
13. From the Settings area in the navigation panel of the Avaya One Touch Video 3.0 application, click **Customer Configuration**.
    The ACC Web Customer Configuration page appears.
14. From the Cluster box, select the cluster that you created. This is the primary address that the Audio/Video in Collaboration Agent client will use to connect to the Flash Media Gateways.
15. From the Protocol box, select **rtmps**. The Audio/Video in Collaboration Agent client will use RTMPS to establish connections across the Flash domain.
16. From the Profile Name box, select the profile that you created.
17. From the Meetme Route Name box, select the MeetMe conferencing route that you created. This is the route that the Audio/Video in Collaboration Agent client will use to connect callers to a MeetMe conference.

18. From the Event Route Name box, select the Event conferencing route that you created. This is the route that the Audio/Video in Collaboration Agent client will use to connect callers to an Event conference.
19. Check the **Audio Available** check box if you want to make the audio capability available to the Audio/Video in Collaboration Agent client using this configuration. This option is available only if licensed.
20. Check the **Video Available** check box if you want to make the video capability available to the Audio/Video in Collaboration Agent client using this configuration. This option is available only if licensed.
21. Check the Default Audio Selected check box if you want to make the audio capability available by default to the Audio/Video in Collaboration Agent client using this configuration.
22. Check the Default Video Selected check box if you want to make the video capability available by default to the Audio/Video in Collaboration Agent client using this configuration.
23. Click **Generate** to create the client configuration file (`AccWebCustomerConfig.xml`).
    The Configuration Text dialog box appears and displays the contents of the `AccWebCustomerConfig.xml`.
24. Click **Save**.
25. Using the Select location for download by dialog box, specify where you want to save the file `AccWebCustomerConfig.xml`, and then click **Save**.
26. Click **Log Off** at the top of the page to log off Avaya One Touch Video 3.0.
27. Log on to the Personal Agent Manager server as `ntsysadm` through ssh or directly on the server console.
28. Enter **`su -`** to log on as root.
29. At the prompt `password`, type the root password, and press **Enter**.
30. Copy the file `AccWebCustomerConfig.xml` file to the directory `/var/mcp/media/prov_pa_installs/otv/` on the Personal Agent Manager server.
31. At the prompt, type `chown -R ntappsw:ntappgrp /var/mcp/media/prov_pa_installs/otv` and press **Enter**.
32. At the prompt, type `chmod -R 770 /var/mcp/media/prov_pa_installs/otv` and press **Enter**.

Upgrading Audio/Video in Collaboration Agent

If Avaya releases a new service pack or a new feature pack, you may have to upgrade the Audio/Video in Collaboration Agent feature. The process of upgrading the Audio/Video in Collaboration Agent feature is the same for service packs, feature packs, and patch releases. The only difference between these three types of releases is the method of obtaining the software from PLDS.

Related topics:

Upgrading the Audio/Video in Collaboration Agent server software on page 488
Upgrading the Audio/Video in Collaboration Agent Management Portal software on page 489
Upgrading the Audio/Video in Collaboration Agent client software on page 490

Chapter 24: Hardening Avaya Aura® Conferencing

This chapter describes the procedures to perform security hardening on the core servers (Element Manager servers and Avaya Media servers) of an Avaya Aura® Conferencing 7.2 system. This chapter is intended to be used for initial hardening of an Avaya Aura® Conferencing 7.2 system.

For maximum security, all scripts are run via the Linux sudo command to allow the scripts to access privileged devices without having to be the root user. You may be prompted to enter a password when running scripts mentioned in this chapter. If so, enter the administrator password (that is, ntsysadm, ntappadm, etc.) under which you are currently logged in, unless instructed otherwise.

Configuring the BIOS password

Most planar BIOS provide the ability to configure an administrative password. If the BIOS on the server allows an administrative password to be configured, use the Administrator password, and refer to the server hardware installation guide for details on how to configure the BIOS password.

If the BIOS password can be configured, it must be configured on each server in the system.

Note:

A BIOS Power-On password is also available on most systems. However, because using the BIOS Power-On password can result in a service outage, use the BIOS administrative password. Do not configure a Power-On password.

Configuring the BIOS boot order

For maximum security, you must set the BIOS boot order to **Hard Disk First, CD-ROM Second** for each server. For details on configuring the BIOS boot order, see the server hardware installation guide that was used to install the servers.

Setting operating system inactive account auditing

About this task

This task must be performed on all Element Manager servers and Avaya media servers.

Procedure

1. Log onto the server as the *ntsysadm* user.
2. At the command prompt, enter **`configInactiveLoginAudit`** and press **Enter**.
3. At the prompt `Enter 'c' to configure, 'd' to display, or 'q' to quit [c/d/q]`, enter `c` to configure the audit, and press **Enter**.
4. At the prompt `Do you wish to enable Inactive Login Auditing? (Y/N) [Y]?`, enter `y` to turn on the audit, and press **Enter**.
5. At the prompt `Do you want to exempt any login accounts from the audit? (Y/N) [Y]?`, enter `y` to exempt login accounts from the audit, and press **Enter**.
6. Press **Enter** to accept the default list of exempted accounts.
7. At the prompt `Maximum number of inactive days before login account is locked`, press **Enter** to accept the default value for the number of days before account inactivity prior to account lock out.

Configuring the operating system warning banners

Use this procedure to configure warning banners to display a message before users enter their user names and password, and another message after a successful log on. Warning banners typically state the legal implications of logging on to a system.

Following two warning banners are available in the platform:

- **/etc/issue** (displayed before login)

  Note:

  For SSH, the file **/etc/issue** is shown after users enter their user name and before they enter their password. This is considered a pre-login warning banner for SSH.

- **/etc/motd** (displayed after login)

To configure the operating system warning banners, perform the following steps:

1. Configure the pre-login warning banner. See Configuring the pre-login warning banner on page 369.
2. Configure the post-login warning banner. See Configuring the post-login warning banner on page 369.
3. Verify the warning banners. See Verifying the warning banners on page 370.

Configuring the pre-login warning banner

About this task

Use this procedure to configure the warning banner that is displayed before users enter their user names and passwords. This task must be performed on all Element Manager servers and Avaya Media Servers.

Procedure

1. Log onto the server as the *ntsysadm* user.
2. At the command prompt, enter `vi /etc/issue` and press **Enter** to edit the pre-login banner.

   Note:

   You may use an editor other than *vi*.
3. Either cut and paste or type in the pre-login warning banner.
4. Save the file and exit the editor.

Configuring the post-login warning banner

About this task

Use this procedure to configure the warning banner that is displayed after the users log on successfully. This task must be performed on all Element Manager servers and Avaya Media Servers.

Procedure

1. Log onto the server as the *ntsysadm* user.
2. At the command prompt, enter `vi /etc/motd` and press **Enter** to edit the post-login banner.

   Note:

   You may use an editor other than *vi*.

3. Either cut and paste or type in the post-login warning banner.
4. Save the file and exit the editor.

Verifying the warning banners

About this task

Use this procedure to verify the pre-login and post-login warning banners. For SSH, the pre-login banner is displayed after the you enter your user name and before you are prompted for your password. The post-login banner is displayed after you enter your password and before you are presented with a shell prompt.

Procedure

1. Remotely access the server via SSH.
2. At the logon prompt, enter your user name and press **Enter**.
   The pre-login banner is displayed after the you enter your user name and before you are prompted for your password.
3. Enter your password and press **Enter**.
   The post-login banner is displayed after you enter your password.

   If the warning banners are not displayed after you configure them, contact the next level of support. Do not continue until you can verify the warning banners are displayed correctly.

Configuring operating system password and account policies

About this task

Use this procedure to configure the password complexity rules to ensure that user passwords are more secure. Password complexity rules apply only to subsequently configured passwords. This task must be performed on all Element Manager servers and Avaya Media Servers.

Procedure

1. Log onto the server as the *ntsysadm* user.
2. At the command prompt, enter **`pwConfig`** and press **Enter**.
3. If you are prompted for your password, enter your password and press **Enter**.

4. At the prompt `Selection [1 to 5]` for the **Password Configuration Options** menu, enter `2` to select **Change Current Settings** and press **Enter**.
5. Using the values from the **OS Password and Account Settings** section, enter the appropriate value and press **Enter** at each prompt.
6. At the prompt `Press Enter to continue`, press **Enter**.
7. At the prompt `Selection [1 to 5]` for the **Password Configuration Options** menu, enter `4` to select **Save current settings to system files** and press **Enter**.
8. At the prompt `Press Enter to continue`, press **Enter**.
9. At the prompt `Selection [1 to 5]` for the **Password Configuration Options** menu, enter `5` to exit the menu and press **Enter**.

Resetting the GRUB password

About this task

Use this procedure to configure the Linux Grand Unified Bootloader (GRUB) password. The GRUB password prevents unauthorized access to the bootloader. Once the password complexity is configured, you must reset the GRUB password to comply with these new settings. This task must be performed on all Element Manager servers and Avaya Media Servers.

Procedure

1. Log onto the server as the *ntsysadm* user.
2. At the command prompt, enter **`grubPWConfig`** and press **Enter**.
3. At the prompt `Enter 'c' to configure, 'd' to display, or 'q' to quit [c/d/q]`, enter `c` to configure the password and press **Enter**.
4. At the prompt `Enter the "bootloader" password`, enter a policy-compliant GRUB password and press **Enter**.
5. At the prompt `Enter the "bootloader" password again`, enter the GRUB password again and press **Enter**.

Hardening the database

About this task

This task must be performed on all servers that have the database installed.

Procedure

1. Log onto the server as the *ntsysadm* user.
2. At the command prompt, enter **`hardenDb`** and press **Enter**.

Configuring administrator accounts

Creating new user-specific accounts

About this task

This task must be performed for each OS administrator on each server. There should be at least one administrator per role on every system. The data mentioned in the following steps refers to the **OS Administrators** section from the **OS Hardening** tab of the Avaya Aura® Conferencing 7.2 Intelligent Workbook.

Procedure

1. Log onto the server as the *ntsysadm* user.
2. At the command prompt, enter **`userMgt`** and press **Enter**.
3. At the prompt `Enter Selection > (1 to 8)` for the **User Configuration Manager** menu, enter `1` to select **Add new user** and press **Enter**.
4. At the prompt `Please enter a user name [Between 6-30 chars]`, enter the *<role> username* and press **Enter**.
5. At the prompt `Enter Selection > (0,1000-10000) [0]`, press **Enter** to select the default value.
6. Enter the number for the appropriate role. The first role is the user's primary role. Separate multiple role entries with a comma (`,`).
7. Press **Enter**.

8. At the prompt `Would you like to continue (Y/N) [N]?`, enter `y` and press **Enter**.
9. At the prompt `Enter the <Role> username password` prompt, enter the initial password and press **Enter**.

   Note:

   This password is for initial login purposes only. The administrator will be required to change this password upon first login.
10. At the `Enter the <Role> username password` prompt, enter the initial password again and press **Enter**.
11. At the prompt `Would you like to add another user: (Y/N) [N]?`, enter `y` and press **Enter**.
12. Repeat steps 4 – 11 for the remaining OS administrators, selecting the appropriate role for each administrator. There should be only one role for each administrator.

    Note:

    All deployments do not use all roles that are available on the system. Add only those administrator accounts that are used in your deployment.

Example

Following is an example of a system that contains the pre-configured users and newly created administrators.

User	UID	Roles	Local Auth State	Sudo
[1] ntsysadm	20229	SSA	enabled	Y
[2] ntsecadm	20230	SA	enabled	N
[3] ntappadm	20228	AA	enabled	N
[4] ntbackup	20231	BA	enabled	N
[5] ntdbadm	20232	DBA	enabled	N
[6] ntossadm	20225	OSS	enabled	N
[7] init	20234	SSA, AA, DBA	disabled	Y
[8] craft	20235	AA	disabled	N
[9] jackSSA	20236	SSA	enabled	N
[10] tonySA	20237	SA	enabled	N
[11] chloeAA	20238	AA	enabled	N
[12] allisonBA	20239	BA	enabled	N

User	UID	Roles	Local Auth State	Sudo
[13] kimbDBA	20240	DBA	enabled	N

Allowing administrator sudo access

About this task

In the pre-configured installation, the *ntsysadm* user is given full sudo access, which allows that administrator to become root. Only administrators with full sudo access can become root, so you should give this privilege only to administrators that can be trusted with this level of authority. Full sudo access can only be granted when the **userMgt** tool is run via the root user.

Note:

If the *ntsysadm* user is deleted before a new SSA is given full sudo access, you must run the script **userMgt** via the console (that is, the attached KVM) when logged in as the root user.

Use this task to configure the System Security Administrator (SSA) username with sudo capabilities.

Procedure

1. Log onto the server as the *ntsysadm* user.
2. At the command prompt, enter **su -** and press **Enter**.
3. Enter the root password and press **Enter**.
4. Enter **userMgt.pl** and press **Enter**.
5. At the prompt `Enter Selection > (1 to 9)` for the **User Configuration Manager** menu, enter `6` to select **Sudo access management** and press **Enter**.
6. From the list of administrators, select the **System Security Administrator (SSA) username** and press **Enter**.
7. At the prompt `Would you like to continue (Y/N) [N]?`, enter `y` to continue and press **Enter**.
8. At the prompt `Would you like to allow/deny sudo for another user: (Y/N) [N]?`, enter `n` and press **Enter**.

Loading a new authentication file

About this task

After installation, the Client Services accounts are configured with the default authentication file. You must replace the default authentication file with the site-specific authentication file.

You must perform this task on each server.

Procedure

1. Upload the new authentication file to the *ntsysadm* user.
2. Log onto the server as the *ntsysadm* user.
3. At the command prompt, type `loadauth -f <new_authentication_file_pathname>` and press **Enter**.

Deleting pre-configured OS administrator accounts

About this task

This task must be performed on each server.

Note:

Before performing this procedure, make sure you have configured at least one user with the SSA role and sudo access. You must create at least one administrator per role on every system. For more information, see Creating new user-specific accounts on page 372.

Procedure

1. Log onto the server using the System Security Administrator (SSA) username.

   Note:

   Do not login as *ntsysadm* because that administrator will be deleted in this procedure.

2. At the command prompt, enter **`userMgt`** and press **Enter**.
3. At the prompt `Enter Selection > (1 to 8)` for the **User Configuration Manager** menu, enter `2` to select **Delete a user** and press **Enter**.
   A list of all administrators on the system is displayed. You must delete the following administrators from the system via this menu:
   - ntsysadm
   - ntsecadm

- ntappadm
- ntbackup
- ntdbadm
- ntossadm

4. When prompted to confirm the deletion of each user, enter `y` and press **Enter**.
5. At the **User Configuration Manager** menu, enter `5` to select **List users on this system** and press **Enter**.
6. Confirm that there are no pre-configured users listed. The only users listed should be those listed in **OS Administrators**.

Example

Following is an example of a system where all pre-configured accounts except Avaya Services accounts have been deleted, an administrator for the five major roles has been created, and full sudo access has been provided to one SSA user.

User	UID	Roles	Local Auth State	Sudo
[1] init	20234	SSA, AA, DBA	disabled	Y
[2] craft	20235	AA	disabled	N
[3] jackSSA	20236	SSA	enabled	Y
[4] tonySA	20237	SA	enabled	N
[5] chloeAA	20238	AA	enabled	N
[6] allisonBA	20239	BA	enabled	N
[7] kimbDBA	20240	DBA	enabled	N

Configuring the access control list (ACL)

There are two parts to the ACL configuration: internal ACL rules and external ACL rules. The internal rules pertain to connections that are used within the system and are auto-generated from the Avaya Aura® Conferencing database. The external rules pertain to restricting external access to Avaya Aura® Conferencing. You must configure the external rules manually. The following sections describe how to configure both internal and external ACL rules.

Note:

You must complete all tasks provided in Configuring internal ACL rules on page 377 and Configuring external ACL rules on page 379 before the ACL configuration is complete. The

internal ACL rules will be applied only when the external ACL rules are configured and committed.

Configuring internal ACL rules

About this task

Use the following procedure to configure internal ACL rules.

Procedure

1. Generate an internal ACL configuration file. See Generating an internal ACL configuration file on page 377.
2. Install an internal ACL configuration file on the primary Element Manager server. See Installing an internal ACL configuration file on the primary Element Manager server on page 378.
3. Install an internal ACL configuration file on all other servers. See Installing an internal ACL configuration file on all other servers on page 378.

Generating an internal ACL configuration file

Before you begin

You must be able to log onto the primary Element Manager server a user with the Application Administrator (AA) role.

About this task

Use the following procedure to generate an internal ACL configuration file.

Procedure

1. Log onto the primary Element Manager server as a user with the AA role.
2. At the command prompt, enter `cd /var/mcp/install` and press **Enter**.
3. Enter `mcpGenIntACLConfig.pl` and press **Enter**.
   The internal ACL configuration file has now been generated and resides on the primary Element Manager server. You must now install the internal ACL configuration file on all servers in the system (including the primary Element Manager server).

Installing an internal ACL configuration file on the primary Element Manager server

Before you begin

You must be able to log onto the primary Element Manager server as a user the System Security Administrator (SSA) role.

About this task

Use the following procedure to install an internal ACL configuration file on the primary Element Manager server.

Procedure

1. Log onto the primary Element Manager server as a user with the SSA role.
2. At the command prompt, enter `mcpInstIntACLConf –copy` and press **Enter**.

Installing an internal ACL configuration file on all other servers

Before you begin

You must be able to log onto the primary Element Manager server a user with the System Security Administrator (SSA) role.

About this task

Use the following procedure to install an internal ACL configuration file on all other servers.

Procedure

1. Log onto the server as a user with the SSA role.
2. At the command prompt, enter `mcpInstIntACLConf` and press **Enter**.
3. At the prompt `Remote server IP address`, enter the primary Element Manager server internal OAM IP address and press **Enter**.
4. At the prompt `SFTP user id`, enter the SSA user name defined on the primary Element Manager server and press **Enter**.
5. At the prompt `SFTP password`, enter the SSA password and press **Enter**.
6. At the prompt `Please retype the password to confirm`, re-enter the SSA password and press **Enter**.
7. At the prompt `Confirm (Y or N)`, enter `y` and press **Enter**.

Note:

If you receive an error message that the remote host identification has changed, see Fixing remote host SSH keys on page 394 to fix the problem. Once you fix the keys, retry the script on this server.

8. Repeat Steps 1 through 7 on all remaining servers in the system.

Note:

The internal ACL rules are applied to the system only after you commit the ACL rules via the **iptcfg** tool. See Importing an external ACL configuration file on page 380.

Configuring external ACL rules

About this task

There are multiple methods available for configuring external ACL rules. The **iptcfg** tool provides an interactive menu that enables you to

- configure the settings for an individual node
- configure the settings for a port
- configure the DSCP settings
- import configuration files

The import files used in this section were auto-generated after the platform was installed. If the import file want not generated automatically, you must create that file manually.

When external ACL rules are committed via the **iptcfg** tool, the internal ACL rules file (previously installed) is used by the **iptcfg** tool to create firewall rules for the internal nodes. No further action is required to include the internal ACL rules.

Use the following procedure to configure external ACL rules.

Procedure

1. If the Avaya Media Server is deployed on the target server, prepare the Avaya Media Server. See Preparing the Avaya Media Server on page 380.
2. Perform one of the following steps:
   - Create a configuration file and then import it using the **iptcfg** tool. See Importing an external ACL configuration file on page 380.
   - Configure the rules manually using the **iptcfg** tool. See Configuring external ACL rules manually (using the iptcfg tool) on page 382.

3. Verify the ACL configuration. See Verifying the ACL configuration on page 385.

Preparing the Avaya Media Server

Before you begin

- You must be able to log onto the server as a user with the System Security Administrator (SSA) role.
- You must know the root password.

About this task

Perform this procedure on all servers where the Avaya Media Server is deployed, regardless of the layout type (that is, co-resident or standalone).

Procedure

1. Log onto the server as a user with the SSA role.
2. At the prompt, enter `su -` and press **Enter**.
3. At the prompt password, enter the root password, and press **Enter**.
4. Enter `aacconfiginstall.pl` and press **Enter**.
5. At the prompt `Do you install Media Server and Application Server on the same server ? (Y/N)`, perform one of the following steps:
   - If the Avaya Media Server is located with other Application Server components (for example, co-resident redundant configuration, co-resident redundant with DMZ configuration, co-resident simplex configuration, and co-resident simplex with DMZ configuration), enter `y` and press **Enter**.
   - If the Avaya Media Server is not located with other Application Server components (for example, standalone redundant configuration and standalone simplex configurations), enter `n` and press **Enter**.
6. At the prompt `Proceed (Y or N)` after the warning about committing system default settings to iptables, enter `y` and press **Enter**.

Importing an external ACL configuration file

Before you begin

You must be able to log onto the server as a user with the System Security Administrator (SSA) role.

About this task

Use the following procedure to import an external ACL configuration file. The import files are server specific. As a result, each server in the Avaya Aura® Conferencing system will require

its own import file containing IP addresses that are specific to that server. The Element Manager server import file and the Avaya Media Server import file differ slightly.

The Avaya Media Server ACL import file has additional syntax that is not present in the Element Manager Server import file. For more information, see the Avaya Media Server-specific ACL import example file, which is located in the directory `/opt/mcp/ipt/example` on an Avaya Media Server. You must use the root login to access this directory.

You can view an example of an Element Manager server ACL configuration file with instructions on how to configure the file. This example file is located in the directory `/opt/mcp/ipt/example` on the Avaya Aura® Conferencing server. You must use the root login to access this directory.

Note:

Since the Element Manager server import file and the Avaya Media Server import file differ slightly, it is important that you use the appropriate example file for each server type.

The following are examples of external trusted nodes that you may need to configure in the import file:

- remote syslog server
- remote NTP server
- administrator PCs
- DNS servers

To see an example of an external ACL configuration file, see Example of import.dat file on page 387.

To see the lists of trusted nodes, trusted ports, and DSCP settings that you must configure on each server according to your deployment layout, see External ACL configuration settings on page 386.

Note:

You must perform this procedure on all servers in the Avaya Aura® Conferencing system.

Procedure

1. Log onto the server as a user with the SSA role.
2. At the prompt, enter `su -` and press **Enter**.
3. At the password prompt, enter the root password, and press **Enter**.
4. Create an ACL import file based on a server-specific ACL import example file (import.dat).

   The example file of an Element Manager server ACL configuration file is located in the directory `/opt/mcp/ipt/example` on the Avaya Aura® Conferencing server.

The Avaya Media Server-specific ACL import example file is located in the directory `/opt/mcp/ipt/example` on an Avaya Media Server.

Note:

Ensure that the trusted nodes listed in the import file contain the IP address of the administrator PC from which you log onto the server. If the administrator PC is not configured as a trusted node, you will be unable to access this server once the ACL rules are committed. (Access to this server will be blocked.)

5. After you create the ACL import file, enter `iptcfg` and press **Enter**.
   The IPTables Configurations Options menu appears.
6. At the prompt `Selection [1 to 9]`, enter `4` to select **Import Configurations**, and press **Enter**.
   A warning appears informing you that this operation will revise the existing IPTables rules.
7. At the prompt `Proceed (Y or N)`, enter `y` and press **Enter**.
8. At the prompt `Import file name (full path)`, enter the full path and ACL import file name for this server and press **Enter**.
   The following warning appears:

   ```
   WARNING: Trusted nodes must include those from which the user
   logs into the current server to perform the maintenance
   tasks. If you have not specified them as trusted nodes in the
   import file, you will not be able to log in to the server
   again after the importing has completed.
   ```
9. At the prompt `Proceed (Y or N)`, enter `y` and press **Enter**.

Configuring external ACL rules manually (using the iptcfg tool)

Before you begin

You must be able to log onto the server as a user with the System Security Administrator (SSA) role.

About this task

Use this procedure to configure the external ACL rules using the **iptcfg** tool. See External ACL configuration settings on page 386 to determine the list of trusted nodes, trusted ports, and DSCP settings you must configure on each server.

Note:

You must perform this procedure on all servers in the Avaya Aura® Conferencing system.

Procedure

1. Log onto the server as a user with the SSA role.
2. At the command prompt, enter `iptcfg` and press **Enter**.
   The IPTables Configurations Options menu appears.
3. At the prompt `Selection [1 to 9]`, enter `1` to select **Configure Trusted Nodes**, and press **Enter**.
   The Trusted Nodes Configuration Options menu appears.
4. Perform the following steps for each trusted node you want to add to the configuration:
   a. At the prompt `Selection [1 to 6]`, enter `2` to select **Add a new trusted node configuration**, and press **Enter**.
   b. Enter the local IPv4 node address.
   c. At the prompt `Enter trusted node type`, enter `1` to add a single trusted node to the local IPv4 address you entered in Step B, and press **Enter**.
   d. Enter the IPv4 trusted node address, and press **Enter**.
   e. Enter `y` and press **Enter** to confirm your action.
   f. Repeat Steps A through E for each trusted node you want to add to the configuration.
5. At the prompt `Selection [1 to 6]` for the Trusted Nodes Configuration Options menu, enter `5` to select **Return to main menu**, and press **Enter**.
6. Enter `y` and press **Enter** to confirm your action.
   The IPTables Configurations Options menu appears.

   Note:

   The list of trusted nodes is not added to the IPTables rules yet. The changes will be committed to the IPTables rules after you complete this procedure.
7. At the prompt `Selection [1 to 9]`, enter `2` to select **Configure Trusted Ports**, and press **Enter**.
   The Trusted Port Configuration Options menu appears.
8. Perform the following steps for each trusted port you want to be enabled on the server:
   a. At the prompt `Selection [1 to 4]`, enter `1` to select **List all trusted port configuration**, and press **Enter**.
   The list of all trusted port configurations is displayed.
   b. At the prompt `Selection [1 to 4]`, enter `2` to select **Modify a trusted port configuration**, and press **Enter**.
   c. At the prompt `Enter ID of trusted port configuration to be modified`, enter the ID of the port you want to modify (from the list of all trusted port configuration), and press **Enter**.

d. Press **Enter** to confirm your action.
e. At the prompt `Enter port status`, enter `1` to enable the port or enter `0` to disable the port.
f. Press **Enter**.
g. Press **Enter** to confirm your change.
h. Repeat Steps A through G for each trusted port you want to enable on the server.

9. At the prompt `Selection [1 to 4]` for the Trusted Port Configuration Options menu, enter `3` to select **Return to main menu**, and press **Enter**.
10. Enter `y` and press **Enter** to confirm your action.
The IPTables Configurations Options menu appears.

Note:

The list of trusted ports is not added to the IPTables rules yet. The changes will be committed to the IPTables rules after you complete this procedure.

11. At the prompt `Selection [1 to 9]`, enter `3` to select **DSCP Marking**, and press **Enter**.
The DSCP Marking Configuration Options menu appears.
12. Perform the following steps for each DSCP value you want to configure on the server:

a. At the prompt `Selection [1 to 4]`, enter `1` to select **Show DSCP marking configuration**, and press **Enter**.
The DSCP marking configuration is displayed.
b. At the prompt `Selection [1 to 4]`, enter `2` to select **Modify DSCP values**, and press **Enter**.
c. At the prompt `Enter ID of the DSCP category to be modified`, enter the ID of the DSCP value you want to modify (displayed in the DSCP marking configuration), and press **Enter**.
d. Enter the DSCP value and press **Enter**.
e. Press **Enter** to confirm your change.
f. Repeat Steps A through E for each DSCP value you want to configure on the server.

13. At the prompt `Selection [1 to 4]` for the DSCP Marking Configuration Options menu, enter `3` to select **Modify DSCP marking status**, and press **Enter**.
14. Enter `1` to enable the DSCP marking status or enter `0` to disable it.
15. Press **Enter**.
16. Press **Enter** to confirm your change.
17. At the prompt `Selection [1 to 5]` for the DSCP Marking Configuration Options menu, enter `4` to select **Return to main menu**, and press **Enter**.

18. Enter `y` and press **Enter** to confirm your action.
    The IPTables Configurations Options menu appears.

    Note:

    The DSCP configuration changes are not added to the IPTables rules yet. The changes will be committed to the IPTables rules after you complete this procedure.

19. At the prompt `Selection [1 to 9]`, enter `5` to select **Commit IPTables Rules**, and press **Enter**.
20. At the prompt `Proceed (Y or N)`, enter `y` and press **Enter**.
    The following warning appears:

    ```
    WARNING: Trusted nodes must include those from which the user
    logs into the current server to perform the maintenance
    tasks. If you have not configured these as trusted nodes, you
    will not be able to log in to the server again after the
    configuration changes are committed.
    ```

21. At the prompt `Proceed (Y or N)`, enter `y` and press **Enter**.

Verifying the ACL configuration

Before you begin

You must be able to log onto the server as a user with the System Security Administrator (SSA) role.

About this task

Use the following procedure to verify the ACL configuration.

Note:

You must perform this procedure on all Avaya Aura® Conferencing core servers and Avaya Media Servers.

Procedure

1. Log onto the server as a user with the SSA role.
2. At the command prompt, enter `ipstatus -n` and press **Enter**.
   The list of trusted nodes is displayed.
3. Verify that the list of trusted nodes contains the trusted nodes that you configured either in the import file or manually.

Note:

The full list of trusted nodes contains internal ACL trusted nodes as well as external trusted nodes that you configured either in the import file or manually. The list of external trusted nodes is a subset of all ACL rules.

4. Enter `ipstatus -p` and press **Enter**.
   The list of trusted ports is displayed.
5. Verify that the list of trusted ports matches the trusted ports that you configured either in the import file or manually.
6. Enter `ipstatus -d` and press **Enter**.
   The list of DSCP values is displayed.
7. Verify that the list of DSCP values matches the DSCP values that you configured either in the import file or manually.
8. Ensure that all rules according to the external ACL configuration table are configured. See External ACL configuration settings on page 386.

External ACL configuration settings

The following table shows how you should configure the trusted ports, trusted nodes, and DSCP marking on each server on the Avaya Aura® Conferencing system for each deployment layout.

Table 46: External ACL configuration settings

Deployment layout	Servers	Trusted Ports	Trusted Nodes	DSCP Marking
Co-resident (simplex and redundant)	Element Manager servers	6000 - 42599	• DSN server • remote NTP servers • remote syslog server • administrator PC	Disabled
Co-resident with DMZ (simplex and redundant)	Element Manager servers	6000–42599	• DSN server • remote NTP servers • remote syslog server • administrator PC	Disabled

Deployment layout	Servers	Trusted Ports	Trusted Nodes	DSCP Marking
	Web Conferencing Servers	443	• DNS server • remote NTP servers	Disabled
Standalone (simplex and redundant)	Element Manager servers		• DSN server • remote NTP servers • remote syslog server • administrator PC	Disabled
	Web Conferencing Servers	443	• DNS server • remote NTP servers	Disabled
	Avaya Media Servers	6000 - 42599	• DNS server • remote NTP servers	Disabled

Example of import.dat file

The rules for an external ACL configuration file appear in:

`/opt/mcp/ipt/example/import.dat`

Follow the instructions in the example file to configure an ACL configuration file properly.

Here is an example of the import.dat file (external ACL configuration file) for Element Manager servers in co-resident redundant and co-resident simplex layouts:

```
trusted node 192.168.209.241 192.168.209.212
trusted node 192.168.209.241 192.168.209.10
trusted node 192.168.209.241 192.168.209.20
trusted node 192.168.209.241 192.168.209.13
siptcpport 5060 0
siptcptlsport 5061 0
httpport 80 0
httpsport 443 1
dscpenabled falsed
dscpvalue 1 48
dscpvalue 2 18
dscpvalue 3 16
mediaports 6000 42599 1
```

Configuring a file system baseline

About this task

A baseline is a snapshot of all the system files including their size and permissions. You can compare baselines from various times to determine what has changed over a given period of time. You should create baselines on a regular basis or if there are any significant changes to the system, such as an upgrade.

This task must be performed on all Element Manager servers and Avaya media servers.

Procedure

1. Log onto the server using the System Security Administrator (SSA) username.
2. At the command prompt, enter **`fsibaseline`** and press **Enter**.

   At any time, you can compare the current system against previous baselines to determine what has changed. Refer to the Security Guide for more details on managing and comparing baselines.

Enabling Tomcat webserver access and error logs for the Element Manager

Procedure

1. Open the browser and access Element Manager Console from System Manager.
2. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Configuration Parameters**.
3. From the **Parm Group** drop-down box in the Element Manager Configuration Parameters window, select **WebServer**.
4. Select **EnableAccessLogs**.
5. Click **Edit (-/+)**.
6. From the Value box, select **true**.
7. Click **Apply**.
8. Close the Element Manager Configuration Parameters window.

Enabling Tomcat webserver access logs and audit logging for the Provisioning Manager

About this task

Use this task to enable the following settings for all Provisioning Managers in the system:

- Tomcat webserver access and error logs
- the generation of audit logs for Collaboration Agent and SOPI requests

Procedure

1. Open the browser and access Element Manager Console from System Manager.
2. In the navigation pane of Element Manager Console, select **Feature Server Elements > Provisioning Managers > <*Provisioning Manager name*> > Configuration Parameters**.
3. From the **Parm Group** drop-down box in the Provisioning Manager Configuration Parameters window, select **WebServer**.
4. Select **EnableAccessLogs**.
5. Click **Edit (-/+)**.
6. From the Value box, select **true**.
7. Click **Apply**.
8. From the **Parm Group** drop-down box in the Provisioning Manager Configuration Parameters window, select **PersonalAgent**.
9. Select **GenerateAuditLogs**.
10. Click **Edit (-/+)**.
11. From the Value box, select **true**.
12. Click **Apply**.
13. Close the Provisioning Manager Configuration Parameters window.
14. Repeat Steps 2 through 14 for each Provisioning Manager.

Enabling Tomcat webserver access logs and audit logging for the Personal Agent Manager

About this task

Use this task to enable the following settings for all Personal Agent Managers in the system:

- Tomcat webserver access and error logs
- the generation of audit logs for Collaboration Agent and SOPI requests

Procedure

1. Open the browser and access Element Manager Console from System Manager.
2. In the navigation pane of Element Manager Console, select **Feature Server Elements > Personal Agent Managers > <*Personal Agent Manager name*> > Configuration Parameters**.
3. From the **Parm Group** drop-down box in the Personal Agent Manager Configuration Parameters window, select **WebServer**.
4. Select **EnableAccessLogs**.
5. Click **Edit (-/+)**.
6. From the Value box, select **true**.
7. Click **Apply**.
8. From the **Parm Group** drop-down box in the Personal Agent Manager Configuration Parameters window, select **PersonalAgent**.
9. Select **GenerateAuditLogs**.
10. Click **Edit (-/+)**.
11. From the Value box, select **true**.
12. Click **Apply**.
13. Close the Personal Agent Manager Configuration Parameters window.
14. Repeat Steps 2 through 14 for each Personal Agent Manager.

Configuring local logon password policies for Element Manager Console and Provisioning Client

About this task

Use this procedure to configure the password policies for the local logon administration accounts for Element Manager Console and Provisioning Client.

Note:

The local logon account password policies do not affect the single-sign on (SSO) passwords used to access Element Manager Console and Provisioning Client via System Manager.

Procedure

1. Open the browser and access Element Manager Console locally (`https://<IP address>:12121` where *<IP address>* is the EM Internal OAM Service IP address. This is the logical IP address of the server running Element Manager Console).
2. Log in as the *admin* user.
3. From the Administration menu in Element Manager Console, select **Password Rules**.
4. In the Password Rules dialog box, update each setting according to the values in **EM/Prov Admin Password Policy** section of the Avaya Aura® Conferencing Intelligent Workbook.
5. When finished, click **Apply**.

Configuring local logon account login rules for Element Manager Console and Provisioning Client

About this task

Use this procedure to configure the login rules for the local logon administration accounts for Element Manager Console and Provisioning Client.

Note:

The local logon login rules do not affect the single-sign on (SSO) logon accounts used to access Element Manager Console and Provisioning Client via System Manager.

Procedure

1. Open the browser and access Element Manager Console locally (`https://<IP address>:12121` where *<IP address>* is the EM Internal OAM Service IP address. This is the logical IP address of the server running Element Manager Console).
2. Log in as the *admin* user.
3. From the Administration menu in Element Manager Console, select **Login Rules**.
4. From the **Login Interface** drop-down box in the Login Rules dialog box, select **Configuration Management (OMI)**.
5. Update each setting for the Element Manager Console local logon accounts according to the values in **OMI - Session Timeout (minutes), OMI - Failed Login Attempts before Lockout, OMI - Lockout Duration (minutes)** and **OMI - Account Inactivity (days)** in the Avaya Aura® Conferencing Intelligent Workbook.
6. From the **Login Interface** drop-down box, select **Provisioning Management (PROV)**.
7. Update each setting for the Provisioning Client local logon accounts according to the values in **Prov - Session Timeout (minutes), Prov - Failed Login Attempts before Logout, Prov - Lockout Duration (minutes)** and **PROV - Account Inactivity (days)** in the Avaya Aura® Conferencing Intelligent Workbook.
8. Click **Apply**.

Changing the Element Manager SNMP community string

About this task

The SNMP community string can only be changed for servers that are online and reachable on the network. Before performing this task, ensure that all servers in the system are reachable from the active Element Manager's server.

Procedure

1. Open the browser and access Element Manager Console from System Manager.
2. In the navigation pane of Element Manager Console, select **Feature Server Elements > SNMP Profiles**.
3. In the SNMP Profiles window, click **Add (+)**.
4. In the Add Server SNMP Profiles dialog box, perform the following steps:
   a. In the Profile Name box, enter the appropriate SNMP profile name.

b. In the Read Community String box, enter the appropriate SNMP Read Community String.
c. In the Write Community String box, enter the appropriate SNMP Write Community String.
d. Click **Apply**.

5. Close the SNMP Profiles window.
6. In the navigation pane of Element Manager Console, select **Servers**.
7. In the Servers window, select the server.
8. Click **Edit (-/+)**.
9. From the SNMP Profile drop-down box in the Edit Server dialog box, select the appropriate SNMP profile name.
10. Click **Apply**.
11. Repeats Steps 8 through 11 for each server listed.

Note:

If new servers are added, be sure to select the new SNMP profile when creating the new server.

Removing the default staging certificates

About this task

The final step in hardening the system is to remove the default staging certificates from the truststore. Make sure *all* sanity checks (including talking to the Avaya media server) have been successfully completed before performing this task. Once this task is completed, the system will no longer be accessible via the staging certificate.

Note:

You must restart the network elements after performing this procedure.

Procedure

1. Open the browser and access Element Manager Console from System Manager.
2. In the navigation pane of Element Manager Console, select **Security > Certificate Management > Truststore**.
3. In the Truststore window, select the row that contains **CN=Default Staging Certificate**.
4. Click **Delete (-)**.

5. In the Confirmation dialog box, click **Yes**.
6. Restart the network elements for the changes to take effect and to clear alarms.

Configuring Avaya Media Server DSCP

About this task

This task must be performed for each Avaya Media Server cluster in the system.

Procedure

1. Open the browser and access Element Manager Console from System Manager.
2. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <*Cluster name*> > DSCP Settings**.
3. In the **SIP QoS DSCP** box in the DSCP Settings dialog box, enter the appropriate value.
4. In the **Audio QoS** box, enter the appropriate value.
5. In the **Video QoS** box, enter the appropriate value.
6. Click **Apply**.
7. Restart the Avaya Media Server network elements for the cluster.
8. Repeat Steps 2 through 7 for each Avaya Media Server cluster in the system.

Fixing remote host SSH keys

About this task

When an SSH session is created for the first time, the remote servers public key is stored in `/root/.ssh/known_hosts`. If this key changes for any reason (a server reinstall is the primary reason), then SSH will not allow a connection to continue until that key is manually removed from the `known_hosts` file.

If the following warning is displayed when running the mcpInstIntACLConf scripts, the file `/root/.ssh/known_hosts` must be modified before the SSH connection to the remote server will succeed:

```
WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! IT IS POSSIBLE THAT
SOMEONE IS DOING SOMETHING NASTY! Someone could be eavesdropping on
you right now (man-in-the-middle attack)! It is also possible that
```

```
the RSA host key has just been changed. The fingerprint for the RSA
key sent by the remote host is 60:75:7a:9e:af:88:85:e7:c7:3d:
82:d6:c5:7e:a8:a8. Please contact your system administrator. Add
correct host key in /root/.ssh/known_hosts to get rid of this
message.
```

To modify the file `/root/.ssh/known_hosts`, perform this task on the server where the script is being run.

Procedure

1. Log onto the server as an SSA user.
2. At the command prompt, enter **`su -`** and press **Enter**.
3. Enter the root password and press **Enter**.
4. Edit the file `/root/.ssh/known_hosts`.

   Each line in this file has an IP address followed by the public key for that IP address.
5. Delete the line for the remote server.
6. Save the file.
7. Once the file has been modified, retry the script from the same server.

Chapter 25: Configuring collaboration aware clients for Avaya Aura® Conferencing

This chapter describes the settings you must configure to use the following “collaboration aware” clients with Avaya Aura® Conferencing 7.2:

- Avaya Flare® Experience for Windows
- Avaya Flare® Experience for iPad Devices
- the following Avaya 96x1 SIP telephones:
  - Avaya 9608 SIP Telephone
  - Avaya 9611G SIP Telephone
  - Avaya 9621G SIP Telephone
  - Avaya 9641G SIP Telephone

Configuring the settings for Avaya Flare® Experience for Windows

About this task

Use this procedure to configure the appropriate settings in Avaya Communication Manager and System Manager for Avaya Flare® Experience for Windows.

Use the Avaya Aura® System Manager administration interface to modify the Avaya Communication Manager settings and add or modify a user. For more information, see *Installing and Configuring Avaya Aura® Session Manager* on the Avaya Web site at http://www.avaya.com/support.

Note:

Avaya Flare® Experience for Windows supports only SIP endpoints. H.323 endpoints are not supported.

Procedure

1. For Avaya Communication Manager, perform the following steps:
   - For the Communication Manager signaling group associated with Avaya Session Manager, set **Initial IP-IP Direct Media** to **y**.
   - On page 19 of System Parameters – Features, set **SIP Endpoint Managed Transfer** to **y**.
   - On page 4 of the IP-Options System Parameters, set **Override ip-codec-set for SIP direct-media connections** to **y**.
2. For each Avaya Flare® Experience for Windows extension, perform the following steps:
   - Set an **Avaya E.164** communication address.
   - Set Template to 9640SIP (for example, **DEFAULT_9640SIP_CM_6_2**).
   - Enable **IP SoftPhone**.
   - Enable **IP Video Softphone**.
   - Set **Type of 3PCC Enabled** to **Avaya**.
   - Configure eight call appearances to provide support for Adhoc conferences.
   - Enable **Presence Buddy** for Aura® contacts.
   - Set **Origination Application Sequence** to the Communication Manager server.
   - Set **Termination Application Sequence** to the Communication Manager server.
   - Enable **Conference Profile** and configure the settings for the user's Avaya Aura® Conferencing profile.

Configuring the settings for Avaya Flare® Experience for iPad Devices

About this task

Use this procedure to configure the appropriate settings in Avaya Communication Manager and System Manager for Avaya Flare® Experience for iPad Devices.

Use the Avaya Aura® System Manager administration interface to modify the Avaya Communication Manager settings and add or modify a user. For more information, see

Installing and Configuring Avaya Aura® Session Manager on the Avaya Web site at http://www.avaya.com/support.

Note:

Avaya Flare® Experience for iPad Devices supports only SIP endpoints. H.323 endpoints are not supported.

Procedure

1. For Avaya Communication Manager, perform the following steps:
   - For the Communication Manager signaling group associated with Avaya Session Manager, set **Initial IP-IP Direct Media** to **y**.
   - On page 19 of System Parameters – Features, set **SIP Endpoint Managed Transfer** to **y**.
   - On page 4 of the IP-Options System Parameters, set **Override ip-codec-set for SIP direct-media connections** to **y**.
2. For each Avaya Flare® Experience for iPad Devices extension, perform the following steps:
   - Set an **Avaya E.164** communication address.
   - Set Template to 9640SIP (for example, **DEFAULT_9640SIP_CM_6_2**).
   - Enable **IP SoftPhone**.
   - Set **Type of 3PCC Enabled** to **Avaya**.
   - Configure eight call appearances to provide support for Adhoc conferences.
   - Enable **Presence Buddy** for Aura® contacts.
   - Set **Origination Application Sequence** to the Communication Manager server.
   - Set **Termination Application Sequence** to the Communication Manager server.
   - Enable **Conference Profile** and configure the settings for the user's Avaya Aura® Conferencing profile.

Configuring the settings for Avaya 96x1 SIP telephones

About this task

Use this procedure to configure the appropriate settings in the 46xxsettings.txt file and System Manager for the following Avaya 96x1 SIP telephones:

- Avaya 9608 SIP Telephone
- Avaya 9611G SIP Telephone
- Avaya 9621G SIP Telephone
- Avaya 9641G SIP Telephone

Use the Avaya Aura® System Manager administration interface to add or modify a user. For more information, see *Installing and Configuring Avaya Aura® Session Manager* on the Avaya Web site at http://www.avaya.com/support.

Procedure

1. In the 46xxsettings.txt file, set the parameter `CONFERENCE_FACTORY_URI` to the Adhoc conferencing service URI access number with SIP domain. For example, if the Adhoc conferencing service URI access number with SIP domain is 1244501@yourcompany.com, you would specify the following text in the 46xxsettings.txt file:`SET CONFERENCE_FACTORY_URI "1244501@yourcompany.com"`)
2. For each Avaya 96x1 SIP telephone extension, perform the following steps:
   - Configure eight call appearances to provide support for Adhoc conferences.
   - Enable **Conference Profile** and configure the settings for the user's Avaya Aura® Conferencing profile.

Chapter 26: Deploying the Avaya Aura® Conference Manager Add-in for Microsoft Outlook®

The Avaya Aura® Conference Manager Add-in for Microsoft Outlook® uses Outlook's Calendar Meeting feature to help users create and manage their conference invitations.

Note:

The Avaya Aura® Conference Manager Add-in for Microsoft Outlook® works with Microsoft Outlook 2007 and Microsoft Outlook 2010.

You can use one of the following models for deploying the Avaya Aura® Conference Manager Add-in for Microsoft Outlook®:

- ClickOnce deployment

  With the ClickOnce deployment, you must place the Avaya Aura® Conference Manager Add-in files on to a web server or other public location (like a network share) that Avaya Aura® Conferencing users can access. The users will then run the Avaya Aura® Conference Manager Add-in installer from that location. Once the users install the Avaya Aura® Conference Manager Add-in, updates will be applied automatically when available. For this deployment, each user must run the installer.

- Centralized software deployment

  With the centralized software deployment, you may configure a group policy so that individual computer configurations are updated. The Windows registry is modified to point to the Microsoft Outlook Add-in deployment manifest. When Microsoft Outlook is restarted, it will automatically download the Avaya Aura® Conference Manager Add-in from the specified location.

Note:

Once installed, the Avaya Aura® Conference Manager Add-in will check for updates every two weeks at the same location from which Avaya Aura® Conference Manager Add-in was installed. Make sure that location contains the latest version of the Avaya Aura® Conference Manager Add-in. To publish an updated version of the Avaya Aura® Conference Manager Add-in, remove the contents of the folder at that location, and then place the new files in that location.

Implementing a ClickOnce deployment

Before you begin

- You must have the file *asu_version_date_time.zip* (for example, *asu_1.0.0.176_2012-12-13_15-44-20.zip*) , which is bundled with Collaboration Agent. The file *asu_version_date_time.zip* is located in `/var/mcp/media/prov_pa_installs/outlook/asu` on the server where Avaya Aura® Conferencing 7.2 is installed.
- To use the Avaya Aura® Conference Manager Add-in for Microsoft Outlook®, a user must have:
  - Microsoft Outlook 2007 or Microsoft Outlook 2010 installed
  - an account (with a moderator code) on the Avaya Aura® Conferencing 7.2 system

About this task

Use this procedure to implement the Avaya Aura® Conference Manager Add-in for Microsoft Outlook using the ClickOnce deployment. With the ClickOnce deployment, each user must run the Avaya Aura® Conference Manager Add-in installer.

Procedure

1. Unzip the contents of the file *asu_version_date_time.zip* (for example, *asu_1.0.0.176_2012-12-13_15-44-20.zip*) on a web server that all users can access. The file *asu_version_date_time.zip* contains the installation files for the Avaya Aura® Conference Manager Add-in. The file *asu_version_date_time.zip* is located in `/var/mcp/media/prov_pa_installs/outlook/asu` on the server where Avaya Aura® Conferencing 7.2 is installed.
2. Open your web browser and make sure you can browse the folder on the web server that contains the files you unzipped in Step 1.
3. From the folder that contains the installation files for the Avaya Aura® Conference Manager Add-in, download the file *setup.exe* to a PC running Microsoft Windows.
4. On the Windows PC that contains the file *setup.exe* that you downloaded in Step 3, perform the following steps:
   a. Select **Start > All Programs > Accessories > Command Prompt**.
   b. In the Command Prompt window, type the following command:

      ```
      setup.exe -url="http://FQDN_or_IP_address_of_your_server/Outlook Add-In"
      ```

      where `"http://FQDN_or_IP_address_of_your_server/Outlook Add-In"` is the URL to the folder that contains the Avaya Aura® Conference Manager Add-in installation files.

Comments? infodev@avaya.com

c. Upload the modified *setup.exe* file back to the folder that contains the installation files for the Avaya Aura® Conference Manager Add-in.

5. Make sure each user performs the following steps to install the Avaya Aura® Conference Manager Add-in:

   a. Open your web browser and go to the folder that contains the Avaya Aura® Conference Manager Add-in installation files.
   b. Click **setup.exe**.
   c. When prompted to run or save setup.exe, click **Run**.
   d. When prompted to confirm that you want to run this program, click **Run**.
   e. In the Avaya Aura Conference Manager Setup dialog box, read the license agreement.
   f. Click **Accept** to accept the terms of the license agreement.
   g. In the Microsoft Office Customization Installer dialog box, click **Install**.
   The Avaya Aura® Conference Manager Add-in is installed.
   h. When the installation is complete, click **Close**.
   i. Start Microsoft Outlook.
   The Avaya Aura dialog box should appear, prompting you to enter your user name, password, and service host.

      The service host is the name of the Web Conferencing Host that you entered in the Provisioning Client window. It must be the hostname, not the IP address.
   j. Enter your user name, password, and address of the service host, and then click **Save**.

Related topics:

Configuring a Web conferencing host on page 255

Implementing a centralized software deployment

Before you begin

- To use the Avaya Aura® Conference Manager Add-in, the PC must contain the following software:
  - Microsoft Outlook 2007 or Microsoft Outlook 2010
  - Microsoft Windows Installer 3.1. (Typically, this is already present on a Windows PC.)
  - Microsoft .NET 4.0 Framework Client Profile
  - Microsoft VSTO 4.0 Runtime

- Avaya Event Log Source. This software configures the source in the Windows System Event Log so that the Microsoft Outlook Add-in can log events under the name **Avaya Aura Outlook Conference Manager**.

Microsoft Windows Installer 3.1, Microsoft .NET 4.0 Framework Client Profile, Microsoft VSTO 4.0 Runtime, and Avaya Event Log Source are available in the file *asu_version_date_time.zip* (for example, *asu_1.0.0.176_2012-12-13_15-44-20.zip*), which is bundled with Collaboration Agent. The file *asu_version_date_time.zip* is located in `/prov_pa_installs/outlook/` on the server where Avaya Aura® Conferencing 7.2 is installed.

- You have Administrative privileges on the Windows PC. (You need to access the Windows Registry.)

About this task

Use this procedure to implement the Avaya Aura® Conference Manager Add-in for Microsoft Outlook using the centralized deployment. With the centralized deployment, you can configure your domain to remotely deploy software to client computers from a central location.

Procedure

1. Unzip the contents of the file *asu_version_date_time.zip* (for example, *asu_1.0.0.176_2012-12-13_15-44-20.zip*) to a folder. The file *asu_version_date_time.zip* contains the installation files for the Microsoft Outlook Add-in. The file *asu_version_date_time.zip* is located in `/prov_pa_installs/outlook/` on the server where Avaya Aura® Conferencing 7.2 is installed.
2. Modify the Windows Registry file *aacAddin.reg* to point to the location of the deployment manifest for the Avaya Aura® Conference Manager Add-in. An example of the manifest setting in the Windows Registry is:

   ```
   "Manifest"="http://localhost/Outlook Add-In v.1.0.0.141/
   Avaya.Aura.ConferenceManager.vsto"
   ```

3. On each client PC, perform the following steps:
   a. Install Microsoft VSTO 4.0 Runtime.
   b. Install Avaya Event Log Source.
   c. Install Microsoft .NET 4.0 Framework Client Profile.
   d. Download and save the file *aacAddin.reg* to your desktop.
   e. Right-click on *aacAddin.reg* and select **Merge**.
   f. Exit Microsoft Outlook.
   g. Restart Microsoft Outlook.
   h. In the Microsoft Office Customization Installer dialog box, click **Install**. The Avaya Aura dialog box should appear, prompting you to enter your user name, password, and service host.

      The service host is the name of the Web Conferencing Host that you entered in the Provisioning Client window. It must be the hostname, not the IP address.

i. Enter your user name, password, and address of the service host, and then click **Save**.

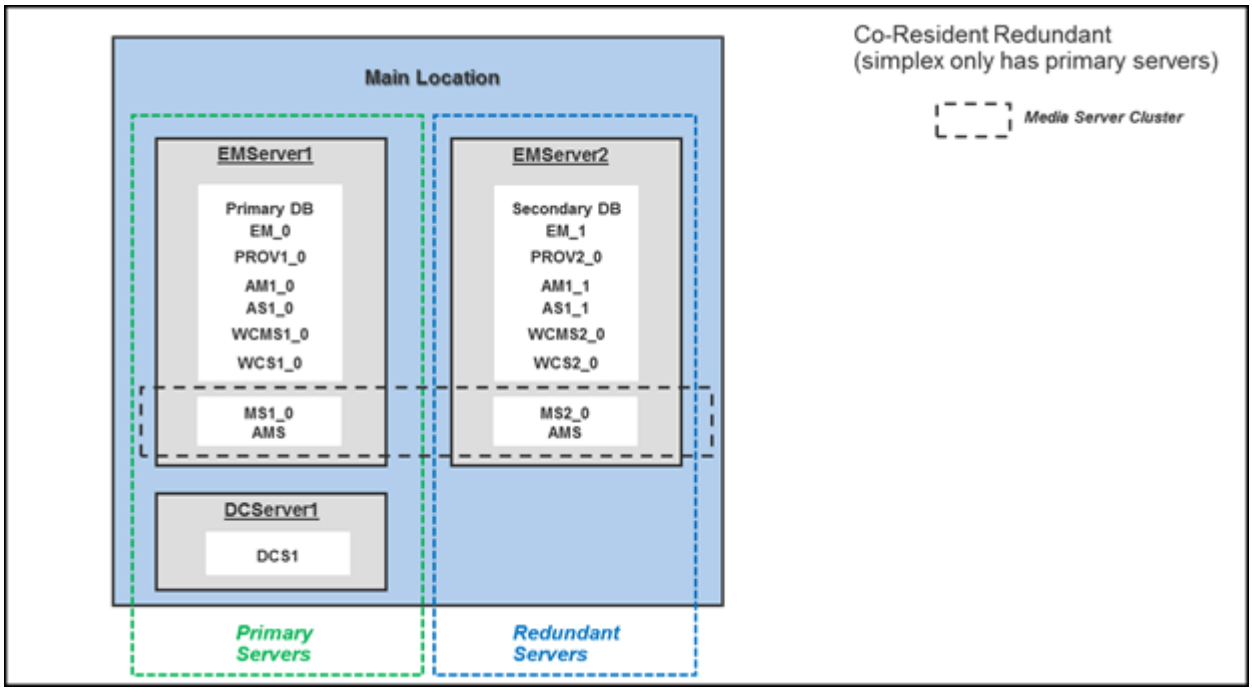
Related topics:

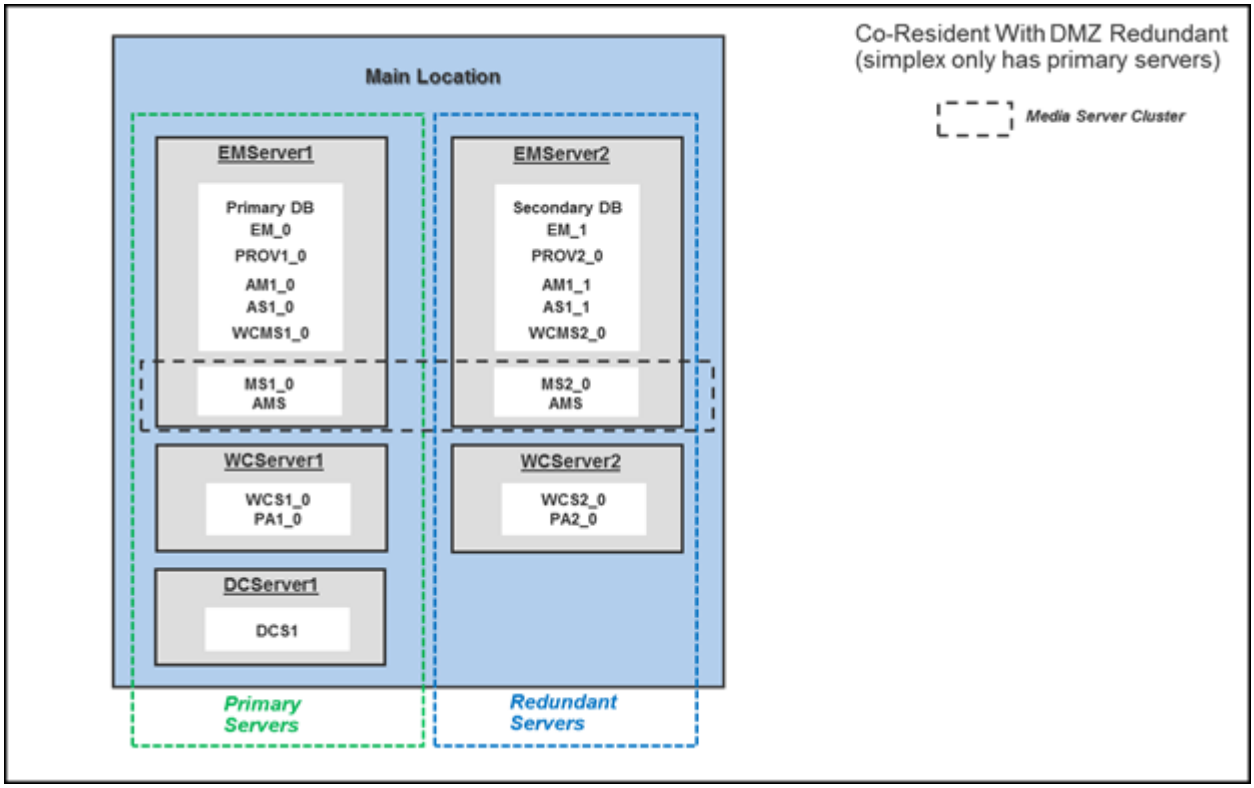
Configuring a Web conferencing host on page 255

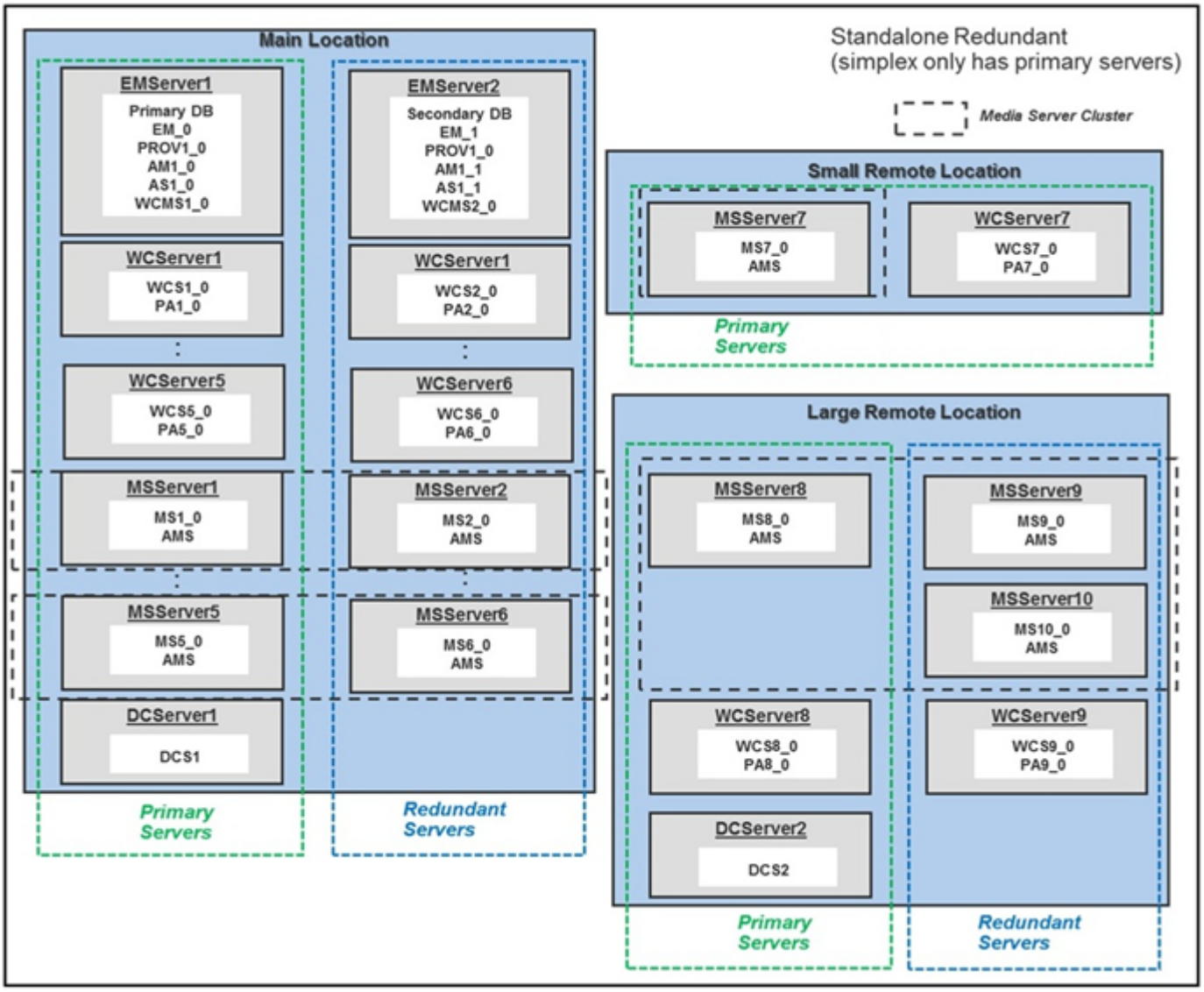
Chapter 27: Upgrading to Release 7.2

This section describes how to upgrade your existing Avaya Aura® Conferencing Release 7.0 system to Release 7.2.

Before upgrading the system, you must identify the primary servers and redundant servers in a redundant deployment. In a simplex deployment, there are no redundant servers. The following diagrams show the supported deployment configurations and identify the primary and redundant server reference in the upgrade procedure.




Co-Resident With DMZ Redundant
(simplex only has primary servers)
Media Server Cluster
Main Location
EMServer1
Primary DB
EM_0
PROV1_0
AM1_0
AS1_0
WCMS1_0
MS1_0
AMS
EMServer2
Secondary DB
EM_1
PROV2_0
AM1_1
AS1_1
WCMS2_0
MS2_0
AMS
WCServer1
WCS1_0
PA1_0
WCServer2
WCS2_0
PA2_0
DCServer1
DCS1
Primary Servers
Redundant Servers



You can expand standalone configurations to have media servers in multiple remote locations. Note that the previous diagram does not depict all potential configurations. The media servers in the remote locations may be used to host local conferencing or may be configured to support cascading. Regardless, the media servers are always in clusters. Each cluster has at least a primary media server assigned to it. When determining the primary servers to upgrade in a remote location, examine the configuration for each media server cluster in that location and select the primary media server.

Depending on your deployment configuration, see the appropriate section:

- To upgrade a co-resident deployment, see Upgrade procedure for a co-resident deployment on page 412.
- To upgrade a standalone deployment, see Upgrade procedure for a standalone deployment on page 423.

Note:

Avaya recommends allocating at least one day to the task of upgrading Avaya Aura® Conferencing release 7.0 to release 7.2. This estimate of time does not include an LDAP integration. Avaya recommends performing an LDAP integration on another day.

Upgrading a co-resident deployment to Release 7.2

Before you begin checklist

The following checklist provides the high level steps and considerations prior to beginning your upgrade of an Avaya Aura® Conferencing co-resident deployment.

#	Task	Description	Notes	✔
1	Download the Avaya Aura® Conferencing 7.2 Intelligent Workbook from the Avaya Web site. The Intelligent Workbook addresses the following new components available in Avaya Aura® Conferencing 7.2: • Recording server(s) (to support the Recording feature) • Flash Media Gateway server(s) (to support the Audio/Video in Collaboration Agent feature)	Go to http://support.avaya.com/ to download the Avaya Aura® Conferencing Intelligent Workbook.		
2	Determine your hardware type.	1. Obtain the Avaya Aura® Conferencing 7.2 Upgrade Kit from Avaya. The Upgrade Kit		

#	Task	Description	Notes	✔
	1. Are you using on an HP ProLiant DL360 G7? **OR** 2. Are you are using a repurposed Dell™ PowerEdge™ R610 or an IBM S8800 system?	enables you to upgrade the HP ProLiant DL360 G7 to support the Recording feature. The Upgrade Kit contains two 900 GB hard disk drives. **OR** 2. You must install Avaya Aura® Conferencing 7.2 on a new HP ProLiant DL360 G7. **Note:** You can repurpose the Dell PowerEdge R610 or IBM S8800 as a host for the Web Conferencing server and/or Flash Media Gateways server.		
3	Store the Avaya Aura® Conferencing 7.0 disks for Avaya Aura® Conferencing software installation and patches in a secure place: • AAC Platform DVD-ROM • Application Bundle DVD-ROM • Platform patches DVD-ROM **Note:** You will need the Avaya Aura® Conferencing 7.0 software if you want to perform a rollback.	DVD-ROM disks were provided. You can also download from Avaya PLDS and burn your own CD- or DVD-ROM (for advanced users only).		
4	Obtain the latest Avaya Aura® Conferencing 7.2 disks for software	DVD-ROM disks are provided. You can also download from Avaya PLDS and burn your own CD- or DVD-ROM (for advanced users only).		

#	Task	Description	Notes	✔
	installation and patches: • AAC Platform DVD-ROM • Application Bundle DVD-ROM • Platform patches DVD-ROM			

Upgrade procedure for a co-resident deployment

The following table provides a high-level view of the tasks involved in upgrading a co-resident deployment to Release 7.2.

Note:

Upgrading to Release 7.2 is an out-of-service procedure regardless of whether the system is in a simplex or redundant deployment configuration.

#	Task	Description	Notes	✔
1	Review the prerequisites.	See Before you begin checklist on page 410.		
2	Back up the: • Avaya Aura® Conferencing 7.0 database • Avaya Media Servers • Avaya Aura® Conferencing 7.0 server	See “Backing up Avaya Aura® Conferencing” in this guide.		
3	Copy and extract the Avaya Aura® Conferencing7.2 installation files to the servers.	See Copying and extracting installation files to servers on page 427.		

#	Task	Description	Notes	✔
4	If you have a redundant system, drop database replication.	See Dropping database replication on page 429.		
5	If you have multiple locations, stop and undeploy all network element instances on both the primary server and the redundant server for each remote location.	See Stopping and undeploying all network element instances on both the primary and redundant servers in each remote location on page 430.		
6	If you have a redundant system, stop and undeploy all network element instances *except the database network element instance* on the redundant servers in the main location.	See Stopping and undeploying all network element instances except the database on the redundant servers in the main location on page 431.		
7	Stop and undeploy all network element instances *except the Element Manager network element and database network element* on the primary servers in the main location.	See Stopping and undeploying all network element instances except the Element Manager and database instances on the primary servers in the main location on page 431.		
8	Stop the primary instance of the Element Manager network element.	See Stopping the primary network element instance of Element Manager on page 432.		
9	Patch the Avaya Aura® Conferencing Platform (operating system) on the primary servers in the main location.	See Patching the Avaya Aura Conferencing Platform on the primary servers in the main location on page 437.		

#	Task	Description	Notes	✔
10	Configure the DNS client.	See Configuring a DNS client on page 494.		
11	Upgrade the database software on the primary database server.	See Upgrading the database software on the primary database server on page 437.		
12	Upgrade the Avaya Aura® Conferencing Element Manager and primary database.	See Upgrading the Avaya Aura Conferencing Element Manager and primary database on page 438.		
13	Upgrade the remaining network element instances on the primary servers in the main location.	See Upgrading the remaining network element instances on the primary servers in the main location on page 439.		
14	Verify that the Avaya Aura® Conferencing system is operating correctly for users in the main location.	See Verifying system operation in the main location on page 439.		
15	If you have a multi-location configuration, upgrade the primary servers and verify the system is operating properly for users at each remote location.	See Upgrading the primary servers in each remote location and verifying operation on page 440.		
16	If you have a redundant system, upgrade the redundant network element instances *except the database network element instance* in the main location.	See Upgrading the redundant network element instances except the database in the main site on page 441.		
17	If you have a redundant system and a multi-location configuration, upgrade the redundant network element	See Upgrading the redundant servers and network element instances in each		

#	Task	Description	Notes	✔
	instances and Avaya Media Servers in each remote location.	remote location on page 441.		
18	If you have a redundant system, upgrade the database software on the secondary database server.	See Upgrading the database software on the secondary database server on page 442.		
19	If you have a redundant system, set up database replication.	See Setting up database replication on page 443.		
20	On the Avaya Aura® Conferencing7.2 system, back up: • the database • the primary server • the secondary server **Note:** Copy all backup files to an external server. Do not leave the backup files on the Avaya Aura® Conferencing 7.2 servers. (You will be removing the hard drives from your existing servers during the upgrade process.)	See “Backing up Avaya Aura® Conferencing” in this guide.		
21	Install the 900 Gb drives from the Avaya Aura® Conferencing Upgrade Kit.	See Installing the 900 Gb hard drives into the HP DL360 G7 server on page 417.		
22	Reconfigure the RAID 1 configuration using the HP SmartStart CD.	See Reconfiguring the RAID 1 arrays using the HP SmartStart CD on page 131.		

#	Task	Description	Notes	✔
23	Start the installation process. **Important:** The Installing Linux procedure guides you through the installation process with links to individual procedures. Upon completion of each step, return to the next step in the Installing Linux procedure by clicking the link at the end of each individual procedure. **Note:** To support the DNS feature, you must configure the DNS client. See Configuring a DNS client on page 494.	See Installing the AAC Platform on page 116.		
24	Verify that all the required components are operational and error free after completing the Linux operating system installation.	See Verifying the AAC Platform installation on page 129.		
25	Format and mount the second RAID.	See Formatting and mounting the second RAID on page 132.		
26	Install the components for Avaya Aura® Conferencing 7.2.	See Installing the components for Avaya Aura Conferencing on page 135.		
27	Install the Avaya Media Server.	See Installing Avaya Media Server on page 134.		

#	Task	Description	Notes	✔
28	Patch database software.	See Patching database software on page 492.		
29	Restore the system from the Avaya Aura® Conferencing 7.2 backup you copied to an external server.	See “Restoring Avaya Aura® Conferencing” in this guide.		

Installing the 900 Gb hard drives into the HP DL360 G7 server

Before you begin

- You have backed up the AAC 7.0 system.
- You have the AAC 7.2 Upgrade Kit, which contains the two 900 Gb hard drives.
- You have the HP DL360 document set. For more information, see Downloading HP documentation on page 105.

About this task

Use this procedure to install the two 900 Gb hard drives from the AAC 7.2 Upgrade Kit into the HP DL360 G7 server.

Procedure

1. Observe safety warnings.
2. Observe all ESD safety precautions before unwrapping the new hard drives.
3. Power off the HP DL360 G7 server.
4. Lift the release lever on hard drive bay 3 on the server and remove the 300 Gb hard drive from hard drive bay 3. For more information about the locations of the hard drive bays, see Front view of HP DL360 G7 Server on page 106.
5. Insert a new 900 Gb drive into hard drive bay 3.
6. When the locking tab engages on the 900 Gb hard drive, close the release lever to securely seat the 900 Gb hard drive in hard drive bay 3.
7. Insert a new 900 Gb drive into hard drive bay 4.
8. When the locking tab engages on the 900 Gb hard drive, close the release lever to securely seat the 900 Gb hard drive in hard drive bay 4.

Reconfiguring the RAID 1 arrays using the HP SmartStart CD

Before you begin

- You have installed the two 900 Gb hard drives from the AAC 7.2 Upgrade Kit.
- You have the HP SmartStart CD.

About this task

Use this procedure to configure the four hard drives to two RAID 1 arrays on the HP DL360 G7 server.

Procedure

1. On the HP DL360 G7 server, insert the HP SmartStart CD into the CD-ROM drive.
2. Boot the system from the HP SmartStart CD.
3. When prompted, select the language you want to use, and then click **Next**.
4. Read the user license agreement.
5. To accept the user license agreement, click **Agree**.
6. When prompted to select the operation you want to begin, click **Maintenance**.
7. When prompted to select the maintenance operation you want to begin, click **HP Array Configuration and Diagnostics**.
8. In the Array Configuration Utility, select the device (for example, **Smart Array P410I in Embedded Slot**).
   The list of logical drives is displayed.
9. Remove all logical drives:
   a. Select the logical drives in the left panel.
   b. Click **Delete** in the right panel.
   c. When prompted, confirm that you want to remove the logical drives.
      The list of unassigned drives is displayed.
10. Create the first RAID:
    a. Click the **Wizard** tab.
    b. On the Wizard tab, click **Add Logical Drive**.
    c. Select the first two hard drives (HDD1 300 Gb in hard drive bay 1 and HDD2 300 Gb in hard drive bay 2), and click **Next**.
    d. When prompted to add remaining hard drives to the RAID, click **Next** to skip this step.
    e. In the Fault Tolerance section, select **RAID 1**, and click **Next**.
       The first RAID is now created.

11. Create the second RAID:
    a. Click the **Wizard** tab.
    b. On the Wizard tab, click **Add Logical Drive**.
    c. In the Select Logical Drive Creation Method section, select **Create Logical Drive or New Array**.
    d. Select the two remaining hard drives (HDD3 900 Gb in hard drive bay 3 and HDD4 900 Gb in hard drive bay 4), and click **Next**.
    e. In the Fault Tolerance section, select **RAID 1**, and click **Next**.
    The second RAID is now created.
12. On the bottom, left-corner of the window, click **Exit ASU** and exit from HP SmartSmart Tools.
    The server reboots.
13. Eject the HP SmartStart CD from the server.
    The hard drives are configured to the RAID arrays.

Formatting and mounting the second RAID

Before you begin

You have installed the two 900 Gb hard drives from the AAC 7.2 Upgrade Kit.

About this task

Use this procedure to format and mount the second logical drive on the HP DL360 G7 server.

Note:

The Recording feature requires the second logical drive. You must format and mount the second logical drive before installing the Avaya Media Server platform.

Procedure

1. Log on to the server as a user with the SSA role (for example, `ntsysadm`) through ssh or directly on the server console.
2. Enter **`su -`** to log on as root.
3. At the prompt `password`, type the root password, and press **Enter**.
4. Type `mcpDataDiskMgt.pl -q`, and press **Enter** to check that the second logical drive is available.
   The system should display information indicating that the RAID status is okay and the query command succeeded. An example of the output is:

```
The expected data partition '/dev/cciss/c0dlpl' is not
present on the system.
The raid controller reports:
```

```
A logical drive is available.
It is 838.2 GB large and RAID 1.
It has a RAID status of OK.
Query command succeeded.
```

5. Type `mcpDataDiskMgt.pl -f`, and press **Enter** to format the second logical drive.
   The system displays the following information:

```
Are you certain that you wish to reformat this disk?
All information that is currently on it will be lost! (Y/N) [N]?
```

6. Type `y`, and press **Enter** .
   The system should display the following information:

```
Format command succeeded.
```

7. Type `mcpDataDiskMgt.pl -q`, and press **Enter** to check that the second logical drive is ready for mounting.
   The system should display information indicating that the RAID status is okay and the query command succeeded. An example of the output is:

```
The expected data partition '/dev/cciss/c0dlpl' is not
currently mounted on /var/mcp/datadisk.
The raid controller reports:
A logical drive is available.
It is 838.2 GB large and RAID 1.
It has a RAID status of OK.
Query command succeeded.
```

8. Type `mcpDataDiskMgt.pl -m`, and press **Enter** to mount the second logical drive.
   The system should display the following information:

```
Created mount point
Mount command succeeded.
```

9. Type `mcpDataDiskMgt.pl -q`, and press **Enter** to check that the second logical drive is mounted.
   The system should display information indicating that the correct data partition is mounted. An example of the output is:

```
The correct data partition is mounted on the expected mount point.
The mount point information reported by the operating system is:
/dev/ciss/c0dlpl /var/mcp/datadisk ext3 rw, nosuid, nodev, data=ordered 0
The raid controller reports:
A logical drive is available.
It is 838.2 GB large and RAID 1.
It has a RAID status of OK.
Query command succeeded.
```

Upgrading a standalone deployment to Release 7.2

Before you begin checklist

The following checklist provides the high level steps you must perform before upgrading your Avaya Aura® Conferencing Release 7.0 standalone deployment to Release 7.2.

#	Task	Description	Notes	✔
1	Download the Avaya Aura® Conferencing 7.2 Intelligent Workbook from the Avaya Web site. The Intelligent Workbook addresses the following new components available in Avaya Aura® Conferencing 7.2: • Recording server(s) (to support the Recording feature) • Flash Media Gateway server(s) (to support the Audio/Video in Collaboration Agent feature)	Go to http://support.avaya.com/ to download the Avaya Aura® Conferencing Intelligent Workbook.		
2	Install the standalone Recording server(s). The Recording server must be an HP ProLiant DL360 G7 that contains two 900 GB drives.			

#	Task	Description	Notes	✔
3	Install the Flash Media Gateway server(s).			
4	Store the Avaya Aura® Conferencing 7.0 disks for Linux and software installation, and patches in a secure place: • AAC Platform DVD-ROM • Application Bundle DVD-ROM • Platform patches DVD-ROM **Note:** You will need the Avaya Aura® Conferencing 7.0 software if you want to perform a rollback.	DVD-ROM disks were provided. You can also download from Avaya PLDS and burn your own CD- or DVD-ROM (for advanced users only).		
5	Obtain the latest Avaya Aura® Conferencing 7.2 disks for Linux and software installation, and patches: • AAC Platform DVD-ROM • Application Bundle DVD-ROM • Platform patches DVD-ROM	DVD-ROM disks are provided. You can also download from Avaya PLDS and burn your own CD- or DVD-ROM (for advanced users only).		

Upgrade procedure for a standalone deployment

The following table provides a high-level view of the tasks involved in upgrading an existing Avaya Aura® Conferencing standalone system to Release 7.2.

Note:

Upgrading to Release 7.2 is an out-of-service procedure regardless of whether the system is in a simplex or redundant deployment configuration.

#	Task	Description	Notes	✔
1	Review the prerequisites.	See Before you begin checklist on page 421.		
2	Back up the: • Avaya Aura® Conferencing 7.0 database • Avaya Media Servers • Avaya Aura® Conferencing 7.0 server	See "Backing up Avaya Aura® Conferencing" in this guide.		
3	Copy and extract the Avaya Aura® Conferencing7.2 installation files to the servers.	See Copying and extracting installation files to servers on page 427.		
4	If you have a redundant system, drop database replication.	See Dropping database replication on page 429.		
5	If you have multiple locations, stop and undeploy all network element instances on both the primary server and the redundant server for each remote location.	See Stopping and undeploying all network element instances on both the primary and redundant servers in each remote location on page 430.		
6	If you have a redundant system, stop and	See Stopping and undeploying all		

#	Task	Description	Notes	✔
	undeploy all network element instances *except the database network element instance* on the redundant servers in the main location.	network element instances except the database on the redundant servers in the main location on page 431.		
7	Stop and undeploy all network element instances *except the Element Manager network element and database network element* on the primary servers in the main location.	See Stopping and undeploying all network element instances except the Element Manager and database instances on the primary servers in the main location on page 431.		
8	Stop the primary instance of the Element Manager network element.	See Stopping the primary network element instance of Element Manager on page 432.		
9	Patch the Avaya Aura® Conferencing Platform (operating system) on the primary servers in the main location.	See Patching the Avaya Aura Conferencing Platform on the primary servers in the main location on page 437.		
10	Upgrade the database software on the primary database server.	See Upgrading the database software on the primary database server on page 437.		
11	Upgrade the Avaya Aura® Conferencing Element Manager and primary database.	See Upgrading the Avaya Aura Conferencing Element Manager and primary database on page 438.		
12	Upgrade the remaining network element instances on the primary servers in the main location.	See Upgrading the remaining network element instances on the primary servers in the main location on page 439.		

#	Task	Description	Notes	✔
13	Verify that the Avaya Aura® Conferencing system is operating correctly for users in the main location.	See Verifying system operation in the main location on page 439.		
14	If you have a multi-site configuration, upgrade the primary servers and verify the system is operating properly for users at each remote location.	See Upgrading the primary servers in each remote location and verifying operation on page 440.		
15	If you have a redundant system, upgrade the redundant network element instances *except the database network element instance* in the main location.	See Upgrading the redundant network element instances except the database in the main site on page 441.		
16	If you have a redundant system and a multi-location configuration, upgrade the redundant network element instances and Avaya Media Servers in each remote location.	See Upgrading the redundant servers and network element instances in each remote location on page 441.		
17	If you have a redundant system, upgrade the database software on the secondary database server.	See Upgrading the database software on the secondary database server on page 442.		
18	If you have a redundant system, set up database replication.	See Setting up database replication on page 443.		
19	Optionally, you can upgrade memory.	See Upgrading memory for the HP DL360 G7 server on page 452.		

Note:

Once you have completed the upgrade, you may configure the following new features for Release 7.2:

- Audio SRTP
- Recording
- Audio/Video in Collaboration Agent

Related topics:

Copying and extracting installation files to servers on page 427
Dropping database replication on page 429
Stopping and undeploying all network element instances on both the primary and redundant servers in each remote location on page 430
Stopping and undeploying all network element instances except the database on the redundant servers in the main location on page 431
Stopping and undeploying all network element instances except the Element Manager and database instances on the primary servers in the main location on page 431
Stopping the primary network element instance of Element Manager on page 432
Moving the Web Conferencing Management Server (WCMS) to the enterprise on page 433
Patching the Avaya Aura Conferencing Platform on the primary servers in the main location on page 437
Upgrading the database software on the primary database server on page 437
Upgrading the Avaya Aura Conferencing Element Manager and primary database on page 438
Upgrading the remaining network element instances on the primary servers in the main location on page 439
Verifying system operation in the main location on page 439
Upgrading the primary servers in each remote location and verifying operation on page 440
Upgrading the redundant network element instances except the database in the main site on page 441
Upgrading the redundant servers and network element instances in each remote location on page 441
Upgrading the database software on the secondary database server on page 442
Setting up database replication on page 443

Copying and extracting installation files to servers

Before you begin

Make sure you have the latest version of the following Avaya Aura® Conferencing software:

- Avaya Aura® Conferencing Server Platform
- Avaya Aura® Conferencing Application Bundle
- Avaya Aura® Conferencing Platform Patch

You can download iso images of this software from PDLS and burn the iso images to DVD-ROM.

About this task

Use this procedure to copy the Avaya Aura® Conferencing.

Procedure

1. Copy the Avaya Aura® Conferencing Platform Patch iso image to the primary Element Manager server, and then copy the Avaya Aura® Conferencing Platform Patch iso image to the all other servers that you want to patch.
   a. Log on to the primary Element Manager server as a user with the SA role (for example, `ntappadm`) through ssh or directly at the server console.
   b. Copy the Avaya Aura® Conferencing Platform Patch to `/var/mcp/media/` on the server or insert the Avaya Aura® Conferencing Platform Patch DVD-ROM .
   c. Log on to the primary Element Manager server as `ntsysadm`) through ssh or directly at the server console.
   d. At the command prompt, enter `su -` and press **Enter**.
   e. Type the root password, and press **Enter**.
   f. Copy the Avaya Aura® Conferencing Platform Patch to `/var/mcp/os/install/` on the server or insert the Avaya Aura® Conferencing Platform Patch DVD-ROM .

      If you are installing a feature pack or a service pack, copy the patch to the `/var/mcp/os/install/images` directory.
   g. Verify that the new Avaya Aura® Conferencing Platform Patch load (for example, `mcp_core_linux_ple2-17.0.1.patches.r-1.ext.iso)` is present in the directory `/var/mcp/os/install/`.

      If you are installing a feature pack or a service pack, check the `/var/mcp/os/install/images` directory.
   h. Copy the Avaya Aura® Conferencing Platform Patch iso file to the remaining servers that you want to patch over the network using the command `scp <load_name> <login>@<server_ip>:/var/mcp/loads/images` (for

example, `scp /var/mcp/os/install/mcp_core_linux_ple2-17.0.1.patches.r-1.ext.iso ntappadm@192.168.209.138:/var/mcp/media`).

Example for a feature pack or a service pack: `scp /var/mcp/os/install/images/mcp_core_linux_ple2-17.0.1.patches.r-1.ext.iso ntappadm@192.168.209.138:/var/mcp/media`

i. Log on to the server as a user with the SSA role (for example, `ntsysadm`) through ssh or directly at the server console.
j. At the prompt, type `su-` and press **Enter**.
k. Enter the root password and press **Enter**.
l. Move the Avaya Aura® Conferencing Platform Patch iso file to the directory `/var/mcp/os/install/` using the command `mv /var/mcp/media/<load_name> /var/mcp/os/install/` (for example, `mv /var/mcp/media/mcp_core_linux_ple2-17.0.1.patches.r-1.ext.iso /var/mcp/os/install/`).

   Example for a feature pack or a service pack: `mv /var/mcp/media/mcp_core_linux_ple2-17.0.1.patches.r-1.ext.iso /var/mcp/os/install/images`
m. Repeat Steps h through l for each server.

2. Copy the Avaya Aura® Conferencing Application Bundle iso file to the primary Element Manager server and extract the content. If you are using a DVD, insert the disk.

   a. Log on to the primary Element Manager server as a user with the AA role (for example, `ntappadm`) through ssh or directly at the server console.
   b. Copy the Avaya Aura® Conferencing Application Bundle iso file to `/var/mcp/extract`.
   c. Access the directory that contains the new database installer, type `mcpExtractContent -aat` and press **Enter** to extract the content.

3. If you are not using the Avaya Aura® Conferencing Application Bundle, copy the all components individually.

   a. Log on to the primary Element Manager server as a user with the SSA role (for example, `ntsysadm`) through ssh or directly at the server console.
   b. Copy the new database installer (for example, `installer-mcp-postgresql-9.0.6-14.AAC.LINUX64.zip)` to `/var/mcp/media` on the server .
   c. Verify that the new database installer is present in the directory `/var/mcp/media`.
   d. Copy the new Avaya Aura® Conferencing Application software load (for example, `MCP_17.0.14.0_2013-08-19-1307.zip)` to `/var/mcp/loads` on the server.

e. Verify that the new Avaya Aura® Conferencing Application software load is present in the directory `/var/mcp/loads`.

4. Clear the alarms using Element Manager Console.
   a. Log on to Element Manager Console.
   b. Right-click the Alarm Summary bar in the Element Manager Console window, and select **Logical View**.
      The Logical View window appears.
   c. Wait for the `Load Available` alarm to appear for the Element Manager.
   d. In the Logical View window, double-click on the **Element Manager** folder.
   e. Select **ElementManager_0** and click **Alarm Browser**.
      The Alarm Browser--Element Manager_0 window appears and displays a `LOADS 801 Load(s) Available` alarm.
   f. In the Alarm Browser--Element Manager_0 window, select the `LOADS 801 Load(s) Available` alarm, and click **Clear**.
5. Copy the Avaya Media Server load to each server where an Avaya Media Server is deployed.
   a. Log on to the first server as a user with the AA role (for example, `ntappadm`) through ssh or directly at the server console.
   b. Copy the Avaya Media Server load zip file (for example, `MCP_MediaServer_7.5.0.329_2013.17.77.zip)` to `/var/mcp/loads` on the server. (The Avaya Media Server load zip file was extracted from the Avaya Aura® Conferencing Application Bundle in Step 2.)
   c. Verify that the new Avaya Media Server load zip file is present in the directory `/var/mcp/loads`.
   d. Copy the Avaya Media Server load zip file over the network to the remaining servers where Avaya Media Server are deployed using the command `scp <load_name> <login>@<server_ip>:/var/mcp/loads/` (for example, `scp /var/mcp/loads/ MCP_MediaServer_7.5.0.329_2012.17_77.zip ntsysadm@192.168.209.138:/var/mcp/loads/`).

Result

All required installation files are present on the servers, and the system is ready to be upgraded.

Dropping database replication

About this task

Use the following procedure to drop database replication.

Procedure

1. In Element Management Console, verify there are no replication transactions in the database monitor.
2. Log on to the server hosting EM instance 0 as `ntdbadm` or an account with the DBA role.
3. Type `cd /var/mcp/run/MCP_15.0/mcpdb_0/bin/util` and press **Enter**.

   If you are installing a feature pack or a service pack, type `cd /var/mcp/run/MCP_17.0/mcpdb_0/bin/util` and press **Enter**.
4. Type `./cleanupReplication.pl` and press **Enter**.
   The system displays the following information:

```
You are about to drop replication between the 2 Databases. This will put
both
Databases into a "single mode", and changes will not be replicated between
them.
Please Confirm (Y/N): [N]
```

5. Type `y`, and press **Enter**.
   The system displays the following information:

```
Cleaning up PRIMARY DB replication
Cleaning up replication on PRIMARY completed successfully.
Cleaning up SECONDARY DB replication
Cleaning up replication on SECONDARDY database completed successfully..

cleanupReplication.pl Completed at
```

Note:

If this information is not displayed, stop and contact Avaya support.

Stopping and undeploying all network element instances on both the primary and redundant servers in each remote location

About this task

Use this procedure to stop and undeploy all network element instances deployed on the primary server and redundant servers in each remote location.

Procedure

1. For the remote location, stop all network element instances *except Avaya Media Server network element instances* deployed on all servers . See Stopping a non-Avaya Media Server network element instance on page 443.

2. Lock and stop all Avaya Media Server network element instances on all servers for the remote location. See Locking and stopping an Avaya Media Server instance on page 445.
3. Undeploy all network element instances *except the database network element instance* on all servers for the remote location. See Undeploying a network element instance on page 444.
4. Repeat Steps 1 through 3 for every remote location.

Stopping and undeploying all network element instances except the database on the redundant servers in the main location

About this task

Use this procedure to stop and undeploy all network element instances *except the Avaya Media Server instances and database network element instances* deployed on the redundant servers in the main location.

Procedure

1. For the main location, stop all network element instances *except Avaya Media Server network element instances and database network element instances* deployed on all servers . See Stopping a non-Avaya Media Server network element instance on page 443.
2. Lock and stop all Avaya Media Server network element instances on the redundant servers for the main location. See Locking and stopping an Avaya Media Server instance on page 445.
3. Undeploy all network element instances *except the database network element instance* on the redundant servers for the main location. See Undeploying a network element instance on page 444.

Stopping and undeploying all network element instances except the Element Manager and database instances on the primary servers in the main location

About this task

Use this procedure to stop and undeploy all network element instances *except the Element Manager instances and database network element instances* deployed on the primary servers in the main location.

Procedure

1. In the main location, stop all network element instances *except Avaya Media Server network element instances, Element Manager instances, and database network element instances* deployed on the primary servers . See Stopping a non-Avaya Media Server network element instance on page 443.
2. Lock and stop all Avaya Media Server network element instances deployed on the primary servers for the main location. See Locking and stopping an Avaya Media Server instance on page 445.
3. Undeploy all network element instances *except the Element Manager instances and database network element instances* on the primary servers in the main location. See Undeploying a network element instance on page 444.

Stopping the primary network element instance of Element Manager

About this task

Use this procedure to stop the primary network element instance of Element Manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements**> **Element Manager** > **Element Manager** > **NE Maintenance**.
2. In the NE Maintenance window, select the row for the primary instance of Element Manager (EM_0).
3. Click **Stop**.
   The Confirmation dialog box appears, prompting you to confirm that you want to stop the active Element Manager.
4. In the Confirmation dialog box, click **OK**.
5. Close the Maintenance window.

Result

The network element instance is stopped.

Moving the Web Conferencing Management Server (WCMS) to the enterprise

Note:

This procedure only applies if you have a standalone deployment that uses a Demilitarized Zone (DMZ). It applies to deployments that have redundancy and also to deployments that do not have redundancy (simplex layouts).

For the Avaya Aura® Conferencing 7.0 release, the WCMS resided on a separate server in the DMZ. For the Avaya Aura® Conferencing 7.2+ release, Avaya has moved the WCMS from the separate server in the DMZ to the Element Manager (EM) server in the enterprise. So, if you have a standalone deployment with a DMZ and are upgrading from Avaya Aura® Conferencing 7.0 to Avaya Aura® Conferencing 7.2, you must perform this task. If you have a co-resident deployment that uses a DMZ, the WCMS is already on the EM server.

After you move the WCMS to the enterprise, you must update the synchronization between the two WCMS instances. For more information, see Updating the Web Conferencing Management Server resync on page 436.

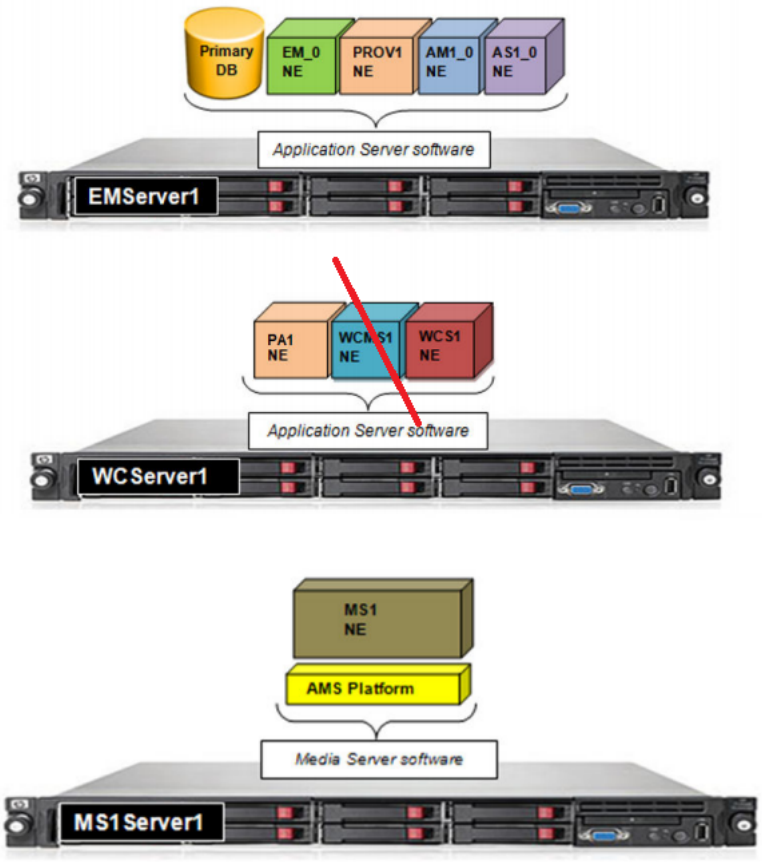


Figure 19: Avaya Aura® Conferencing 7.0 deployment layout

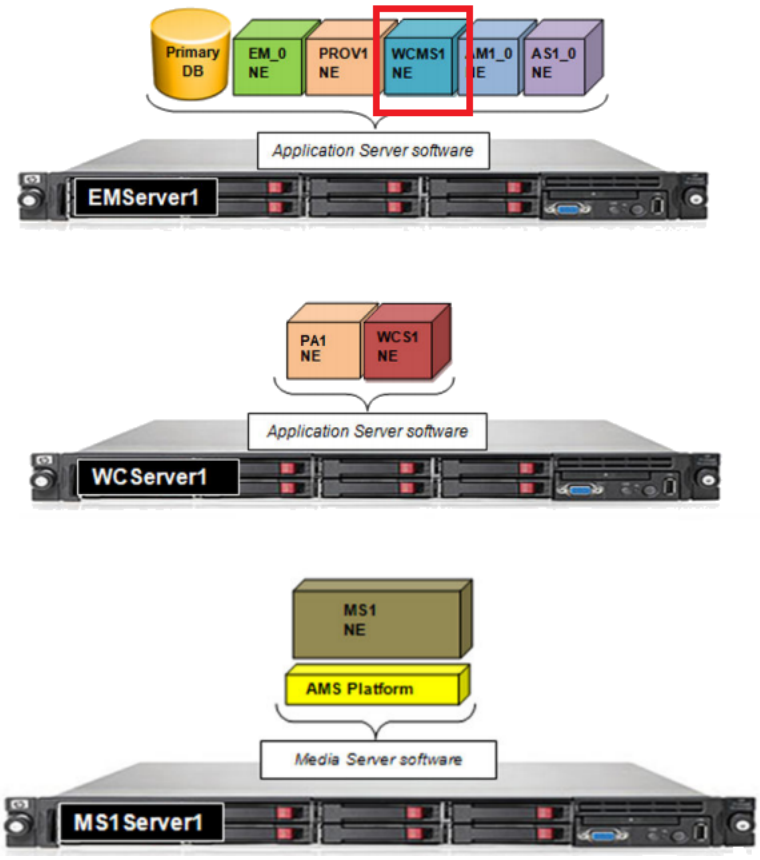


Figure 20: Avaya Aura® Conferencing 7.2 deployment layout

About this task

Use this task to move the WCMS from a separate server in the DMZ to the EM server in the enterprise.

Procedure

1. Stop all running WCMS, Web Conferencing Server (WCS), Personal Agent (PA), and Provisioning Agent (PROV) network element instances.

   See Stopping a Network Element instance on page 472.

2. Undeploy all WCMS network element (NE) instances.

   See Stopping and undeploying a network element instance on page 534.

3. Change the servers for WCMS network element instances to EM servers.

   For example, in the case of a standalone simplex layout, the new value will be `EMServer1`.

   a. In the EM graphic user interface (GUI), navigate to **Feature Server Elements** > **Web Conferencing Management Servers** > **<WCMS NE>** > **Instance**.
   b. Select the WCMS NE instance.
   c. Click **+/- (Edit)**.

d. On the resulting dialog, select the EM server and click **Apply**.

4. Deploy all WCMS NE instances.
   See Deploying a Network Element instance on page 493.
5. Change the certificate required for the WCMS in accordance with the guidances for certificate configuration.
   See Automated security.
6. Change the meeting event processor to Provisioning Manager.
   See Configuring the meeting event processor for the Web conferencing management server on page 182.
7. Ensure that TCP port 8444 is open between the DMZ and the enterprise to allow connectivity between the Collaboration Agent and the WCMS.
   For more information, see the *Avaya Aura® Conferencing Port Matrix Guide*, which is available on http://support.avaya.com/.
8. Start all stopped WCMS, WCS, PA, and PROV network element instances.
   See Starting a Network Element instance on page 476.

Related topics:

Enterprise DMZ deployment on page 62
Migrating to and from a DMZ on page 186
Updating the Web Conferencing Management Server (WCMS) Rsync configuration on page 436

Updating the Web Conferencing Management Server (WCMS) Rsync configuration

About this task

Use this task to update Web Conferencing Management Server (WCMS) rsync configuration.

Procedure

1. Log on to the secondary Element Manager server as a user with the SSA role (for example, ntsysadm) through ssh or directly at the server console.
2. At the prompt, type `su -` and press **Enter**.
3. Type the root password, and then press **Enter** to become the root user.
4. At the prompt, type `su - rsyncappsw` and press **Enter**.
5. At the prompt, type `ssh-keygen -R XXX.XXX.XXX.XXX`, where `XXX.XXX.XXX.XXX` is IP address of the secondary Element Manager server, and press **Enter**.

6. At the prompt, type `ssh-keyscan -t rsa XXX.XXX.XXX.XXX >> /home/rsyncappsw/.ssh/known_hosts`, where `XXX.XXX.XXX.XXX` is IP address of the secondary Element Manager server, and press **Enter**.

Result

Web Conferencing Management Server rsync configuration is updated.

Patching the Avaya Aura Conferencing Platform on the primary servers in the main location

About this task

Use this procedure to apply the Avaya Aura Conferencing Platform patches (operating system) to each primary server in the main location.

Procedure

Install the Avaya Aura Conferencing patches on each primary server in the main location. See Patching the Avaya Aura Conferencing Platform on page 446.

Upgrading the database software on the primary database server

About this task

Use this procedure to upgrade the database software on the primary database server.

Procedure

1. Log on to the primary Element Manager server (that is, the server hosting EM instance 0) as a user with the SA role (for example, `ntappadm`) through ssh or directly at the server console.
2. At the prompt, type `cd /var/mcp/install` and press **Enter**.
3. At the prompt, type `./mcpDbSwUpgrade.pl –primary` and press **Enter**.
   A communications test to the target database server is performed, and a configuration summary is presented. You are prompted to select the target database patch zip file.

Note:

If you receive an error or you are not prompted to select the target database patch zip file, stop and contact Avaya support.

4. Type the number of the patch zip file you want to use and press **Enter**.
   The following message appears:

   ```
   Continue with Database Software UPGRADE? (Y/N) [N]:
   ```

5. Type `y` and press **Enter**.
   The following message appears and the patching process starts for the database:

   ```
   UPGRADE, for Database Software on <ip_address> ...

   Upgrading Database Software...please be patient
   ```

   Depending on the server hardware and the target server receiving the installation, the installation process could take up to 15 minutes.

   Once the installation is complete, the following message appears:

   ```
   mcpDbSwUpgrade Completed Successfully.
   ```

   Note:

   If the message does not appear, stop and contact Avaya support.

Result

The database upgrade is complete.

Upgrading the Avaya Aura Conferencing Element Manager and primary database

About this task

Use this procedure to upgrade the Avaya Aura® Conferencing Element Manager and primary database.

Procedure

1. Log on to the server hosting EM instance 0 as a user with the AA role (for example, `ntappadm`) through ssh or directly at the server console.
2. At the prompt, type `cd /var/mcp/install`and press **Enter**.
3. At the prompt, type `./mcpUpgradeNextRel.pl` and press **Enter**.
   The list of available loads appears. Avaya Aura® Conferencing 7.2 loads have the filename `MCP_17.x.x.xx_2013-xx-xx-xxxx.zip`.
4. Type the number of the load you want to use, and press **Enter**.
   The following message appears and the upgrade starts for the MCP database and Element Manager:

```
--- Invoking mcpUpgrade => to upgrade the EM & Database ---
```

Note:

If the upgrade message does not appear, stop and contact Avaya support.

Once the upgrade of the MCP database and Element Manager is complete, the following message appears:

```
--- EM & DataBase Upgrade Complete ---
```

Note:

If an error occurs (for example, due to loss of network connectivity), retry the `mcpUpgradeNextRel.pl` command after you resolve the problem. If an error occurs again, stop and contact Avaya support.

Result

The MCP database and Element Manager are upgraded to Release 7.2.

Upgrading the remaining network element instances on the primary servers in the main location

About this task

Use this procedure to upgrade the remaining network element instances on the primary servers in the main location.

Procedure

1. Upgrade the Avaya Media Servers software on each primary server in the main location that hosts an Avaya Media Server. See Upgrading an Avaya Media Server on page 448.
2. Upgrade all network element instances deployed on the primary servers in the main location. See Upgrading a network element instance on page 447.
3. Upgrade the Document Conversion Server (if present) in the main location. See Upgrading a Document Conversion Server on page 449.

Verifying system operation in the main location

About this task

Use this procedure to verify the system is operating properly for users in the main location.

Procedure

1. Verify the system is operating properly in the main location.
2. If the system is not operating properly, contact your next level of support. You may need to perform a rollback.

Note:

Contact your next level of support before performing a rollback. If a roll back is required, you will have to roll back the primary servers at the main location only.

Upgrading the primary servers in each remote location and verifying operation

About this task

Use this procedure to upgrade the primary servers in each remote location and verify system operation for the remote location.

Procedure

1. Install the Avaya Aura Conferencing Platform patch for each primary server in the remote location. See Patching the Avaya Aura Conferencing Platform on page 446.
2. Upgrade the primary Avaya Media Server software in each media server cluster in the remote location. See Upgrading an Avaya Media Server on page 448.
3. Upgrade all the network element instances deployed on each primary server in the remote location. See Upgrading a network element instance on page 447.
4. Upgrade the Document Conversion Server (if present) in the remote location. See Upgrading a Document Conversion Server on page 449.
5. Verify that the system is operating properly for users in the remote location. See Verifying system operation for a location after an upgrade on page 451.
6. Repeat Steps 1 through 5 for each remote location.

Upgrading the redundant network element instances except the database in the main site

About this task

Use this procedure to upgrade the redundant network element instances *except the database instance* in the main location.

Procedure

1. Install the Avaya Aura Conferencing Patch on each redundant server in the remote location. See Patching the Avaya Aura Conferencing Platform on page 446.
2. Upgrade redundant Avaya Media Servers in the main location. See Upgrading an Avaya Media Server on page 448.
3. Upgrade all the network element instances deployed on redundant servers in the main location. See Upgrading a network element instance on page 447.

Upgrading the redundant servers and network element instances in each remote location

About this task

Use this procedure to upgrade the redundant servers and network element instances in each remote location.

Procedure

1. Install the Avaya Aura Conferencing Patch on each redundant server in the remote location. See Patching the Avaya Aura Conferencing Platform on page 446.
2. Upgrade redundant Avaya Media Servers in the remote location. See Upgrading an Avaya Media Server on page 448.
3. Upgrade all the network element instances deployed on redundant servers in the remote location. See Upgrading a network element instance on page 447.
4. Repeat Steps 1 through 4 for each remote location.

Upgrading the database software on the secondary database server

About this task

Use this procedure to upgrade the database software on the secondary database server.

Procedure

1. Log on to the primary Element Manager server (that is, the server hosting EM instance 0) as a user with the SA role (for example, `ntappadm`) through ssh or directly at the server console.
2. At the prompt, type `cd /var/mcp/install` and press **Enter**.
3. At the prompt, type `./mcpDbSwUpgrade.pl –secondary` and press **Enter**.
   A communications test to the target database server is performed, and a configuration summary is presented. You are prompted to select the target database patch zip file.

   Note:

   If you receive an error or you are not prompted to select the target database patch zip file, stop and contact Avaya support.
4. Type the number of the patch zip file you want to use and press **Enter**.
   The following message appears:

   ```
   Continue with Database Software UPGRADE? (Y/N) [N]:
   ```
5. Type `y` and press **Enter**.
   The following message appears and the patching process starts for the database:

   ```
   UPGRADE, for Database Software on <ip_address> ...

   Upgrading Database Software...please be patient
   ```

   Depending on the server hardware and the target server receiving the installation, the installation process could take up to 15 minutes.

   Once the installation is complete, the following message appears:

   ```
   mcpDbSwUpgrade Completed Successfully.
   ```

   Note:

   If the message does not appear, stop and contact Avaya support.

Result

The database upgrade is complete.

Setting up database replication

About this task

Use the following procedure to set up database replication.

Procedure

1. Log on to the server hosting EM instance 0 as `ntappadm` or an account with the AA role.
2. Type `cd /var/mcp/install` and press **Enter**.
3. Type `./setupDBReplication.pl` and press **Enter**.
   The system displays the following information:

```
Deploying files to xxx.xxx.xxx.xxx...
Deploying files to the Secondary DB
Deploying files to xxx.xxx.xxx.xxx...
DB Operation Completed.

Resync from primary DB to secondary DB. This will take a while, please be
patient and wait ...
setupDBReplication.pl completed successfully
```

Note:

If this information is not displayed, stop and contact Avaya support.

4. In Element Manager Console, verify that the alarms `No connection to DB instance` clear within a couple of minutes.

Common administration procedures

Stopping a non-Avaya Media Server network element instance

About this task

Use this procedure to stop a non-Avaya Media Server network element instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements**> ***<network element type>*** > ***<network element instance you want to stop>*** > **NE Maintenance**.
2. In the Maintenance window, select the row that has a value of the target instance in the ID column.
3. Click **Stop**.
   The Maint state changes from “None” to “Stopping,” indicating that the stop operation is in progress. When the stop operation is complete, the following state changes occur:
   - The Maint state changes back to “None.”
   - The Admin state changes from “Online” to “Offline.”
4. Close the Maintenance window.

Result

The network element instance is stopped.

Undeploying a network element instance

About this task

Use this procedure to undeploy a network element instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements**> ***<network element type>*** > ***<network element instance you want to stop>*** > **NE Maintenance**.
2. In the Maintenance window, select the row that has a value of the target instance in the ID column.
3. Click **Undeploy**.
   The Maint state changes from “None” to “Undeploying,” indicating that the undeploy operation is in progress. When the undeploy operation is complete, the Maint state changes back to “None.”
4. Close the Maintenance window.

Result

The network element instance is undeployed.

Locking and stopping an Avaya Media Server instance

About this task

Use this procedure to stop an Avaya Media Server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server network element instance you want to stop*> > Service Maintenance**.
2. In the Media Server Service Maintenance window, select the Avaya Media Server instance.
3. Click **Pending Lock**.
   All new requests will be redirected to other Avaya Media Servers in the cluster. All existing sessions are allowed to continue, but new sessions are not allowed.
4. In the navigation pane of Element Manager Console, select **Key Performance Indicators > Monitoring and Reporting > Sessions**.
5. Watch the number of sessions on the Avaya Media Server, and wait for the number of sessions to become 0 or an acceptable small number.
6. When the number of sessions becomes 0 or an acceptable small number, select the Avaya Media Server instance in the Media Server Service Maintenance window and click **Lock**.
   Existing sessions are terminated, and no additional sessions are allowed into the Avaya Media Server, even after the Avaya Media Server restarts.
7. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers** > **<*Media Server network element instance*>** > **NE Maintenance**.
8. In the Media Server NE Maintenance window, select the row that has a value of the target instance in the ID column.
9. Click **Stop**.
   The Maint state changes from “None” to “Stopping,” indicating that the stop operation is in progress. When the stop operation is complete, the following state changes occur:
   - The Maint state changes back to “None.”
   - The Admin state changes from “Online” to “Offline.”
10. Close the Media Server NE Maintenance window.

Result

The Avaya Media Server is stopped. Calls are handled by another Avaya Media Server in the cluster.

Patching the Avaya Aura Conferencing Platform

About this task

Use this procedure to apply server platform patches to the target server.

Procedure

1. Log on to the server as a user with the SSA role (for example, `ntsysadm`) through ssh or directly at the server console.
2. At the prompt, type `su -` and press **Enter** to log on as root.
3. Type the root password, and press **Enter**.
4. Perform one of the following steps:
   - If you want to patch the primary server for the main site, type `cd /var/mcp/os/install/` and press **Enter**.
   - If you want to patch a server for a remote site, type `cd /var/mcp/os/media/` and press **Enter**.
   - If you want to install a feature pack or a service pack, type `cd /var/mcp/os/install/images` and press **Enter**
5. At the prompt, type `patchPlatform.pl <file>.iso -np` where <file>.iso is the patch ISO file.
6. Press **Enter**.
   The patchPlatform.pl tool compares the patches contained in the patch ISO file against the current release of the system.

   If there are no required patches, the following message appears, the tool exits, and the patching procedure is complete:

   ```
   No applicable patche(es).

   Number of patches applied: 0
   ```

   If one or more patches are required, those patches are displayed and then automatically applied to the system. Once the last patch has been applied, the server reboots automatically.
7. After the server reboots, log on to the server using any account.
8. At the prompt, type `mcpRelease.pl` and press **Enter**.

The system displays the release level. The following is an example of the release level information displayed:

```
*** MCP Platform Release ***

System Type: mcp_core_linux_ple2

Release Level: 17.0.1 (via patching)

Hardware Env: Other
```

9. Verify that the release level displayed matches the patch you installed.

   Note:

   If the release level displayed does not match the patch you installed, contact Avaya support.

10. Repeat Steps 1 through 9 for each server.

Result

The server platform patch is complete.

Upgrading a network element instance

About this task

Use this procedure to upgrade a network element instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements**> ***<network element type>*** > ***<network element instance you want to upgrade>*** > **Instance**.
2. In the Instance window, select the row that has a value of the target instance in the ID column.
3. Click **Edit**.
4. From the Load or Patch box in the Edit Instance dialog box, select the target value, and click **Apply**.
5. In the navigation pane of Element Manager Console, select **Feature Server Elements**> ***<network element type>*** > ***<network element instance you want to upgrade>*** > **NE Maintenance**.
6. In the NE Maintenance window, select the row that has a value of the target instance in the ID column.
7. Click **Deploy**.

The Maint state changes from “None” to “Deploying,” indicating that the deploy operation is in progress. When the deploy operation is complete, the following state changes occur:

- The Maint state changes back to “None.”
- The Admin state is “Offline.”
- The link status is “Down.”
- The Oper state is “Unavailable.”

8. Click **Start**.
   The Maint state changes from “None” to “Starting,” indicating that the start operation is in progress. When the start operation is complete, the following state changes occur:
   - The Maint state changes back to “None.”
   - The Admin state is “Online.”
   - The link status is “Up.”
   - The Oper state is “Active.”
9. If you upgraded an Avaya Media Server network element, you must unlock the service state before the media server will accept traffic. Perform the following steps:
   a. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server network element instance you want to unlock*> > Service Maintenance**.
   b. In the Media Server Service Maintenance window, select the Avaya Media Server instance.
   c. Click **Unlock**.
10. Close the NE Maintenance window.

Result

The network element instance is upgraded.

Upgrading an Avaya Media Server

Before you begin

Obtain the Application Bundle DVD-ROM.

About this task

Use this procedure to upgrade the Avaya Media Server software.

Note:

You must upgrade all the Avaya Media Servers in your deployment.

Procedure

1. Log on to the first Avaya Media Server as a user with the SSA role (for example, `ntsysadm`) through ssh or directly at the server console.
2. At the prompt, type `su -` and press **Enter**.
3. Type the root password, and then press **Enter** to become the root user.
4. At the prompt, type `mcpMsInstall.pl` and press **Enter**.
   The install script finds the zipped file. The system will detect more than one zipped file.
5. At the prompt `Please enter number [1 or 2] of selection`, type the number that corresponds to the zipped file containing the upgrade.
   The selected file is unzipped
6. At the prompt `Continue installation? (Y/N)`, type `y` and press **Enter**.
   Information about the load appears on the screen.
7. Type `Y` to confirm you have read the information, and press **Enter**.
   The installer detects a previous version already installed.
8. At the prompt `Proceed with upgrade? (Y/N)`, type `y`, and press **Enter**.
   When the upgrade is complete, the message `Installation completed SUCCESSFULLY` appears. The Avaya Media Server load is now upgraded.
9. Repeat Steps 1 through 8 for every Avaya Media Server in the deployment.

Upgrading a Document Conversion Server

Before you begin

Important:

The Document Conversion Server software is located in the `dcs` directory in the MCP load on the Application Server (for example, `/dcs/dcs_MCP_17.0.0.1_2013-08-16-2200.zip`).

If you copy the software to the Document Conversion Server using a method that differs from the recommended approach, perform the following steps:

1. Right-click the zip file, click **Properties**.
2. On the **General** tab, in the Security section, click **Unblock**.

3. Click **Apply**.
4. Click **OK**.

About this task

Use the following procedure to upgrade the Document Conversion Server.

Procedure

1. Stop the DCS process by closing the command window.
2. Insert the Application Bundle DVD-ROM on the Windows server.
3. Obtain the Document Conversion Server software (for example, `dcs_MCP_17.0.0.1-2013-09-2200.zip`) from the core directory `/dcs/dcs_<version><date-time>.zip`.
4. Copy the zip file to `c:\` and extract the files.

   Note:

   You are prompted to overwrite the existing dcs directory.
5. Remove the read-only attribute on the dcs directory and apply the changes to the sub-directories.
6. Using Windows Explorer, navigate to `c:\`, right-click on the **dcs** folder, and select **Properties**.
7. In the Properties dialog box, uncheck the **Read-only** check box, and then click **Apply**.
8. In the Properties dialog box, click **OK**.
9. Save the settings from the configuration file (`<installed directory>/dcs/htdocs/app/Config.php`).
10. Save the settings from the httpd configuration file (`<installed directory>/dcs/conf/httpd.conf`).
11. Save the certificates. For more information, see “Chapter 10: Installing and configuring the Document Conversion Server.”
12. Navigate to `c:\dcs`.
13. At the prompt, type `Setup DCS.bat` and press **Enter**.

Result

The Document Conversion Server has been upgraded to the target load, and the Document Conversion Server starts.

Verifying system operation for a location after an upgrade

About this task

Use this procedure to verify the system is operating properly for users in a location where the primary servers have been upgraded.

Procedure

Verify the following services are operating properly in the location:

- Web Conferencing
- Document Conversion
- Screen Sharing

If the system is not operating properly, contact your next level of support.

Note:

If the main location passed the verification tests, it is unlikely that a roll back is required.

Verifying system operation for a location

About this task

Use this procedure to verify the system is operating properly for users in a location where the primary servers have been upgraded.

Procedure

Verify the following services are operating properly in the location:

- Audio/Video Conferencing
- Web Conferencing
- Document Conversion
- Screen Sharing
- Recording

If the system is not operating properly, contact your next level of support.

Note:

If the main location passed the verification tests, it is unlikely that a roll back is required.

Upgrading memory for the HP DL360 G7 server

In a standalone deployment, perform this task on the Element Manager server. In the case of a standalone with redundancy deployment, perform this task on both Element Manager servers. This task adds memory to an existing AAC installation. Perform this task if your system has been experiencing any memory shortages.

Note:

This procedure does not apply to the co-resident model.

Before you begin

- You have backed up the AAC system.
- You have the AAC Memory Upgrade Kit.
- You have the HP DL360 document set. For more information, see Downloading HP documentation on page 105.

About this task

Use this procedure to replace the existing 2 GB DIMM RAM memory with new 4 GB DIMM RAM memory.

If using mixed sized DIMMs, insert the larger sized DIMMs in the primary DRAM channels, then move onto the smaller sizes in the correct sequential order. The primary DRAM channels are marked with white tabs.

Install RDIMMs in alphabetical order (slots A through I).

Procedure

1. Observe safety warnings.
2. Observe all ESD safety precautions.
3. Handle the DIMMs with care:
    - Hold DIMMs by the side edges only.
    - Avoid touching the connectors on the bottom of the DIMM.
    - Never wrap your fingers around a DIMM.
    - Avoid touching the components on the sides of the DIMM.

- Never bend or flex the DIMM.

4. Power off the HP DL360 G7 server.
5. Extend the server from the rack.
6. Remove the access panel.
   a. Open the latch
      If it is locked, use a T-15 Torx screwdriver to unlock the latch.
   b. Slide the access panel to the rear of the chassis.
   c. Remove the panel.
7. If installed, remove the BBWC battery pack from air baffle and set it aside.
   Keep the wires connected.
8. Remove the air baffle.

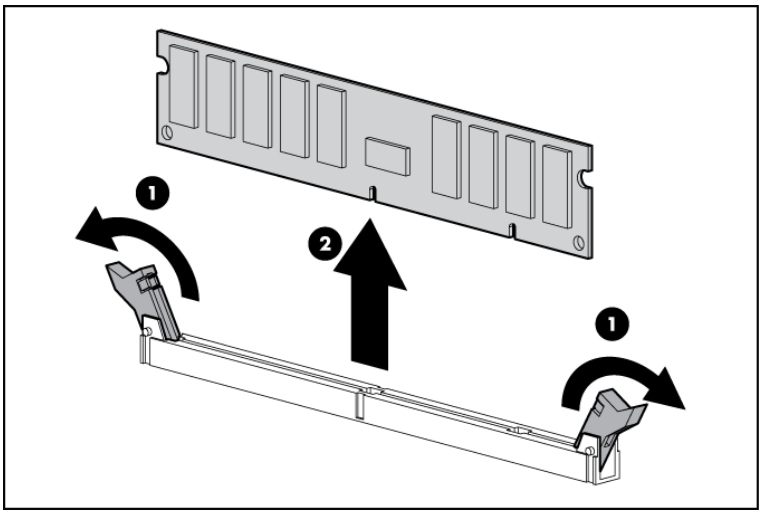


Figure 21: DIMM Removal

9. Open the DIMM slot latches.
10. Remove all existing 2 GB DIMM memory.
11. Install new 4 GB DIMM memory in the Primary DRAM channels, (white colored, slots A, B, C).
12. Reinstall the used 2 GB DIMM memory in the Secondary DRAM channels, (black colored, slots D-I).
13. Reinstall the Air Baffle.

Warning:

Be careful not to damage DIMMS or cables.

14. If removed, reinstall the BBWC battery pack.
15. Install the access panel.

16. Power up the HP DL360 G7 server.

Result

When you successfully install the memory, the server will automatically run a diagnostic on the new memory to test for failures.

Chapter 28: Installing feature packs

This section describes how to install a feature pack for Avaya Aura® Conferencing. A feature pack provides minor, new features to Release 7.2 and may consist of an AAC Platform patch and the Application Core Bundle.

Avaya Aura® Conferencing uses the following naming convention for software updates:

MCP_<major release number>.<feature pack number>.<service pack number>.<patch number>

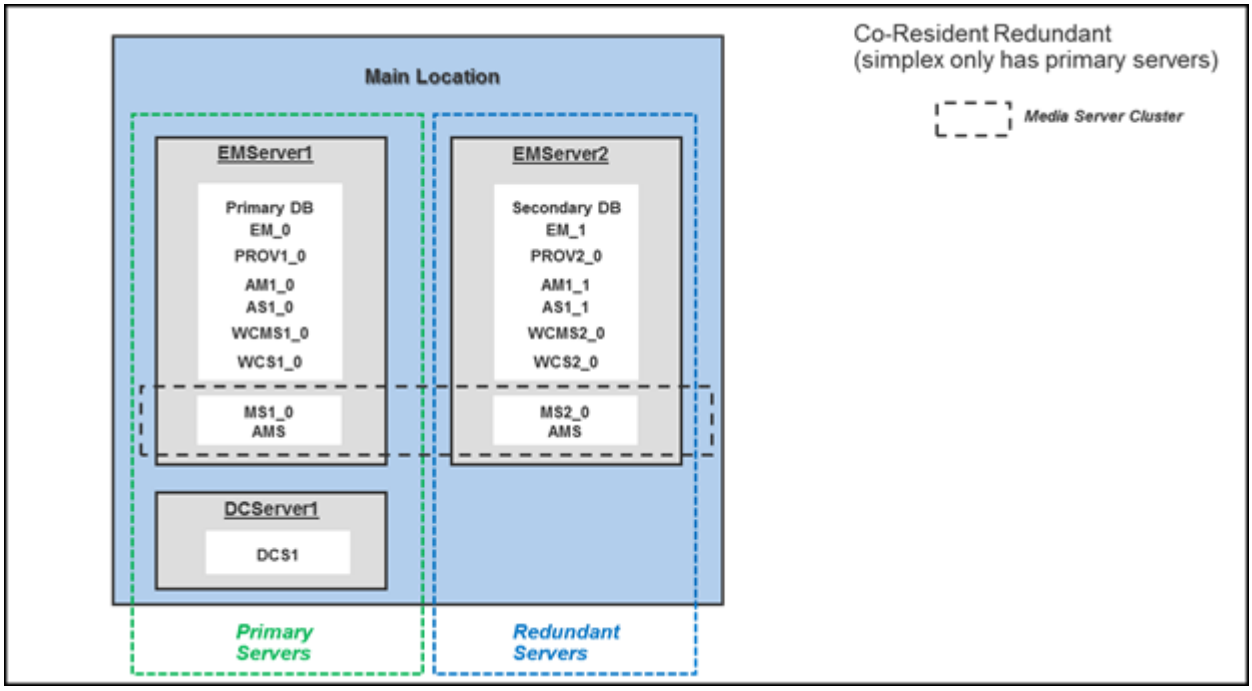
For example:

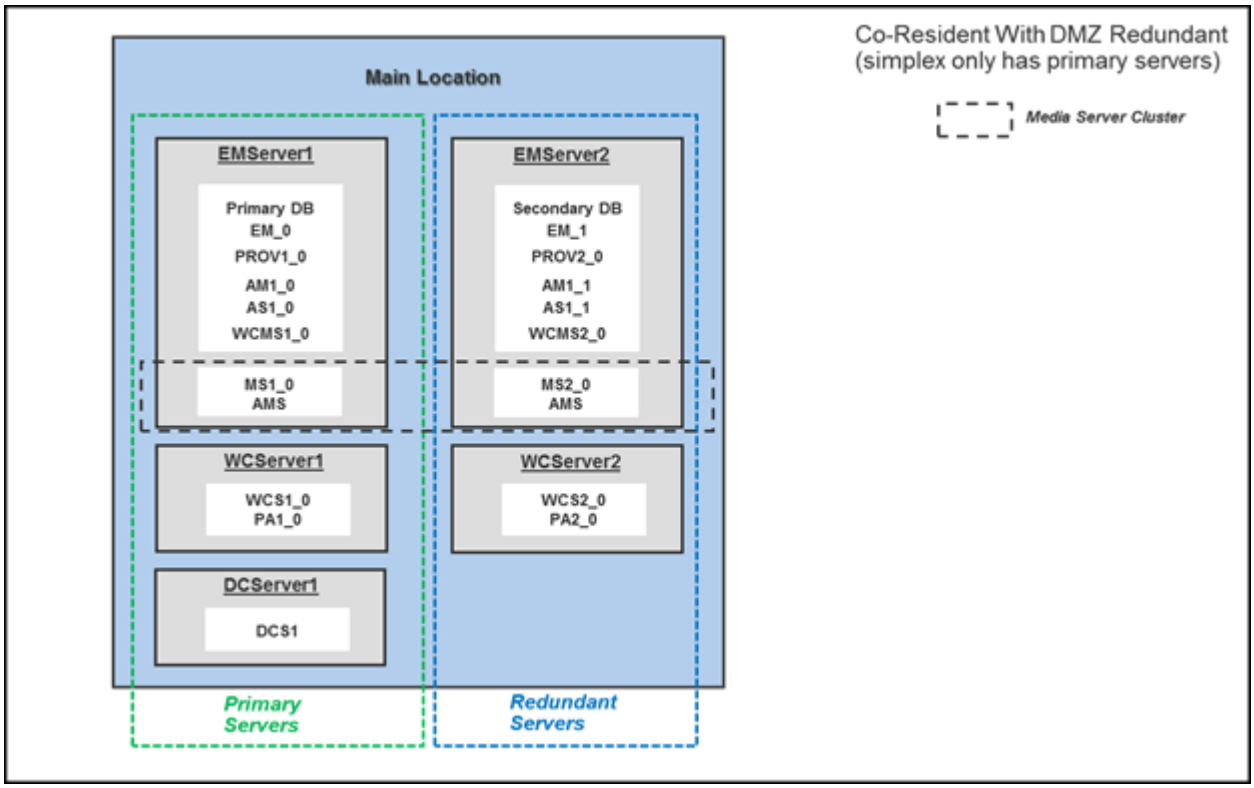
- Avaya Aura® Conferencing 7.2 is a major release, and it is delivered as MCP_**17**.0.0.0.
- The first feature pack for Avaya Aura® Conferencing 7.2 will be delivered as MCP_17.**1**.0.0.
- The first service pack that will be delivered after feature pack MCP_17.1.0.0 will be MCP_17.1.**1**.0.
- The first patch that will be delivered after service pack MCP_17.1.1.0 will be MCP_17.1.1.**1**.

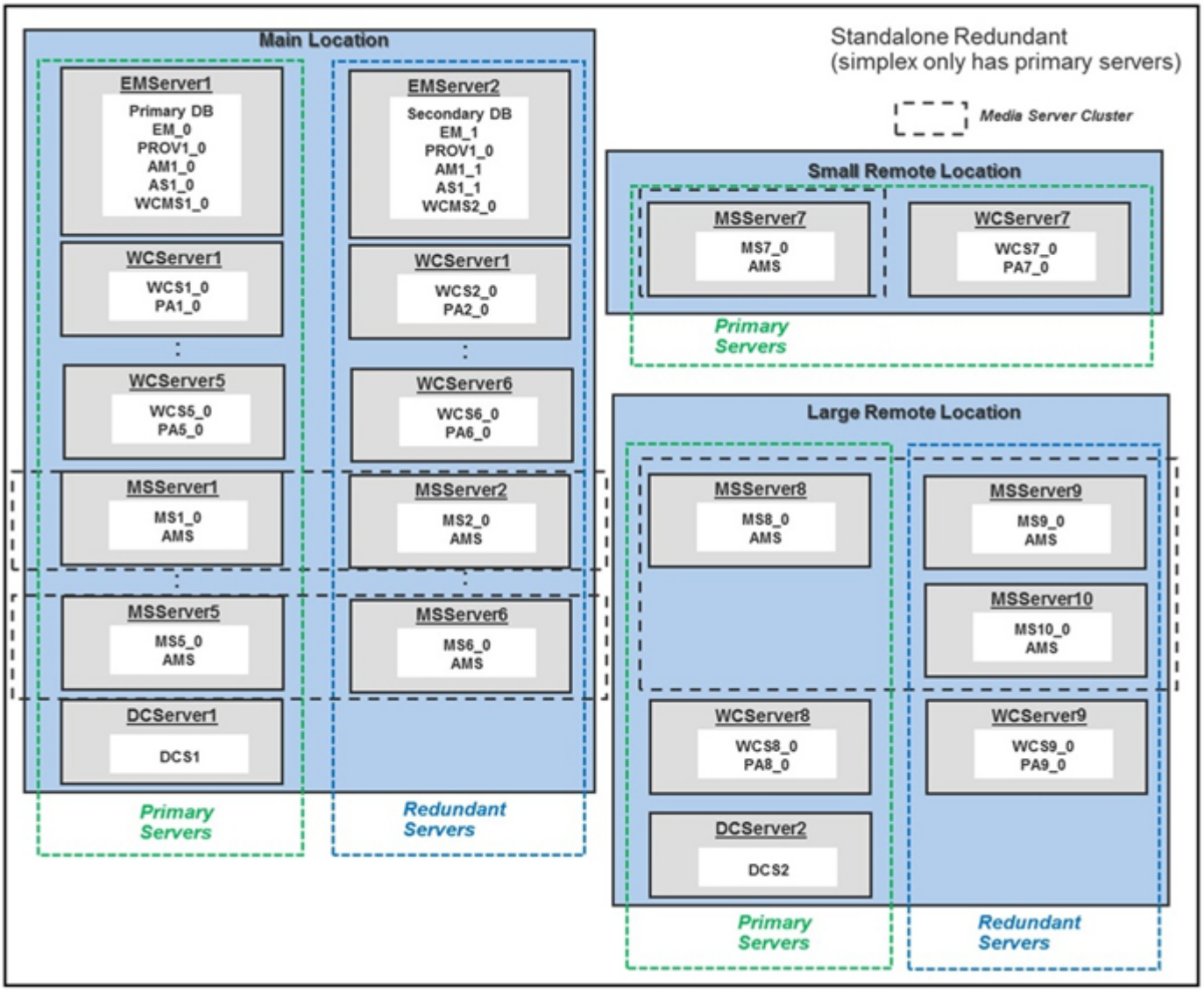
Note:

The software update numbering scheme does not match the official release number for Avaya Aura® Conferencing. Avaya Aura® Conferencing 7.2 is synonymous with MCP_**17**.x.0.0.

Before installing a feature pack, you must identify the primary servers and redundant servers in a redundant deployment. In a simplex deployment, there are no redundant servers. The following diagrams show the supported deployment configurations and identify the primary and redundant server.


Co-Resident Redundant
(simplex only has primary servers)
Media Server Cluster
Main Location
EMServer1
Primary DB
EM_0
PROV1_0
AM1_0
AS1_0
WCMS1_0
WCS1_0
MS1_0
AMS
EMServer2
Secondary DB
EM_1
PROV2_0
AM1_1
AS1_1
WCMS2_0
WCS2_0
MS2_0
AMS
DCServer1
DCS1
Primary Servers
Redundant Servers


Co-Resident With DMZ Redundant
(simplex only has primary servers)
Media Server Cluster
Main Location
EMServer1
Primary DB
EM_0
PROV1_0
AM1_0
AS1_0
WCMS1_0
MS1_0
AMS
EMServer2
Secondary DB
EM_1
PROV2_0
AM1_1
AS1_1
WCMS2_0
MS2_0
AMS
WCServer1
WCS1_0
PA1_0
WCServer2
WCS2_0
PA2_0
DCServer1
DCS1
Primary Servers
Redundant Servers



You can expand standalone configurations to have media servers in multiple remote locations. Note that the previous diagram does not depict all potential configurations. The media servers in the remote locations may be used to host local conferencing or may be configured to support cascading. Regardless, the media servers are always in clusters. Each cluster has at least a primary media server assigned to it. When determining the primary servers to upgrade in a remote location, examine the configuration for each media server cluster in that location and select the primary media server.

Feature pack installation procedure

The following table provides a high-level view of the tasks involved in installing a feature pack on Avaya Aura® Conferencing.

Note:

Installing a feature pack is an out-of-service procedure regardless of whether the system is in a simplex or redundant deployment configuration.

#	Task	Description	Notes	✔
1	Obtain the latest Avaya Aura® Conferencing 7.2 platform and application software files: • Avaya Aura® Conferencing Platform • Avaya Aura® Conferencing Platform Patches • Avaya Aura® Conferencing Application Bundle	Download the software files from PLDS.		
2	Store the currently installed Avaya Aura® Conferencing 7.2 platform and application software files in a secure location so you can perform a rollback in the unlikely event of a feature pack installation failure.			
3	Back up the: • Avaya Aura® Conferencing database • Avaya Media Servers • Avaya Aura® Conferencing server platforms	See Backing up on page 497.		
4	Copy and extract the Avaya Aura® Conferencing 7.2	See Copying and extracting installation files to servers on page 427.		

#	Task	Description	Notes	✔
	installation files to the servers.			
5	If you have a redundant system, drop database replication.	See Dropping database replication on page 429.		
6	If you have multiple sites, stop and undeploy all network element instances on both the primary server and the redundant server for each remote site.	See Stopping and undeploying all network element instances on both the primary and redundant servers in each remote location on page 430.		
7	If you have a redundant system, stop and undeploy all network element instances *except the database network element instance* on the redundant servers in the main site.	See Stopping and undeploying all network element instances except the database on the redundant servers in the main location on page 431.		
8	Stop and undeploy all network element instances *except the Element Manager network element and database network element* on the primary servers in the main site.	See Stopping and undeploying all network element instances except the Element Manager and database instances on the primary servers in the main location on page 431.		
9	Stop the primary instance of the Element Manager network element.	See Stopping the primary network element instance of Element Manager on page 432.		
10	Patch the Avaya Aura® Conferencing Platform (operating system) on the primary servers in the main site.	See Patching the Avaya Aura Conferencing Platform on the primary servers in the main location on page 437.		

#	Task	Description	Notes	✔
11	If you have not yet configured DNS, configure the DNS client.	See Configuring a DNS client on page 494.		
11	Upgrade the database software on the primary database server.	See Upgrading the database software on the primary database server on page 437.		
12	Upgrade the Avaya Aura® Conferencing Element Manager and primary database.	See Upgrading the Avaya Aura Conferencing Element Manager and primary database on page 438.		
13	Upgrade the remaining network element instances on the primary servers in the main site.	See Upgrading the remaining network element instances on the primary servers in the main location on page 439.		
14	Verify that the Avaya Aura® Conferencing system is operating correctly for users in the main site.	See Verifying system operation in the main location on page 439.		
15	If you have a multi-site configuration, upgrade the primary servers and verify the system is operating properly for users at each remote site.	See Upgrading the primary servers in each remote location and verifying operation on page 440.		
16	If you have a redundant system, upgrade the redundant network element instances *except the database network element instance* in the main site.	See Upgrading the redundant network element instances except the database in the main site on page 441.		
17	If you have a redundant system and a multi-site configuration, upgrade the redundant network	See Upgrading the redundant servers and network element instances in each		

#	Task	Description	Notes	✔
	element instances and Avaya Media Servers in each remote site.	remote location on page 441.		
18	If you have a redundant system, upgrade the database software on the secondary database server.	See Upgrading the database software on the secondary database server on page 442.		
19	If you have a redundant system, set up database replication.	See Setting up database replication on page 443.		

Chapter 29: Installing service packs and patches

This section describes how to install service packs and patches for Avaya Aura® Conferencing. A service pack is a collection of software fixes that is delivered at regular intervals (typically four weeks) between major releases (for example, Release 7.2)/features packs. A patch contains emergency fixes and is delivered as needed between major releases/feature packs/service packs. Both service packs and patches are delivered through the Avaya PLDS as individual files.

Note:

Installing a service pack or patch is an in-service procedure.

Avaya Aura® Conferencing uses the following naming convention for software updates:

MCP_<major release number>.<feature pack number>.<service pack number>.<patch number>

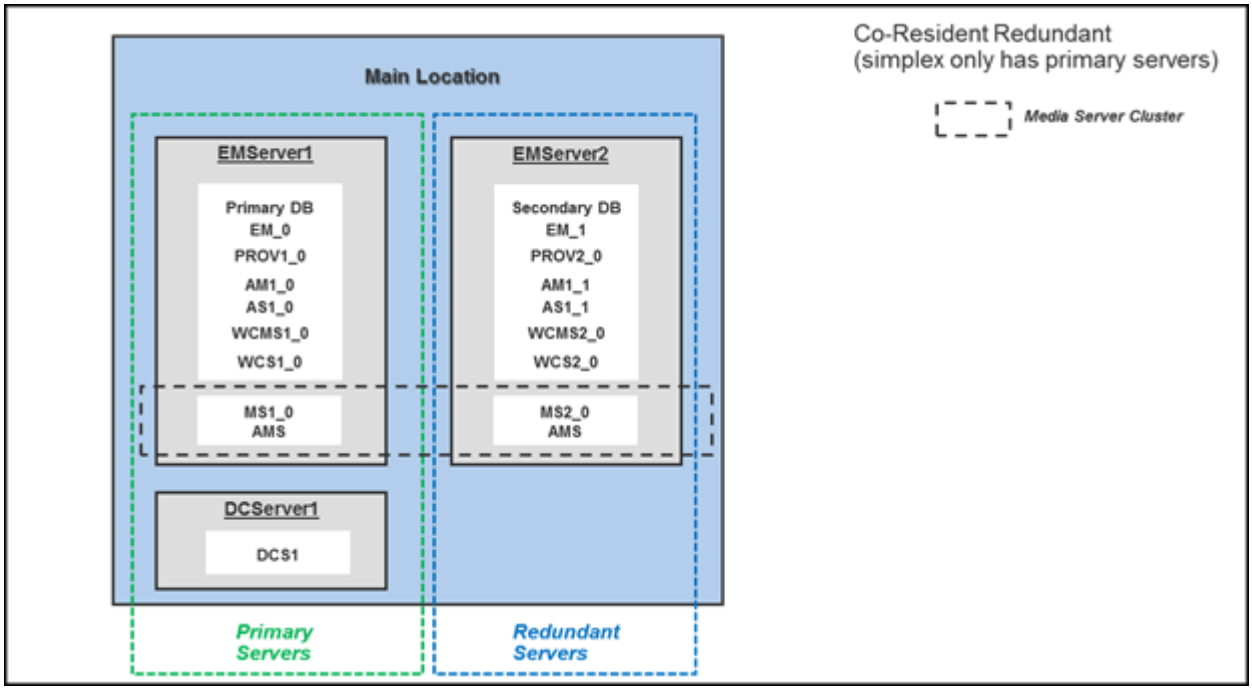
For example:

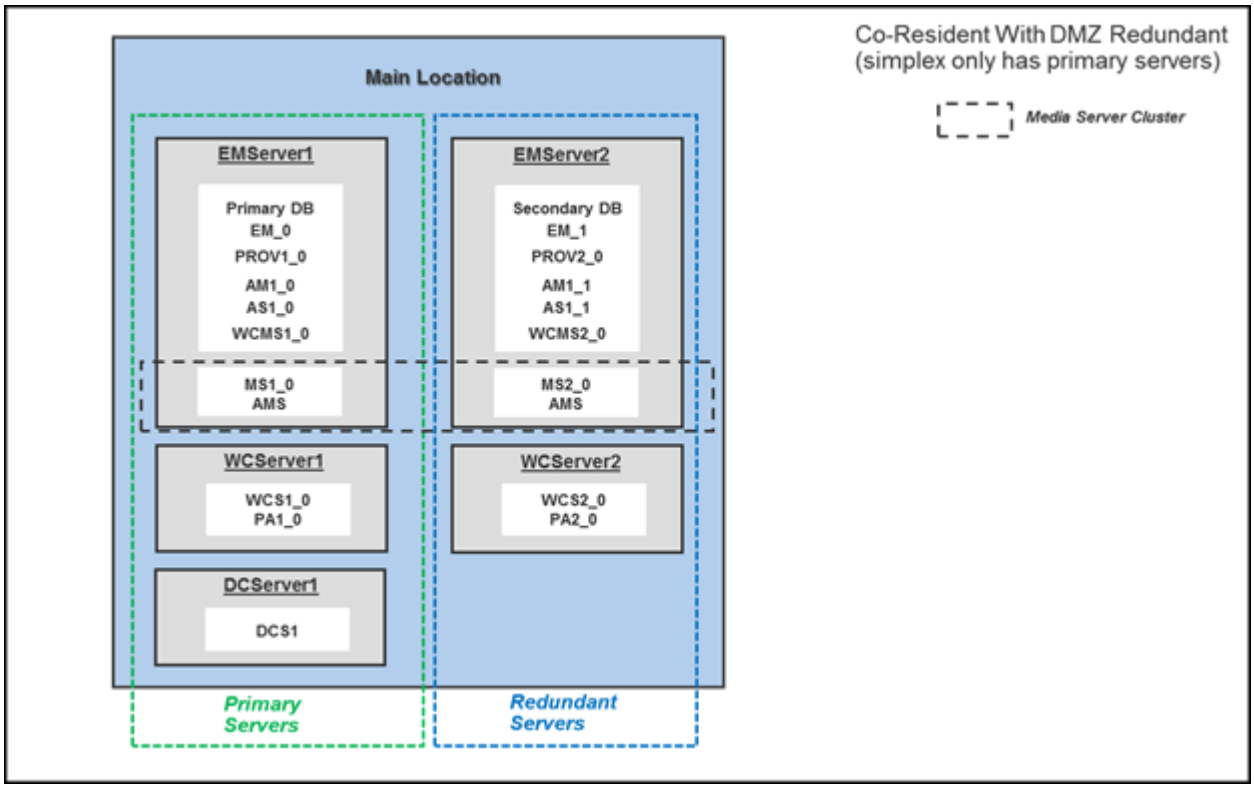
- Avaya Aura® Conferencing 7.2 is a major release, and it is delivered as MCP_**17**.0.0.0.
- The first feature pack for Avaya Aura® Conferencing 7.2 will be delivered as MCP_17.**1**.0.0.
- The first service pack that will be delivered after feature pack MCP_17.1.0.0 will be MCP_17.1.**1**.0.
- The first patch that will be delivered after service pack MCP_17.1.1.0 will be MCP_17.1.1.**1**.

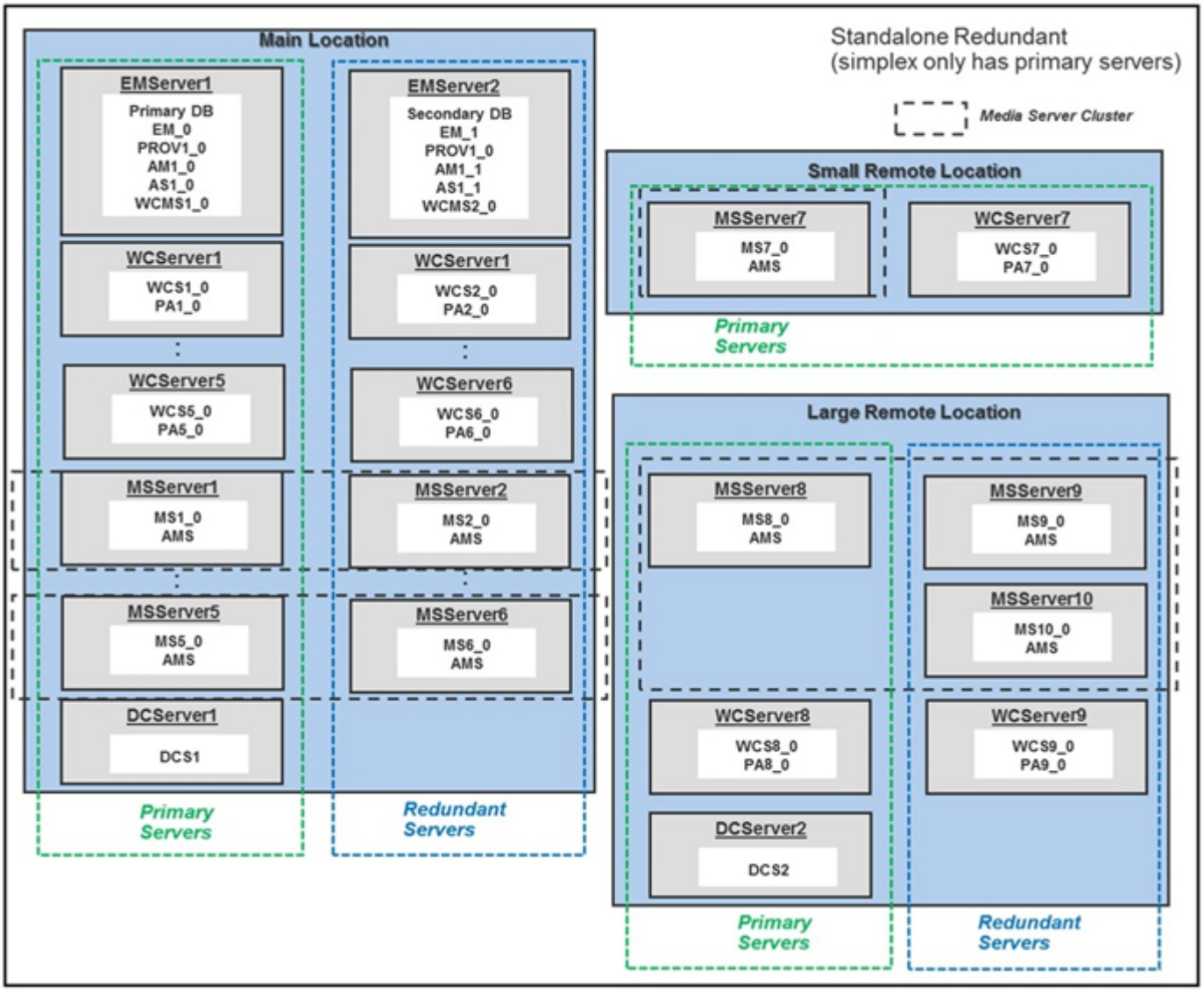
Note:

The software update numbering scheme does not match the official release number for Avaya Aura® Conferencing. Avaya Aura® Conferencing 7.2 is synonymous with MCP_**17**.x.0.0.

Before installing service packs and patches, you must identify the primary servers and redundant servers in a redundant deployment. In a simplex deployment, there are no redundant servers. The following diagrams show the supported deployment configurations and identify the primary and redundant server.


Co-Resident Redundant
(simplex only has primary servers)
Media Server Cluster
Main Location
EMServer1
Primary DB
EM_0
PROV1_0
AM1_0
AS1_0
WCMS1_0
WCS1_0
MS1_0
AMS
EMServer2
Secondary DB
EM_1
PROV2_0
AM1_1
AS1_1
WCMS2_0
WCS2_0
MS2_0
AMS
DCServer1
DCS1
Primary Servers
Redundant Servers


Co-Resident With DMZ Redundant
(simplex only has primary servers)
Media Server Cluster
Main Location
EMServer1
Primary DB
EM_0
PROV1_0
AM1_0
AS1_0
WCMS1_0
MS1_0
AMS
EMServer2
Secondary DB
EM_1
PROV2_0
AM1_1
AS1_1
WCMS2_0
MS2_0
AMS
WCServer1
WCS1_0
PA1_0
WCServer2
WCS2_0
PA2_0
DCServer1
DCS1
Primary Servers
Redundant Servers



You can expand standalone configurations to have media servers in multiple remote locations. Note that the previous diagram does not depict all potential configurations. The media servers in the remote locations may be used to host local conferencing or may be configured to support cascading. Regardless, the media servers are always in clusters. Each cluster has at least a primary media server assigned to it. When determining the primary servers to upgrade in a remote location, examine the configuration for each media server cluster in that location and select the primary media server.

Checklist for upgrading and patching Avaya Aura® Conferencing

The following checklist provides a workflow for upgrading and patching Avaya Aura® Conferencing.

Tip:

To determine your current platform version, log on as root and type mcpRelease.pl.

Table 47: Upgrading and patching workflow checklist

#	Task	Description	Notes	✔
1	Obtain all required software files and create DVDs.	Download software files from PLDS.		
2	Copy and extract the installation files to servers.	See Copying and extracting installation files to servers on page 427.		
3	Back up the: • Avaya Aura® Conferencing database • Avaya Media Servers • Avaya Aura® Conferencing server	See “Chapter 9: Backing up Avaya Aura® Conferencing” in *Maintaining and Troubleshooting Avaya Aura® Conferencing*.		
4	Patch the operating system (if a new platform patch is available).	See Applying operating system patches to the system servers on page 470.		
5	If you want to support DNS, you must configure the DNS client.	See Configuring a DNS client on page 494.		
6	Patch the Avaya Aura® Conferencing database (if a new	See Applying patches to the database on page 479.		

Comments? infodev@avaya.com

#	Task	Description	Notes	✔
	database patch is available).			
7	Upgrade or patch the Avaya Aura® Conferencing software.	See Upgrading or patching the Avaya Aura® Conferencing software on page 480.		

Copying and extracting installation files to servers

Before you begin

Make sure you have the latest version of the following Avaya Aura® Conferencing software:

- Avaya Aura® Conferencing Server Platform
- Avaya Aura® Conferencing Application Bundle
- Avaya Aura® Conferencing Platform Patch

You can download iso images of this software from PDLS and burn the iso images to DVD-ROM.

About this task

Use this procedure to copy the Avaya Aura® Conferencing.

Procedure

1. Copy the Avaya Aura® Conferencing Platform Patch iso image to the primary Element Manager server, and then copy the Avaya Aura® Conferencing Platform Patch iso image to the all other servers that you want to patch.
   a. Log on to the primary Element Manager server as a user with the SA role (for example, `ntappadm`) through ssh or directly at the server console.
   b. Copy the Avaya Aura® Conferencing Platform Patch to `/var/mcp/media/` on the server or insert the Avaya Aura® Conferencing Platform Patch DVD-ROM .
   c. Log on to the primary Element Manager server as `ntsysadm`) through ssh or directly at the server console.
   d. At the command prompt, enter `su -` and press **Enter**.
   e. Type the root password, and press **Enter**.

f. Copy the Avaya Aura® Conferencing Platform Patch to `/var/mcp/os/install/` on the server or insert the Avaya Aura® Conferencing Platform Patch DVD-ROM .

   If you are installing a feature pack or a service pack, copy the patch to the `/var/mcp/os/install/images` directory.

g. Verify that the new Avaya Aura® Conferencing Platform Patch load (for example, `mcp_core_linux_ple2-17.0.1.patches.r-1.ext.iso)` is present in the directory `/var/mcp/os/install/`.

   If you are installing a feature pack or a service pack, check the `/var/mcp/os/install/images` directory.

h. Copy the Avaya Aura® Conferencing Platform Patch iso file to the remaining servers that you want to patch over the network using the command `scp <load_name> <login>@<server_ip>:/var/mcp/loads/images` (for example, `scp /var/mcp/os/install/mcp_core_linux_ple2-17.0.1.patches.r-1.ext.iso ntappadm@192.168.209.138:/var/mcp/media`).

   Example for a feature pack or a service pack: `scp /var/mcp/os/install/images/mcp_core_linux_ple2-17.0.1.patches.r-1.ext.iso ntappadm@192.168.209.138:/var/mcp/media`

i. Log on to the server as a user with the SSA role (for example, `ntsysadm`) through ssh or directly at the server console.

j. At the prompt, type `su-` and press **Enter**.

k. Enter the root password and press **Enter**.

l. Move the Avaya Aura® Conferencing Platform Patch iso file to the directory `/var/mcp/os/install/` using the command `mv /var/mcp/media/<load_name> /var/mcp/os/install/` (for example, `mv /var/mcp/media/mcp_core_linux_ple2-17.0.1.patches.r-1.ext.iso /var/mcp/os/install/`).

   Example for a feature pack or a service pack: `mv /var/mcp/media/mcp_core_linux_ple2-17.0.1.patches.r-1.ext.iso /var/mcp/os/install/images`

m. Repeat Steps h through l for each server.

2. Copy the Avaya Aura® Conferencing Application Bundle iso file to the primary Element Manager server and extract the content. If you are using a DVD, insert the disk.

   a. Log on to the primary Element Manager server as a user with the AA role (for example, `ntappadm`) through ssh or directly at the server console.

   b. Copy the Avaya Aura® Conferencing Application Bundle iso file to `/var/mcp/extract`.

   c. Access the directory that contains the new database installer, type `mcpExtractContent -aat` and press **Enter** to extract the content.

3. If you are not using the Avaya Aura® Conferencing Application Bundle, copy the all components individually.
   a. Log on to the primary Element Manager server as a user with the SSA role (for example, `ntsysadm`) through ssh or directly at the server console.
   b. Copy the new database installer (for example, `installer-mcp-postgresql-9.0.6-14.AAC.LINUX64.zip)` to `/var/mcp/media` on the server .
   c. Verify that the new database installer is present in the directory `/var/mcp/media`.
   d. Copy the new Avaya Aura® Conferencing Application software load (for example, `MCP_17.0.14.0_2013-08-19-1307.zip)` to `/var/mcp/loads` on the server.
   e. Verify that the new Avaya Aura® Conferencing Application software load is present in the directory `/var/mcp/loads`.
4. Clear the alarms using Element Manager Console.
   a. Log on to Element Manager Console.
   b. Right-click the Alarm Summary bar in the Element Manager Console window, and select **Logical View**.
      The Logical View window appears.
   c. Wait for the `Load Available` alarm to appear for the Element Manager.
   d. In the Logical View window, double-click on the **Element Manager** folder.
   e. Select **ElementManager_0** and click **Alarm Browser**.
      The Alarm Browser--Element Manager_0 window appears and displays a `LOADS 801 Load(s) Available` alarm.
   f. In the Alarm Browser--Element Manager_0 window, select the `LOADS 801 Load(s) Available` alarm, and click **Clear**.
5. Copy the Avaya Media Server load to each server where an Avaya Media Server is deployed.
   a. Log on to the first server as a user with the AA role (for example, `ntappadm`) through ssh or directly at the server console.
   b. Copy the Avaya Media Server load zip file (for example, `MCP_MediaServer_7.5.0.329_2013.17.77.zip)` to `/var/mcp/loads` on the server. (The Avaya Media Server load zip file was extracted from the Avaya Aura® Conferencing Application Bundle in Step 2.)
   c. Verify that the new Avaya Media Server load zip file is present in the directory `/var/mcp/loads`.
   d. Copy the Avaya Media Server load zip file over the network to the remaining servers where Avaya Media Server are deployed using the command `scp <load_name> <login>@<server_ip>:/var/mcp/loads/` (for example, `scp /var/mcp/loads/`

```
MCP_MediaServer_7.5.0.329_2012.17_77.zip
ntsysadm@192.168.209.138:/var/mcp/loads/).
```

Result

All required installation files are present on the servers, and the system is ready to be upgraded.

Applying operating system patches to the system servers

About this task

Use this procedure to apply operating system patches to the system servers.

Procedure

1. Stop all Network Element instances deployed on the primary Element Manager server.
   a. Stop the core Network Element instances deployed on the server: EM_0, PROV1, AM1_0, and AS1_0. See Stopping a Network Element instance on page 472.
   b. Stop the WCMS, WCS, and PA Network Element instances if deployed on the server. See Stopping a Network Element instance on page 472.
   c. Lock and stop the Avaya Media Server instances if deployed on the server. (For example, it will be MS1 in a co-resident layout.) See Locking and stopping an Avaya Media Server instance on page 445.
2. Stop the primary database instance. See Stopping a database instance on page 474.
3. Patch the operating system on the primary Element Manager server. See Patching the operating system on page 474.
4. Start the primary database instance. See Starting a database instance on page 476.
5. Start all Network Element instances deployed on the primary Element Manager server.
   a. Start the core Network Element instances deployed on the server: EM_0, PROV1, AM1_0, and AS1_0. See Starting a Network Element instance on page 476.
   b. Start the WCMS, WCS, and PA Network Element instances if deployed on the server. See Starting a Network Element instance on page 476.

Start and unlock the Avaya Media Server instances if deployed on the server. See Starting and unlocking an Avaya Media Server instance on page 477.

6. Verify that the system (the primary half of the system) is operating properly with the upgraded system.

   Note:

   If the system is not operating properly, perform the rollback procedure.

7. Stop all Network Element instances deployed on the secondary Element Manager server.
   a. Stop the core Network Element instances deployed on the server: EM_1, PROV2, AM1_1, and AS1_1. See Stopping a Network Element instance on page 472.
   b. Stop the WCMS, WCS, and PA Network Element instances if deployed on the server. See Stopping a Network Element instance on page 472.
   c. Lock and stop the Avaya Media Server instances if deployed on the server. (For example, it will be MS2 in a co-resident layout.) See Locking and stopping an Avaya Media Server instance on page 445.
8. Stop the secondary database instance. See Stopping a database instance on page 474.
9. Patch the operating system on the redundant Element Manager server. See Patching the operating system on page 474.
10. Start the secondary database instance. See Starting a database instance on page 476.
11. Start all Network Element instances deployed on the redundant Element Manager server.
    a. Start the core Network Element instances deployed on the server: EM_1, PROV2, AM1_1, and AS1_1. See Starting a Network Element instance on page 476.
    b. Start the WCMS, WCS, and PA Network Element instances if deployed on the server. See Starting a Network Element instance on page 476.
    c. Start and unlock the Avaya Media Server instances if deployed on the server. See Starting and unlocking an Avaya Media Server instance on page 477.
12. Patch the operating system on the servers in remote locations one by one.
    a. Stop all Network Element instances deployed on the server except the Avaya Media Server. See Stopping a Network Element instance on page 472.
    b. Lock and stop Avaya Media Server Network Element instances. See Locking and stopping an Avaya Media Server instance on page 445.
    c. Patch the operating system on the server. See Patching the operating system on page 474.
    d. Start all Network Element instances deployed on the server except the Avaya Media Server. See Starting a Network Element instance on page 476.

e. Start and unlock the Avaya Media Server instances. See Starting and unlocking an Avaya Media Server instance on page 477.

Result

All servers are patched and ready for database and Avaya Aura® Conferencing patching/upgrading.

Related topics:

Locking and stopping an Avaya Media Server instance on page 445
Stopping a Network Element instance on page 472
Stopping a database instance on page 474
Patching the operating system on page 474
Starting a database instance on page 476
Starting a Network Element instance on page 476
Starting and unlocking an Avaya Media Server instance on page 477
Deploying and starting the core Network Element instances on the Primary servers on page 478

Stopping a Network Element instance

About this task

Use this procedure to stop a Network Element instance.

Procedure

1. Log on to Element Manager Console.
2. In the navigation pane of Element Manager Console, select **Feature Server Elements**> ***<Network Element type>*** > ***<Network Element instance you want to stop>*** > **NE Maintenance**.
3. In the Maintenance dialog box, select the row that has a value of the target instance in the ID column.
4. Click **Stop**.
   The Maint state changes from “None” to “Stopping,” indicating that the stop operation is in progress. When the stop operation is complete, the following state changes occur:
   - The Maint state changes back to “None.”
   - The Admin state changes from “Online” to “Offline.”

Result

The Network Element instance is stopped.

Locking and stopping an Avaya Media Server instance

About this task

Use this procedure to stop an Avaya Media Server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server network element instance you want to stop*> > Service Maintenance**.
2. In the Media Server Service Maintenance window, select the Avaya Media Server instance.
3. Click **Pending Lock**.
   All new requests will be redirected to other Avaya Media Servers in the cluster. All existing sessions are allowed to continue, but new sessions are not allowed.
4. In the navigation pane of Element Manager Console, select **Key Performance Indicators > Monitoring and Reporting > Sessions**.
5. Watch the number of sessions on the Avaya Media Server, and wait for the number of sessions to become 0 or an acceptable small number.
6. When the number of sessions becomes 0 or an acceptable small number, select the Avaya Media Server instance in the Media Server Service Maintenance window and click **Lock**.
   Existing sessions are terminated, and no additional sessions are allowed into the Avaya Media Server, even after the Avaya Media Server restarts.
7. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers** > **<*Media Server network element instance*>** > **NE Maintenance**.
8. In the Media Server NE Maintenance window, select the row that has a value of the target instance in the ID column.
9. Click **Stop**.
   The Maint state changes from “None” to “Stopping,” indicating that the stop operation is in progress. When the stop operation is complete, the following state changes occur:
   - The Maint state changes back to “None.”
   - The Admin state changes from “Online” to “Offline.”

10. Close the Media Server NE Maintenance window.

Result

The Avaya Media Server is stopped. Calls are handled by another Avaya Media Server in the cluster.

Stopping a database instance

About this task

Use this procedure to stop a database instance.

Procedure

1. Log on to the server as a user with the SSA role (for example, `ntsysadm`) through ssh or directly on the server console .
2. At the prompt, type `stopDB` and press **Enter**.

   Note:

   If prompted, enter the password for the SSA user.

   The following output should appear:

   ```
   stopDb.pl Started at => <day month date time year> by root
   stopDb.pl Completed at => <day month date time year>
   Reference the following log file for additional details:
   /opt/mcp/db/slogs/stopDb.log
   ```

   Note:

   If the output displayed above does not appear, stop and contact Avaya support.

Patching the operating system

About this task

Use this procedure to apply server platform patches to the target server.

Procedure

1. Log on to the server as a user with the SSA role (for example, `ntsysadm`) through ssh or directly at the server console.
2. At the prompt, type `su -` and root password.
3. Press **ENTER**.
4. At the prompt, type `cd /var/mcp/os/install/` and press **ENTER**.
5. At the prompt, type `patchPlatform.pl <file>.iso -np` where <file>.iso is the patch ISO file.
6. Press **ENTER**.
   The patchPlatform.pl tool compares the patches contained in the patch ISO file against the current release of the system.

   If there are no required patches, the following message appears, the tool exits, and the patching procedure is complete:

   ```
   No applicable patche(es).

   Number of patches applied: 0
   ```

   If one or more patches are required, those patches are displayed and then automatically applied to the system. Once the last patch has been applied, the server reboots automatically.

   ```
   No applicable patche(es).

   Number of patches applied: 0
   ```
7. After the server reboots, log on to the server using any account.
8. At the prompt, type `mcpRelease.pl` and press **ENTER**.
   The system displays the release level. The following is an example of the release level information displayed:

   ```
   *** MCP Platform Release ***

   System Type: mcp_core_linux_ple2

   Release Level: 17.0.1 (via patching)

   Hardware Env: Other
   ```
9. Verify that the release level displayed matches the patch you installed.

   Note:

   If the release level displayed does not match the patch you installed, contact Avaya support.

Result

The server platform patch is complete.

Starting a database instance

About this task

Use this procedure to start a database instance.

Procedure

1. Log on to the server as a user with the SSA role (for example, `ntsysadm`) through ssh or the server console.
2. At the prompt, type `startDB` and press **ENTER**.

   Note:

   If prompted, enter the password for the SSA user.

   The following output should appear:

   ```
   startDb.pl Started at => <day month date time year> by root
   startDb.pl Completed at => <day month date time year>
   Reference the following log file for additional details:
   /opt/mcp/db/slogs/startDb.log
   ```

   Note:

   If the output displayed above does not appear, stop and contact Avaya support.

Result

The database instance is up and running.

Starting a Network Element instance

About this task

Use this procedure to start a Network Element instance.

Procedure

1. Log on to Element Manager Console.
2. In the navigation pane of Element Manager Console, select **Feature Server Elements**> ***<Network Element type>*** > ***<Network Element instance you want to start>*** > **NE Maintenance**.
3. In the Maintenance dialog box, select the row that has a value of the target instance in the ID column.
4. Click **Start**.
   The Maint state changes from “None” to “Starting,” indicating that the start operation is in progress. When the start operation is complete, the following state changes occur:
   - The Maint state changes back to “None.”
   - The Admin state changes from “Offline” to “Online.”
   - The Link state changes from “Down” to “Up.”
   - The Oper state changes from “Unavailable” to either “Active” or “Hot Standby,” based on the instance of the component.

Result

The Network Element instance is up and running.

Starting and unlocking an Avaya Media Server instance

About this task

Use this procedure to start an Avaya Media Server instance.

Procedure

1. Log on to Element Manager Console.
2. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > *<Media Server name>* > NE Maintenance**.
3. In the Media Server Maintenance dialog box, select the row that has a value of the target instance in the ID column.
4. Click **Start**.
   The Maint state changes from “None” to “Starting,” indicating that the start operation is in progress. When the start operation is complete, the following state changes occur:

- The Maint state changes back to “None.”
- The Admin state changes from “Offline” to “Online.”
- The Link state changes from “Down” to “Up.”
- The Oper state changes from “Unavailable” to either “Active” or “Hot Standby,” based on the instance of the component.

5. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers** > **<*Media Server name*>** > **Service Maintenance**.
6. In the Media Server Maintenance dialog box, select the Avaya Media Server.
7. Click the **Unlock** button.

Result

The Avaya Media Server is up and running.

Deploying and starting the core Network Element instances on the Primary servers

About this task

Use this procedure to deploy and start the core network element instances on the primary servers.

Procedure

1. Upgrade the Avaya Media Server software on each stopped Avaya Media Server network instance. See Upgrading the software on page 486.
2. Deploy all network element instances deployed on the primary servers except Avaya Media Server network element instances. See Deploying a Network Element instance on page 493.
3. Start all network element instances deployed on the primary servers except Avaya Media Server network element instances. See Starting a Network Element instance on page 476.
4. Deploy all Avaya Media Server network element instances deployed on the primary servers. See Deploying a Network Element instance on page 493.
5. Start and unlock all Avaya Media Server network element instances on the primary servers. See Starting and unlocking an Avaya Media Server instance on page 477.

Applying patches to the database software

Before you begin

Make sure the database is installed and running. See Starting a database instance on page 476.

About this task

Use this procedure to apply patches to the database software.

Procedure

1. Patch the primary database.
   a. Log on to the primary Element Manager server as a user with the SA role (for example, `ntappadm`) through ssh or directly at the server console.
   b. At the prompt, type `cd /var/mcp/install` and press **ENTER**.
   c. At the prompt, type `./mcpDbSwPatch.pl –primary` and press **ENTER**.
   A communications test to the target database server is performed, and a configuration summary is presented. You are prompted to select the target database patch zip file.
   d. Type the number of the patch zip file you want to use.
   The following message appears:

   ```
   Continue with Database Software PATCH? (Y/N) [N]:
   ```

   e. Type `y`.
   The following message appears and the patching process starts for the database:

   ```
   PATCH, for Database software on <ip_address> ...

   Upgrading Database Software...please be patient
   ```

   Depending on the server hardware and the target server receiving the installation, the installation process could take up to 15 minutes.

   Once the installation is complete, the following message appears:

   ```
   mcpDbSwPatch Completed Successfully.
   ```

   Note:

   If the message does not appear, stop and contact Avaya support.

2. Patch the secondary database.
   a. At the prompt, type `cd /var/mcp/install` and press **ENTER**.
   b. At the prompt, type `./mcpDbSwPatch.pl –secondary` and press **ENTER**.

A communications test to the target database server is performed, and a configuration summary is presented. You are prompted to select the target database patch zip file.

c. Type the number of the patch zip file you want to use.
The following message appears:

```
Continue with Database Software PATCH? (Y/N) [N]:
```

d. Type `y`.
The following message appears and the patching process starts for the database:

```
PATCH, for Database software on <ip_address> ...

Upgrading Database Software...please be patient
```

Depending on the server hardware and the target server receiving the installation, the installation process could take up to 15 minutes.

Once the installation is complete, the following message appears:

```
mcpDbSwPatch Completed Successfully.
```

Note:

If the message does not appear, stop and contact Avaya support.

Result

The Database patch is complete.

Upgrading or patching the Avaya Aura® Conferencing software

About this task

Use this procedure to upgrade or patch the Avaya Aura® Conferencing load.

Note:

Any documents uploaded to web collaboration when the primary WCMS is “down” will be lost.

Procedure

1. Upgrade or patch the MCP database and Element Manager.

- To install a maintenance release, see Upgrading the database and Element Manager on page 483.
- To install a patch release, see Patching the database and Element Manager on page 484.

2. Upgrade or patch the network element instances on each server one by one.
   a. Upgrade all network instances on the server except the Avaya Media Server. See Upgrading and patching a network element on page 485.
   b. Lock and stop Avaya Media Server instances on the server. See Locking and stopping an Avaya Media Server instance on page 445.
   c. Upgrade the Avaya Media Server software. See Upgrading the software on page 486.
   d. Upgrade the Avaya Media Server instances on the server. See Upgrading and patching a network element on page 485.
   e. Start and unlock Avaya Media Server instances on the server. See Starting and unlocking an Avaya Media Server instance on page 477.
3. Upgrade or patch the primary Avaya Media Server instances for each media server cluster.
   a. Lock and stop the primary Avaya Media Server instances for each media server cluster. See Locking and stopping an Avaya Media Server instance on page 445.
   b. Upgrade the Avaya Media Server software on each stopped instance. See Upgrading the software on page 486.
   c. Upgrade the primary Avaya Media Server instances for each media server cluster. See Upgrading and patching a network element on page 485.
   d. Start and unlock the primary Avaya Media Server instances for each media server cluster. See Starting and unlocking an Avaya Media Server instance on page 477.
4. Upgrade or patch the secondary Avaya Media Server network instances for each media server cluster.
   a. Lock and stop the secondary Avaya Media Server instances for each media server cluster. See Locking and stopping an Avaya Media Server instance on page 445.
   b. Upgrade the Avaya Media Server software on each stopped instance. See Upgrading the software on page 486.
   c. Upgrade the secondary Avaya Media Server instances for each media server cluster. See Upgrading and patching a network element on page 485.
   d. Start and unlock the secondary Avaya Media Server instances for each media server cluster. See Starting and unlocking an Avaya Media Server instance on page 477.
5. Upgrade or patch the remaining standard Avaya Media Server network element instances for each media server cluster.

a. Lock and stop the standard Avaya Media Server instances for each media server cluster. See Locking and stopping an Avaya Media Server instance on page 445.
b. Upgrade the Avaya Media Server software on each stopped instance. See Upgrading the software on page 486.
c. Upgrade the standard Avaya Media Server instances for each media server cluster. See Upgrading and patching a network element on page 485.
d. Start and unlock standard Avaya Media Server instances for each media server cluster. See Starting and unlocking an Avaya Media Server instance on page 477.

6. Upgrade each Document Conversion Server.
   a. Log in to Element Manager Console.
   b. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Web Conferencing** > **Default Web Conferencing Server Group**.
   c. Verify the server displayed in the Document Conversion Server box in the Default Web Conferencing Server Group dialog box. If the Document Conversion Server you are upgrading is displayed in the Document Conversion Server box, select a different server from Document Conversion Server box, and click **Apply**.
   d. Log in to Provisioning Client.
   e. In the Provisioning Client window, select **System Management > Routing > Web Conferencing Server Resources**.
   f. Click the Web Conferencing Server Groups tab.
   g. For each location, verify the server displayed in the Document Conversion Server box. If the Document Conversion Server you are upgrading is displayed in the Document Conversion Server box, select a different server from the Document Conversion Server box, and click **Save**.
   h. Upgrade the Document Conversion Server. See Upgrading the Document Conversion Server on page 487.
   i. If you modified the Document Conversion Server setting for any locations in Provisioning Client, set the Document Conversion Server back to its previous setting.
   j. If you modified the Document Conversion Server for the Default Web Conferencing Server Group in Element Manager Console, set the Document Conversion Server back to its previous setting.

Result

The new Avaya Aura® Conferencing load is installed, and the system is up and running.

Related topics:

Upgrading Audio/Video in Collaboration Agent on page 365
Upgrading the MCP database and Element Manager on page 483

Patching the MCP database and Element Manager on page 484
Patching or upgrading a network element on page 485
Upgrading the Avaya Media Server software on page 486
Upgrading the Document Conversion Server on page 487

Upgrading the MCP database and Element Manager

About this task

Use this procedure to upgrade the MCP database and Element Manager to the newest maintenance release.

Procedure

1. Log on to the primary Element Manager server as a user with the AA role (for example, `ntappadm`) through ssh or directly at the server console.
2. At the prompt, type `cd /var/mcp/install`and press **ENTER**.
3. At the prompt, type `./mcpUpgradeMR.pl` and press **ENTER**.
   The list of available loads appears.
4. Type the number of the load you want to use.
   The following message appears and the upgrade starts for the MCP database and Element Manager:

   ```
   --- Invoking mcpUpgrade => to upgrade the EM & Database ---
   ```

   Note:

   If the upgrade message does not appear, stop and contact Avaya support.

   Once the upgrade of the MCP database and Element Manager is complete, the following message appears:

   ```
   --- EM & DataBase Upgrade Complete ---
   ```

   Note:

   If an error occurs (for example, due to loss of network connectivity), retry the mcpUpgradeMR.pl script after you resolve the problem. If an error occurs again, stop and contact Avaya support.

Result

The MCP database and Element Manager are upgraded to the newest maintenance release.

Patching the MCP database and Element Manager

About this task

Use this procedure to patch the MCP database and Element Manager to the newest patch release.

Procedure

1. Log on to the primary Element Manager server as a user with the AA role (for example, `ntappadm`) through ssh or directly at the server console.
2. At the prompt, type `cd /var/mcp/loads`and press **ENTER**.
3. At the prompt, type `./mcpPatch.pl -l <patch_filename>`(for example, `./mcpPatch.pl -l MCP_15.0.13.1_2012-08-15-0717`).
4. Press **ENTER**.
   A configuration summary is displays, and then the following prompt appears:

   ```
   Continue with these settings? (Y/N) [N]:
   ```

5. Type `y`.
   The following message appears and the patching starts for the MCP database and Element Manager:

   ```
   --- Patching the installation scripts
   ```

   Note:

   If the patching message does not appear, stop and contact Avaya support.

   Once the patching of the MCP database and Element Manager is complete, the following message appears:

   ```
   --- EM & DataBase Patch Complete ---
   ```

   Note:

   If an error occurs (for example, due to loss of network connectivity), retry the mcpPatch.pl script after you resolve the problem. If an error occurs again, stop and contact Avaya support.

Result

The MCP database and Element Manager are patched to the newest patch release.

Patching or upgrading a network element

About this task

Use this procedure to patch or upgrade a network element. Both patches and upgrades are distributed as ZIP files. The file names for these ZIP files consist of the components *MCP_release.number_year-month-date-time.zip*. For example, the file `MCP_17.0.13.0_2013-08-03-1201.zip` indicates this ZIP file contains release 17.0.13.0, which was built on August 3, 2013 at 12:01 pm.

You can differentiate between a patch release and an upgrade release by looking at the last digit of the release number in the ZIP file name. For a patch release, the last digit of the release number is always a non-zero digit (for example, MCP_17.0.13.*1*_2013-08-15-1707.zip). For an upgrade release, the last digit of the release number is always a zero (for example, MCP_17.0.13.*0*_2013-08-03-1201.zip).

Use the **Patch** button when installing a new patch release. Use the **Upgrade** button when installing a new maintenance release.

Procedure

1. Log on to Element Manager Console.
2. From the Tools menu, select **Patch/MR Manager**.
3. From the Load or Patch box in the Patch/MR Manager window, select the patch you want to install.
   Green check marks should appear on both the Element Manager folder and the Logical DBs folder.
4. Select the network element type you want to upgrade or patch.
5. Select the network element instance you want to upgrade or patch.
6. Perform one of the following steps:
   - If you want to patch the network element instance, click **Patch**.
   - If you want to upgrade the network element instance, click **Upgrade**.
7. When the NE Maintenance window appears, click **Details** to display the patching or upgrading steps in a status pane at the bottom of the window.
8. Verify that no failures are reported in the status pane at the bottom of the window and the patching or upgrading process completes successfully.

Note:

If there are any failures, stop and contact Avaya support.

Result

The selected network element has been patched or upgraded to the target load.

Upgrading the Avaya Media Server software

Before you begin

Obtain the Application Bundle DVD-ROM.

Note:

If you have a co-resident with redundancy deployment or a standalone with redundancy deployment, you must stop all network elements before performing this procedure. See Stopping a Network Element instance on page 472.

About this task

Use this procedure to upgrade the Avaya Media Server software.

Note:

- You must upgrade all the Avaya Media Servers in your deployment.
- If you have a co-resident with redundancy deployment or a standalone with redundancy deployment, you must stop all network elements before performing this procedure. See Stopping a Network Element instance on page 472.

Procedure

1. Log on to the Avaya Media Server as a user with the SSA role (for example, `ntsysadm`) through ssh or directly at the server console.
2. At the prompt, type `su -` and the root password, and then press **ENTER** to become the root user.
3. At the prompt, type `mcpMsInstall.pl` and press **ENTER**.
   The install script finds the zipped file. The system will detect more than one zipped file.
4. At the prompt `Please enter number [1 or 2] of selection`, type the number that corresponds to the zipped file containing the upgrade.
   The selected file is unzipped
5. At the prompt `Continue installation? (Y/N)`, type `y` and press **ENTER**.
   Information about the load appears on the screen.
6. Type `Y` to confirm you have read the information, and press **ENTER**.
   The installer detects a previous version already installed.
7. At the prompt `Proceed with upgrade? (Y/N)`, type `y`, and press **ENTER**.
8. Start the Avaya Media Server network element instance. See Starting a Network Element instance on page 476.

9. Repeat Steps 1 through 8 for every Avaya Media Server in the deployment.

Result

The message `Installation completed SUCCESSFULLY` appears. The Avaya Media Server load is now upgraded.

Upgrading the Document Conversion Server

Before you begin

Important:

The Document Conversion Server software is located in the `dcs` folder in the MCP load on the Application Server (for example, `/var/mcp/install/MCP_15.x.x.xx_2012-08-16-1238/dcs/dcs_MCP_15.x.x.xx_2012-08-16-1238.zip`).

If you copy the software to the Document Conversion Server using a method that differs from the recommended approach, perform the following steps:

1. Right-click the zip file, click **Properties**.
2. On the **General** tab, in the Security section, click **Unblock**.
3. Click **Apply**.
4. Click **OK**.

About this task

Use the following procedure to upgrade the Document Conversion Server.

Procedure

1. Stop the DCS process.
2. Insert the Application Bundle DVD-ROM on the Windows server.
3. Obtain the Document Conversion Server software (for example, `dcs_MCP_15.0.0.1-2011- 09-2200.zip`) from the core directory `/dcs/dcs_<version><date-time>.zip`.
4. Copy the zip file to `c:\` and extract the files.

   Note:

   You are prompted to overwrite the existing dcs directory.
5. Remove the read-only attribute on the dcs directory and apply the changes to the sub-directories.

6. Using Windows Explorer, navigate to `c:\`, right-click on the **dcs** folder, and select **Properties**.
7. In the Properties dialog box, uncheck the Read-only check box, and then click **Apply**.
8. In the Properties dialog box, click **OK**.
9. Save the settings from the configuration file (`<installed directory>/dcs/htdocs/app/Config.php`).
10. Save the settings from the httpd configuration file (`<installed directory>/dcs/conf/httpd.conf`).
11. Save the certificates. For more information, see “Chapter 10: Installing and configuring the Document Conversion Server.”
12. Navigate to `c:\dcs`.
13. At the prompt, type `Setup DCS.bat` and press **ENTER**.

Result

The Document Conversion Server has been upgraded to the target load.

Upgrading Audio/Video in Collaboration Agent

If Avaya releases a new service pack or a new feature pack, you may have to upgrade the Audio/Video in Collaboration Agent feature. The process of upgrading the Audio/Video in Collaboration Agent feature is the same for service packs, feature packs, and patch releases. The only difference between these three types of releases is the method of obtaining the software from PLDS.

Related topics:

Upgrading the Audio/Video in Collaboration Agent server software on page 488
Upgrading the Audio/Video in Collaboration Agent Management Portal software on page 489
Upgrading the Audio/Video in Collaboration Agent client software on page 490

Upgrading the Audio/Video in Collaboration Agent server software

Before you begin

You must be able to access the Audio/Video in Collaboration Agent server software (AccWeb-a-b-c.i386.rpm.bin).

About this task

Use this procedure to upgrade the Audio/Video in Collaboration Agent server software. You will install the updated software on the Flash Media Gateway server.

Procedure

1. Log on to the Flash Media Gateway server as `ntsysadm` through ssh or directly on the server console.
2. Enter **`su -`** to log on as root.
3. At the prompt `password`, type the root password, and press **Enter**.
4. Copy the file `AccWeb-a-b-c.i386.rpm.bin` from the directory `/var/mcp/media/avica` on the primary Element Manager server into the directory `/var/mcp/media/avica` on the Flash Media Gateway server.
5. Go to the directory `/var/mcp/media/avica` on the Flash Media Gateway server.
6. Type `chmod +x AccWeb-x.x-x.i386.rpm.bin` and press **Enter**.
7. Type `./AccWeb-x.x-x.i386.rpm.bin` and press **Enter**.
   The Avaya Customer Connections Web End User License Agreement (EULA) appears.
8. Read the license agreement.
9. To accept the license agreement and proceed with the upgrade, type `y`.
   The software is upgraded on the server. During the upgrade, the software is upgraded in the directory `/opt/Avaya/AccWeb`, and Red5 Media Server is installed in the directory `/usr/local/red5`.
10. Start the server software.
    At the command prompt, type `service red5 start` and press **Enter**.

Next steps

Proceed to Upgrading the Audio/Video in Collaboration Agent Management Portal software on page 489.

Upgrading the Audio/Video in Collaboration Agent Management Portal software

Before you begin

You must be able to access the Audio/Video in Collaboration Agent Management Portal software (AccWeb-clients-d-e.zip).

About this task

Use this procedure to upgrade the Audio/Video in Collaboration Agent Management Portal software. You will install the updated software on the Element Manager server where the Provisioning Manager (PROV) is installed.

Procedure

1. Log on to the Element Manager server where the Provisioning Manager is installed as `ntsysadm` through ssh or directly on the server console.
2. Enter **`su -`** to log on as root.
3. At the prompt `password`, type the root password, and press **Enter**.
4. Copy the file `AccWeb-clients-d-e.zip` from the directory `/var/mcp/media/avica` on the primary Element Manager server into the directory `/var/mcp/media/avica` on the target server.
5. Go to the directory `/var/mcp/media/avica` on the target server.
6. At the prompt, type `unzip AccWeb-clients-d-e.zip admin/* -d fmgtemp/` and press **Enter**.
7. At the prompt, type `cp -R fmgtemp/admin/* /var/mcp/media/prov_pa_installs/fmgadmin/` and press **Enter**.
8. At the prompt, type `chown -R ntappsw:ntappgrp /var/mcp/media/prov_pa_installs/fmgadmin` and press **Enter**.
9. At the prompt, type `chmod -R 770 /var/mcp/media/prov_pa_installs/fmgadmin` and press **Enter**.
10. At the prompt, type `rm -rf fmgtemp` and press **Enter**.

Next steps

Proceed to Upgrading the Audio/Video in Collaboration Agent client software on page 490.

Upgrading the Audio/Video in Collaboration Agent client software

Before you begin

- You must be able to access the Audio/Video in Collaboration Agent client software (`AacpaOtv-client-f-g.zip`).
- You must be able to access the client configuration file you created (`AccWebCustomerConfig.xml`).

About this task

Use this procedure to upgrade the Audio/Video in Collaboration Agent client software and configuration file you created. You will upgrade this software and configuration file on the Personal Agent Manager server.

Procedure

1. Log on to the Personal Agent Manager server as `ntsysadm` through ssh or directly on the server console.
2. Enter **`su -`** to log on as root.
3. At the prompt `password`, type the root password, and press **Enter**.
4. Go to the directory `/var/mcp/media/prov_pa_installs/otv`.
5. At the prompt, type `\cp -f ACCWebCustomerConfig.xml ACCWebCustomerConfig.xml.bkp`.

   This step creates a backup file of the existing configuration. You will require this information for later steps.
6. Copy the file `AacpaOtv-client-x-y.zip` from the directory `/var/mcp/media/avica` on the primary Element Manager server into the directory `/var/mcp/media/avica` on the Personal Agent Manager server.
7. Go to the directory `/var/mcp/media/avica` on the Personal Agent Manager server.
8. Type `unzip AacpaOtv-client-x-y.zip AacpaOtv/* –d fmgtemp/` and press **Enter**.
9. Type `cp –R fmgtemp/AacpaOtv/* /var/mcp/media/prov_pa/installs/otv` and press **Enter**.
10. Type `rm –rf fmgtemp` and press **Enter**.
11. Create the client configuration file.

    See Creating the client configuration file on page 353.
12. Copy the file `AccWebCustomerConfig.xml` file to the directory `/var/mcp/media/prov_pa_installs/otv/` on the Personal Agent Manager server.
13. At the prompt, type `chown -R ntappsw:ntappgrp /var/mcp/media/prov_pa_installs/otv` and press **Enter**.
14. At the prompt, type `chmod -R 770 /var/mcp/media/prov_pa_installs/otv` and press **Enter**.

Patching database software

Database software patches are installed when the database application software is not current with the latest patches. The patches are applied to the server that hosts the Element Manager database components for the DB_0 primary database and DB_1 secondary database.

About this task

Apply the database software patches for the primary and secondary database servers while logged on to EMServer1.

Procedure

1. Log on to EMServer1 as ntappadm through ssh or directly at the server console.
2. Type `cd /var/mcp/install`, and press **Enter**.
3. Type **`./mcpDbSwPatch.pl -primary`**, and press **Enter**.
   A communication test with the target database server is performed.
4. A list of database patches appear. Type the number that corresponds to the database patch, and press **Enter**.
5. At the prompt `Continue with Database PATCH? (Y/N) [N]`, type `y`, and press **Enter**.
   The following messages appear:

   `Obtaining Current DB software release info on <IP address>`.
   After the patching completes, you see the message `mcpDbSwPatch Completed Successfully`. The database software patching is complete.

   Note:

   Depending on the server hardware and the target server receiving the installation, the installation process could take some time to complete.
6. For co-resident and standalone deployments where there is a secondary database server, repeat steps 1 on page 492 to 5 on page 492 and replace `./mcpDbSwPatch.pl -primary` with `./mcpDbSwPatch.pl -secondary`.

Result

The database software patching is complete for the primary and secondary database.

Deploying a network element instance

About this task

Use this procedure to deploy a network element instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements**> ***<Network Element type>*** > ***<Network Element instance you want to start >*** **Instance**.
2. In the Instance window, select the row that has a value of the target instance in the ID column, and click **Edit**.
3. In he Edit Instance dialog box, change the load or patch value to the target, and click **Apply**.
4. In the navigation pane of Element Manager Console, select **Feature Server Elements**> ***<Network Element type>*** > ***<Network Element instance you want to start*** > **NE Maintenance**.
5. In the Maintenance dialog box, select the row that has a value of the target instance in the ID column.
6. Click **Deploy**.
   The Maint state changes from “None” to “Deploying,” indicating that the deploy operation is in progress. When the deploy operation is complete, the following state changes occur:
   - The Maint state changes back to “None.”
   - The Admin state is “Offline.”
   - The Link state is “Down.”
   - The Oper state is “Unavailable.”

Result

The Network Element instance is deployed.

Configuring a DNS client

About this task

Use this procedure to configure a DNS client.

Procedure

1. Log on to the server as a user with the SSA role (for example, `ntsysadm`) through ssh or the server console.
2. At the prompt, type `updateDNSSettings` and press **ENTER**.
3. At the prompt `Do you want to configure DNS Client? (Y/N) [Y]`, type `y` and press **Enter**.
4. At the prompt `Please select one of the following actions:- [A]dd Domain Suffix(es)- Accept the configuration and [C]ontinueEnter selection [C]`: type `c` to continue or `a` to add suffixes, and press **Enter**.
5. At the prompt `How many DNS Servers would you like to reference (1-3) [1]`, type the number of available DNS servers, and press **Enter**.
6. At the prompt `Enter DNS Server`, type the IP address of the DNS server, and press **Enter**.
7. At the prompt `You entered "<IP address>". Is this correct? (Y/N) [N]`, verify the IP address.
8. If the IP address is correct, type `y` and press **Enter**.
9. At the prompt `Is this information correct? (Y/N) [N]`, verify the output, type `y`, and press **Enter**.
10. At the prompt, type `hostTableConfig -q` and press **Enter**.
11. Find the entries for SMGR, WCS, and DCS in the output for the command you entered in Step 10.
12. At the prompt, type `hostTableConfig -d <SMGR IP address>` and press **Enter**.
13. At the prompt, type `hostTableConfig -d <WCS IP address>` and press **Enter**.
14. At the prompt, type `hostTableConfig -d <DCS IP address>` and press **Enter**.

Result

The DNS client is configured, and the old host entries are removed.

Chapter 30: Backing up Avaya Aura® Conferencing

The complete backup of Avaya Aura® Conferencing consists of backing up the Avaya Aura® System Manager server and the Avaya Aura® Conferencing servers. To back up the entire Avaya Aura® Conferencing system, perform the following steps:

1. Back up the Avaya Aura® System Manager data. For more information, see *Administering Avaya Aura® System Manager.*
2. On every Avaya Aura® Conferencing server, back up the data. (This backup includes database, media server, and operating system backups.)

Note:

There are optional backup jobs that operate on file system integrity (FSI) baseline snapshots. This information is backed up to keep historical records for future reference. This enables you to remove some of the content of the baseline directory to free up space without losing historical data. You can restore the FSI data at a later date to compare against a current baseline. Avaya recommends that you back up the FSI information weekly.

Example 1: Backup of a co-resident redundant layout (EMserver1 and EMServer 2)

To back up this configuration, perform the following steps:

1. On EMServer1, perform the following steps:
    a. Back up the database. (For more information, see Backing up the database on page 499.)
    b. Back up the Avaya Media Server. (For more information, see Backing up an Avaya Media Server on page 502.)
    c. Back up the Avaya Aura® Conferencing server. (For more information, see Backing up an server on page 505.)
2. On EMServer2, perform the following steps:
    a. Back up the Avaya Media Server. (For more information, see Backing up an Avaya Media Server on page 502.)
    b. Back up the Avaya Aura® Conferencing server. (For more information, see Backing up an server on page 505.)

Example 2: Backup of a co-resident simplex layout (EMserver1)

To back up this configuration, perform the following steps on EMServer1:

1. Back up the database. (For more information, see Backing up the database on page 499.)
2. Back up the Avaya Media Server. (For more information, see Backing up an Avaya Media Server on page 502.)
3. Back up the Avaya Aura® Conferencing server. (For more information, see Backing up an server on page 505.)

Example 3: Backup of a standalone redundant layout (EMserver1, EMServer 2, WCserver1, WCserver2, and MS1Server1)

To back up this configuration, perform the following steps:

1. On EMServer1, perform the following steps:
    a. Back up the database. (For more information, see Backing up the database on page 499.)
    b. Back up the Avaya Aura® Conferencing server. (For more information, see Backing up an server on page 505.)
2. On EMServer2, back up the Avaya Aura® Conferencing server. (For more information, see Backing up an server on page 505.)
3. On WCserver1, back up the Avaya Aura® Conferencing server. (For more information, see Backing up an server on page 505.)
4. On WCserver2, back up the Avaya Aura® Conferencing server. (For more information, see Backing up an server on page 505.)
5. On MS1Server1, perform the following steps:
    a. Back up the Avaya Media Server. (For more information, see Backing up an Avaya Media Server on page 502.)
    b. Back up the Avaya Aura® Conferencing server. (For more information, see Backing up an server on page 505.)

Example 4: Backup of a standalone simplex layout (EMserver1, WCserver1, and MS1Server1)

To back up this configuration, perform the following steps:

1. On EMServer1, perform the following steps:
    a. Back up the database. (For more information, see Backing up the database on page 499.)
    b. Back up the Avaya Aura® Conferencing server. (For more information, see Backing up an server on page 505.)
2. On WCserver1, back up the Avaya Aura® Conferencing server. (For more information, see Backing up an server on page 505.)
3. On MS1Server1, perform the following steps:
    a. Back up the Avaya Media Server. (For more information, see Backing up an Avaya Media Server on page 502.)
    b. Back up the Avaya Aura® Conferencing server. (For more information, see Backing up an server on page 505.)

Backing up the database

This section provides the procedures that you perform to:

- back up the database manually
- schedule an automatic backup of the database
- remove scheduled automatic backups of the database

Important:

Avaya recommends that you store backup data in a remote location to facilitate recovery in the event of a server failure.

The backup data rate for a server is approximately 300 megabytes (MB) per minute. The time to create the backup varies with the size of the database. If the database is in use during the backup, the time required to create the backup increases.

Related topics:

Backing up the database manually on page 499
Scheduling automatic database backups on page 500
Removing scheduled automatic database backups on page 501

Backing up the database manually

Before you begin

- You are a user with the DBA role.
- You know the name of the database you want to back up. The system uses the name of the database to derive the directory path to the backup script.

About this task

Use this procedure to perform a manual backup of the primary database.

Note:

The default name for the database is **mcpdb**. The example commands in this procedure use **mcpdb** for the database name. If **mcpdb** is NOT the name of the database (the value for the db.neName parameter from the installprops.txt file), replace **mcpdb_0** with **<your db.neName>_0** in the command.

Procedure

1. Log on to the primary database server as a user with the DBA role.

2. Enter `cd /var/mcp/run/MCP_17.0/mcpdb_0/bin/util`.
3. Enter `./dbBackup.pl <BackupFileName>`.

Result

The backup file is created and stored in the /var/mcp/db/backup/latest folder. The backup file name is <BackupFileName>.tar.gz.

The previous manual backup file was moved to the /var/mcp/db/backup folder. If the /var/mcp/db/backup/latest folder contained a scheduled automatic backup file, the automatic backup file is moved to the /var/mcp/db/backup/AUTO_history folder.

Note:

There is no limit on the number of manual backup files which are stored in the /var/mcp/db/backup folder.

Scheduling automatic database backups

Before you begin

- You are a user with the DBA role.
- You know the name of the database you want to back up. The system uses the name of the database to derive the directory path to the backup script.

About this task

Use this procedure to schedule automatic backups of the primary database.

Important:

Avaya recommends that you schedule backups for off-peak hours. The default backup time is 3:30 a.m.

Note:

The backup data rate is approximately 300 MB per minute. The time to create the backup varies with the size of the database. If the database is in use during the backup, the time required to create the backup increases.

Note:

The default name for the database is **mcpdb**. The example commands in this procedure use **mcpdb** for the database name. If **mcpdb** is NOT the name of the database (the value for the db.neName parameter from the installprops.txt file), replace **mcpdb_0** with **<your db.neName>_0** in the command.

Procedure

1. Log on to the primary database server as a user with the DBA role.
2. Enter `cd /var/mcp/run/MCP_17.0/mcpdb_0/bin/util`.
3. Enter `./scheduleDBBackup.pl`.
4. Enter `E`.
5. Enter the time at which you want to perform the backup (hh:mm format).
6. Enter `Y` to schedule the backup.
7. Enter `Q` to quit.

Result

The backup is scheduled to occur at the specified time and will be stored in the /var/mcp/db/backup/latest folder. The backup file name will be in the format AUTO_dbBackup_on_mm-dd-yy.tar.gz.

The backup file from the previous scheduled automatic backup will be moved to the /var/mcp/db/backup/AUTO_history folder. If the /var/mcp/db/backup/latest folder contains a manual backup file, the manual backup file is moved to the /var/mcp/db/backup folder.

Note:

The /var/mcp/db/backup/AUTO_history folder can contain up to three scheduled backup files (that is, the three latest scheduled backup files).

Removing scheduled automatic database backups

Before you begin

- You are a user with the DBA role.
- You know the name of the scheduled database back up job you want to remove.

About this task

Use this procedure to remove a scheduled automatic backup job of the primary database (that is, change the status to `Not Scheduled`).

Note:

The default name for the database is **mcpdb**. The example commands in this procedure use **mcpdb** for the database name. If **mcpdb** is NOT the name of the database (the value for the db.neName parameter from the installprops.txt file), replace **mcpdb_0** with **<your db.neName>_0** in the command.

Procedure

1. Log on to the primary database server as a user with the DBA role.
2. Enter `cd /var/mcp/run/MCP_17.0/mcpdb_0/bin/util`.
3. Enter `./scheduleDBBackup.pl`.
4. Enter `D` to change the job status to `Not Configured`.
5. Enter `Y` to confirm the change.
6. Enter `Q` to quit.

Result

The system will no longer perform the automatic backup procedure.

Backing up an Avaya Media Server

This section provides the procedures that you perform to:

- back up an Avaya Media Server manually
- schedule an automatic backup of the Avaya Media Server
- remove scheduled automatic backups of an Avaya Media Server

Important:

Avaya recommends that you store backup data in a remote location to facilitate recovery in the event of a server failure.

Related topics:

Removing scheduled automatic database backups on page 501
Backing up an Avaya Media Server manually on page 502
Scheduling automatic backups on an Avaya Media Server on page 503

Backing up an Avaya Media Server manually

Before you begin

- You are a user with the BA or SSA role (for example, ntbackup and ntsysadm).
- You know the sudo password.
- You have root account privileges to access the backup files and log files.

About this task

Use this procedure to manually backup the data of an Avaya Media Server.

Procedure

1. Log on to the server as ntbackup or ntsysadm through SSH or an account with the BA or SSA role.
2. Enter `sudo msBackup.pl`.
3. Enter the sudo password.
4. Enter the password (if required).

Result

A backup summary report appears. The Avaya Media Server backup tool creates a backup file, and the message `Backup successfully completed` appears. The backup file name has the format msBackup_on_yyyy-mm-dd.tar. The backup file is stored in the /var/mcp/ma/MAS/platdata/EAM/Backups/latest folder.

The backup log file containing the summary report is stored in the /var/log/mas folder and has the default file name msBackup.log.yyyymmdd_hhmmss. You can view the backup log file when you are logged on to the server with root privileges.

The previous manual backup file was moved to the /var/mcp/ma/MAS/platdata/EAM/Backups folder. If the /var/mcp/ma/MAS/platdata/EAM/Backups/latest folder contained a scheduled automatic backup file, the automatic backup file is moved to the /var/mcp/ma/MAS/platdata/EAM/Backups/AUTO_history folder.

Note:

There is no limit on the number of manual backup files you can store in the /var/mcp/ma/MAS/platdata/EAM/Backups folder. However, you can have only one manual backup file for a given date. For example, if you perform two backups on the same day, the newest backup (for example, msBackup_on_2012-06-15.tar) overwrites the existing backup (msBackup_on_2012-06-15.tar) in the /var/mcp/ma/MAS/platdata/EAM/Backups/latest folder because the date (YYYY-MM-DD) in the backup file name matches.

Scheduling automatic backups on an Avaya Media Server

Before you begin

- You are a user with the SSA role (for example, ntbackup and ntsysadm).
- You have root account privileges to access the backup files and log files.

About this task

Use this procedure to schedule automatic backups for anAvaya Media Server .

Important:

Avaya recommends that you schedule backups for off-peak hours. The default backup time is 3:30 a.m.

Procedure

1. Log on to the server as ntbackup or ntsysadm through SSH or an account with the SSA role.
2. Enter `msScheduleBackup`.
3. Enter the password (if required).
4. Enter `E` to schedule a daily backup.
5. Enter the time at which you want to perform the backup (hh:mm format).
6. Enter `Y` to confirm.
7. Enter `Q` to quit.

Result

The backup is scheduled to occur at the specified time and will be stored in the /var/mcp/ma/MAS/platdata/EAM/Backups/latest folder. The backup file name will be in the format AUTO_msBackup_on_YYYY-MM-DD.tar.

A summary report of your activity is stored at /var/log/mas/msScheduleBackup.log.yyyymmdd_hhmmss. You can view the backup log file when you are logged on to the server with root privileges.

The backup file from the previous scheduled automatic backup will be moved to the /var/mcp/ma/MAS/platdata/EAM/Backups/AUTO_history folder. If the /var/mcp/ma/MAS/platdata/EAM/Backups/latest folder contains a manual backup file, the manual backup file is moved to the /var/mcp/ma/MAS/platdata/EAM/Backups folder.

Note:

The /var/mcp/ma/MAS/platdata/EAM/Backups/AUTO_history folder can contain up to two scheduled backup files (that is, the two latest scheduled backup files).

Removing scheduled automatic database backups

Before you begin

- You are a user with the DBA role.
- You know the name of the scheduled database back up job you want to remove.

About this task

Use this procedure to remove a scheduled automatic backup job of the primary database (that is, change the status to `Not Scheduled`).

Note:

The default name for the database is **mcpdb**. The example commands in this procedure use **mcpdb** for the database name. If **mcpdb** is NOT the name of the database (the value for the db.neName parameter from the installprops.txt file), replace **mcpdb_0** with **<your db.neName>_0** in the command.

Procedure

1. Log on to the primary database server as a user with the DBA role.
2. Enter `cd /var/mcp/run/MCP_17.0/mcpdb_0/bin/util`.
3. Enter `./scheduleDBBackup.pl`.
4. Enter `D` to change the job status to `Not Configured`.
5. Enter `Y` to confirm the change.
6. Enter `Q` to quit.

Result

The system will no longer perform the automatic backup procedure.

Backing up an Avaya Aura® Conferencing server

The Avaya Aura® Conferencing server backup job encompasses all the data required to restore an Avaya Aura® Conferencing server to its previous functionality in the event of a catastrophic failure.

The Avaya Aura® Conferencing server backup data includes multiple backup sets:

- platform
- application
- loads
- database (database backups) (if present)
- Avaya Media Server (if present)

Each of these backup sets will produce a separate tar file:

- mcpPlatform.<host name>.<date/time stamp>.tar
- mcpApp.<host name>.<date/time stamp>.tar
- mcpLoad.<host name>.<date/time stamp>.tar
- mcpDB.<host name>.<date/time stamp>.tar
- mcpMAS.<host name>.<date/time stamp>.tar
- mcpWCL.<host name>.<date/time stamp>.tar
- mcpSPIRIT.<host name>.<date/time stamp>.tar

Important:

Avaya recommends that you store backup data in a remote location to facilitate recovery in the event of a server failure.

To back up an Avaya Aura® Conferencing server, perform the following steps:

1. Back up the database (if present). (For more information, see Backing up the database on page 499.)
2. Back up the Avaya Media Server (if present). (For more information, see Backing up an Avaya Media Server on page 502.)
3. Back up the Avaya Aura® Conferencing server. You can back up the Avaya Aura® Conferencing server to:
   - a local folder. (For more information, see Backing up an server to a local folder on page 507.)
   - a remote server. (For more information, see Backing up an server to remote server on page 508.)
   - a USB drive. (For more information, see Backing up an server to a USB drive on page 509.)

Related topics:

Backing up an Avaya Aura Conferencing server to a local folder on page 507
Backing up an Avaya Aura Conferencing server to remote server on page 508
Backing up an Avaya Aura Conferencing server to a USB drive on page 509

Backing up an Avaya Aura® Conferencing server to a local folder

Before you begin

- You are a user with the BA or SSA role (for example, ntbackup and ntsysadm).
- You have cleaned up unneeded files from the server. For more information, see Removing unneeded loads from the Element Manager servers on page 516 and Removing unneeded installers of PostgreSQL from the Element Manager server on page 517.
- You have backed up the database if it is the primary database server. For more information, see Backing up the database on page 499.
- You have backed up the Avaya Media Server. For more information, see Backing up an Avaya Media Server on page 502.

About this task

Use this procedure to back up an Avaya Aura® Conferencing server to a local folder.

Procedure

1. Log on to the server using an account with the BA or SSA role.
2. Enter `bkupSvr -local`.
3. Enter the password (if required).

Result

After the backup is complete, a summary report displays the results of the backup. It is important for you to check the following items in the summary report:

- whether all backup sets completed successfully.
- the name and location of the tar file(s) produced.
- the name and location of the log file produced. If errors occurred, see the log file for more information.

The backup files are stored in the var/mcp/backup/local folder.

The backup log files have the file name format bkupsvr.log.yyyy_mm_dd.hh:mm:ss and are stored in one of the following folders:

- /home/ntsysadm/bkup_restore
- /home/ntbackup/bkup_restore

Backing up an Avaya Aura® Conferencing server to remote server

Before you begin

- You are a user with the BA or SSA role (for example, ntbackup and ntsysadm).
- You have cleaned up unneeded files from the server. For more information, see Removing unneeded loads from the Element Manager servers on page 516 and Removing unneeded installers of PostgreSQL from the Element Manager server on page 517.
- You have configured the remote backup parameters. For more information, see Configuring remote backup parameters on page 510.
- You have backed up the database if it is the primary database server. For more information, see Backing up the database on page 499.
- You have backed up the Avaya Media Server. For more information, see Backing up an Avaya Media Server on page 502.

About this task

Use this procedure to back up an Avaya Aura® Conferencing server to a remote server.

Procedure

1. Log on to the server using an account with the BA or SSA role.
2. Enter `bkupSvr -remote`.
3. Enter the password (if required).

Result

After the backup is complete, a summary report displays the results of the backup. It is important for you to check the following items in the summary report:

- whether all backup sets completed successfully.
- the name and location of the tar file(s) produced.
- the name and location of the log file produced. If errors occurred, see the log file for more information.

The backup files are stored in <IP address of remote server> ::/home/<name of user of remote server>/bkup folder.

The backup log files have the file name format bkupsvr.log.yyyy_mm_dd.hh:mm:ss and are stored in one of the following folders:

- /home/ntsysadm/bkup_restore
- /home/ntbackup/bkup_restore

Backing up an Avaya Aura® Conferencing server to a USB drive

Before you begin

- You are a user with the BA or SSA role (for example, ntbackup and ntsysadm).
- You inserted a USB drive into an available USB port.
- You have cleaned up unneeded files from the server. For more information, see Removing unneeded loads from the Element Manager servers on page 516 and Removing unneeded installers of PostgreSQL from the Element Manager server on page 517.
- You have backed up the database if it is the primary database server. For more information, see Backing up the database on page 499.
- You have backed up the Avaya Media Server. For more information, see Backing up an Avaya Media Server on page 502.

About this task

Use this procedure to back up an Avaya Aura® Conferencing server to a USB drive.

Note:

When you specify the `-usbdrive` command line parameter to the specified backup, the backup sets (tar files) are written to and read from the root directory of a locally attached USB storage device (for example, a hard drive or thumb drive). To avoid ambiguity, you can only attach one USB storage device. If you attach two or more USB storage devices, you receive an error, and the backup operation aborts.

Procedure

1. Log on to the server using an account with the BA or SSA role.
2. Enter `bkupSvr -usbdrive`.
3. Enter the password (if required).

Result

After the backup is complete, a summary report displays the results of the backup. It is important for you to check the following items in the summary report:

- whether all backup sets completed successfully.
- the name and location of the tar file(s) produced.
- the name and location of the log file produced. If errors occurred, see the log file for more information.

Configuring remote backup parameters

You must configure remote backup parameters before performing any of the following tasks:

- remote backup (that is, `bkupSvr -remote`)
- remote restore (that is, `restoreSvr -remote`)

The SSA role (ntsysadmm) can configure these remote backup parameters once. After the initial configuration, these parameters are saved and used in any future invocation of the remote backup command and remote restore command. If you change the remote parameters or generate a new SSH key (for example, for security reasons or after reinstalling), use the SSA role to run the configure (`configBkup`) script again to modify the parameters.

The following table displays the remote backup configuration parameters.

Parameter	Can be modified	Description
Remote operation	Y	If disabled, remote backup and remote restore is prohibited. If enabled, you must define the remote IP address and the remote “backup to” directory.
Remote SSH configuration	Y	If configured, the SSH keys were generated successfully for this particular job on the local machine and copied onto the target remote machine in the remote user's .ssh directory.
Remote server IP	Y	This is the IP address of the remote target backup server.
Remote userid	Y	This is the user ID on the remote target backup server. SSH keys will be added to ~userid/.ssh/ authorized_keys on the remote server. This user will become the owner of the backup tar file on the remote server.
Remote “backup to” directory	Y	This is the directory on the remote target backup server where the backup tar file is

		placed. This server must have sufficient storage available and be accessible by remote userid.
Backup sets	N	A backup job may contain more than one backup set. Each backup set produces one tar file and may contain more than one directory. Backup sets are predefined by Avaya.

Important:

When SSH keys are generated, the system prompts you for a pass phrase to protect the keys. The pass phrase is optional, but highly recommended if you are concerned about security. If you do not enter a pass phrase, the SSH keys are stored in clear text. If you enter a pass phrase, the SSH keys are encrypted. You will then use the pass phrase to decrypt the SSH keys at a later time. The pass phrase must meet the following criteria:

- consist of least six characters (space are permitted)
- contain a minimum of one uppercase character, one lowercase character, and one numeric character

No expiration time is assigned to the SSH keys, and the history of former pass phrases is not kept.

Related topics:

Enabling and configuring the remote backup configuration parameters on page 511
Disabling the remote backup configuration parameters on page 512
Configuring and verifying SSH keys on page 513
Cleaning up SSH keys on page 513
Setting the remote configuration backup parameters to the default values on page 514
Viewing the list of backup sets on page 515
Configuring individual remote backup parameters on page 515

Enabling and configuring the remote backup configuration parameters

Before you begin

- You are a user with the SSA role (for example, ntbackup and ntsysadm).
- You have a valid user ID on the remote backup server.

- You know the IP address of the remote backup server (in dot notation).
- You know the full path to the directory on the remote backup server to which you want to store the backup file.

About this task

Use this procedure to enable and configure the remote backup configuration parameters.

Procedure

1. Log on to the server as ntbackup or ntsysadm through SSH or an account with the SSA role.
2. Enter `configBkup`.
3. Enter the password (if required).
4. Enter `2` to schedule a daily backup.
5. Enter `Y` to confirm.
6. Enter the IP address of the backup server (in dot notation).
7. Enter the full path to the remote “backup to” directory.
8. Enter the userid to log on to the remote server
9. Enter the pass phrase.
10. Re-enter the pass phrase.
11. Enter the password for the userid of the remote server
12. Enter `7`.

Result

Communication with the backup server is established, and a result message appears.

Disabling the remote backup configuration parameters

Before you begin

You are a user with the SSA role (for example, ntbackup and ntsysadm).

About this task

Use this procedure to disable the remote backup configuration parameters.

Procedure

1. Log on to the server as ntbackup or ntsysadm through SSH or an account with the SSA role.

2. Enter `configBkup`.
3. Enter the password (if required).
4. Enter `2` to schedule a daily backup.
5. Enter `N` to confirm.
6. Enter `7`.

Result

The remote backup configuration parameters are disabled.

Configuring and verifying SSH keys

Before you begin

You are a user with the SSA role (for example, ntbackup and ntsysadm).

About this task

Use this procedure to set up, verify, and modify SSH keys.

Procedure

1. Log on to the server as ntbackup or ntsysadm through SSH or an account with the SSA role.
2. Enter `configBkup`.
3. Enter the password (if required).
4. Enter `3`.
5. Enter all required parameters.
6. Enter `7`.

Cleaning up SSH keys

Before you begin

You are a user with the SSA role (for example, ntbackup and ntsysadm).

About this task

Use this procedure to remove SSH keys.

Procedure

1. Log on to the server as ntbackup or ntsysadm through SSH or an account with the SSA role.
2. Enter `configBkup`.
3. Enter the password (if required).
4. Enter `4`.
5. Enter `Y`.
6. Enter `7`.

Result

The SSH keys are removed.

Setting the remote configuration backup parameters to the default values

Before you begin

You are a user with the SSA role (for example, ntbackup and ntsysadm).

About this task

Use this procedure to set the remote configuration backup parameters to the default values.

Procedure

1. Log on to the server as ntbackup or ntsysadm through SSH or an account with the SSA role.
2. Enter `configBkup`.
3. Enter the password (if required).
4. Enter `5`.
5. Enter `Y`.
6. Enter `7`.

Result

The remote configuration backup parameters are set to the default values.

Viewing the list of backup sets

Before you begin

You are a user with the SSA role (for example, ntbackup and ntsysadm).

About this task

Use this procedure to view the list of backup sets for the remote backup configuration parameters.

Procedure

1. Log on to the server as ntbackup or ntsysadm through SSH or an account with the SSA role.
2. Enter `configBkup`.
3. Enter the password (if required).
4. Enter `1`.

Result

The list of backup sets for the remote backup configuration parameters are displayed.

Configuring individual remote backup parameters

Note:

This section is optional because all of the major remote backup parameters are configured when you use the `configBkup` script.

When you configure the remote backup configuration parameters with the `configBkup` command, these settings are used for all backup jobs. If desired (for security or space reasons), you can use the following scripts to customize the remote backup configuration parameters for individual jobs:

- `configPlatformBkup`
- `configSvrBkup`
- `configFSIBkup`
- `configKPIBkup`
- `configSecLogArchive`

To use these scripts, you must be a user with the SSA role (for example, ntbackup and ntsysadm).

Removing unneeded loads from the Element Manager servers

Before you begin

- You are a user with the AA role (for example, ntappadm).
- You know the name of the load you want to remove.

About this task

Use this procedure to remove old and unneeded loads from the Element Manager servers. (During a backup, all existing loads are backed up as part of the Application backup set.)

Note:

The /var/mcp/loads folder should contain three or less loads. When an MR with multiple patch loads exists, keep the latest base/MR load and the latest associated patch load.

Important:

You must delete the loads from both the primary Element Manager and the secondary Element Manager simultaneously because the primary Element Manager and the secondary Element Manager monitor the loads. If the load is on one server but not on the other server, the Element Manager copies the loads back to the other Element Manager server.

Procedure

1. Log on to the primary Element Manager server using an account with the AA role (ntappadm).
2. In another window, log on to the secondary Element Manager server using an account with the AA role (ntappadm).
3. On the primary Element Manager server, enter `cd /var/mcp/loads`.
4. On the secondary Element Manager server, enter `cd /var/mcp/loads`.
5. On the primary Element Manager server, enter the following command, but do not press the **ENTER** key:`rm -rf <loadname>`.
6. On the secondary Element Manager server, enter the following command, but do not press the **ENTER** key:`rm -rf <loadname>`.

Comments? infodev@avaya.com

7. As close together as possible, press the **ENTER** key in both the primary Element Manager window and the secondary Element Manager window.

Result

The specified load is removed from the primary Element Manager server and the secondary Element Manager server.

Removing unneeded installers of PostgreSQL from the Element Manager server

Before you begin

- You are a user with the AA role (for example, ntappadm).
- You know the name of the installer you want to remove.

About this task

Use this procedure to remove old and unneeded installers of PostgreSQL from the Element Manager server with the primary database. (During a backup, all existing installers are backed up as part of the Application backup set.)

Note:

The file name format for installers of PostgreSQL is installer-mcp-postgresql-x.x.x-xx.LINUX64.zip.

Procedure

1. Log on to the Element Manager server with the primary database using an account with the AA role (ntappadm).
2. Enter `cd /var/mcp/media`.
3. Enter `rm –rf <filename>`.
4. Repeat Step 3 for each installer you want to remove.

Result

The specified installers of PostgreSQL are removed from the Element Manager server.

Backing up FSI data

A baseline is a snapshot of all the system files including their size and permissions. You can compare baselines from various times to determine what has changed over a given period of time. You should create baselines on a regular basis or if there are any significant changes to the system, such as an upgrade.

Related topics:

Creating an FSI baseline on page 518
Backing up FSI baselines to a local drive on page 519
Backing up FSI baselines to a remote server on page 519
Backing up FSI baselines to a USB drive on page 520

Creating an FSI baseline

Create an FSI baseline on a weekly basis or after any significant changes to the system, such as software installation or upgrade.

This task must be performed on all Element Manager servers and Avaya media servers.

Important:

It can take at least 10 minutes to create a typical baseline.

Before you begin

You are a user with the SSA role or a root user.

Procedure

1. Log on to the server as ntsysadm or an account with the SSA role.
2. Enter `fsibaseline`.
3. Enter the password (if required).
4. If you receive a warning, press any key to continue.
5. Enter `Y` to verify the new FSI baseline configuration.

Backing up FSI baselines to a local drive

Before you begin

- You are a user with the SSA role (for example, ntsysadm).
- You created an initial FSI baseline. For more information, see Creating an FSI baseline on page 518.

About this task

Use this procedure to back up FSI baselines to a local drive.

Procedure

1. Log on to the server using an account with the SSA role.
2. Enter `bkupFSI -local`.
3. Enter the password (if required).

Result

The FSI baseline is backed up.

Backing up FSI baselines to a remote server

Before you begin

- You are a user with the SSA role (for example, ntsysadm).
- You have configured the remote backup parameters. For more information, see Configuring remote backup parameters on page 510.
- You created an initial FSI baseline. For more information, see Creating an FSI baseline on page 518.

About this task

Use this procedure to back up FSI baselines to a remote server.

Procedure

1. Log on to the server using an account with the SSA role.
2. Enter `bkupFSI -remote`.
3. Enter the password (if required).

Result

The FSI baseline is backed up.

Backing up FSI baselines to a USB drive

Before you begin

- You are a user with the SSA role (for example, ntsysadm).
- You inserted a USB drive into an available USB port.
- You created an initial FSI baseline. For more information, see Creating an FSI baseline on page 518.

About this task

Use this procedure to back up FSI baselines to a USB drive.

Note:

When you specify the `-usbdrive` command line parameter to the specified backup, the backup sets (tar files) are written to and read from the root directory of a locally attached USB storage device (for example, a hard drive or thumb drive). To avoid ambiguity, you can only attach one USB storage device. If you attach two or more USB storage devices, you receive an error, and the backup operation aborts.

Procedure

1. Log on to the server using an account with the SSA role.
2. Enter `bkupFSI -usbdrive`.
3. Enter the password (if required).

Result

The FSI baseline is backed up.

Chapter 31: Restoring Avaya Aura® Conferencing

The complete restore of Avaya Aura® Conferencing consists of restoring the Avaya Aura® System Manager server and the Avaya Aura® Conferencing servers. To restore the entire Avaya Aura® Conferencing system, perform the following steps:

1. Restore the Avaya Aura® System Manager data. For more information, see *Administering Avaya Aura® System Manager.*
2. On every Avaya Aura® Conferencing server, restore the data. For more information, see Restoring an server on page 522.

Note:

- Avaya recommends that you create an FSI baseline after you completely restore the Avaya Aura® Conferencing server.
- There are optional restore jobs that operate on file system integrity (FSI) baseline snapshots. The FSI information is not restored if the server is lost and then restored using the `restoreSvr` command. In this case, the historical baseline data would not be useful.

Example 1: Restore of a co-resident redundant layout (EMserver1 and EMServer 2)

To restore this configuration, perform the following steps:

1. On each Avaya Aura® Conferencing server, perform an Avaya Aura® Conferencing server restore. (For more information, see Restoring an server on page 522.)
2. On EMServer1, perform the following steps:
    a. Restore the database. (For more information, see Restoring the database on page 525.)
    b. Restore the Avaya Media Server. (For more information, see Restoring an Avaya Media Server on page 528.)
3. On EMServer2, restore the Avaya Media Server. (For more information, see Restoring an Avaya Media Server on page 528.)

Example 2: Restore of a co-resident simplex layout (EMserver1)

To restore this configuration, perform the following steps on EMServer1:

1. Perform an Avaya Aura® Conferencing server restore. (For more information, see Restoring an server on page 522.)
2. Restore the database. (For more information, see Restoring the database on page 525.)
3. Restore the Avaya Media Server. (For more information, see Restoring an Avaya Media Server on page 528.)

Example 3: Restore of a standalone redundant layout (EMserver1, EMServer 2, WCserver1, WCserver2, and MS1Server1)

To restore this configuration, perform the following steps:

1. On each Avaya Aura® Conferencing server, perform an Avaya Aura® Conferencing server restore. (For more information, see Restoring an server on page 522.)
2. On EMServer1, restore the database. (For more information, see Restoring the database on page 525.)
3. On MS1Server1, restore the Avaya Media Server. (For more information, seeRestoring an Avaya Media Server on page 528 .)

Example 4: Restore of a standalone simplex layout (EMserver1, WCserver1, and MS1Server1)

To restore this configuration, perform the following steps:

1. On each Avaya Aura® Conferencing server, perform an Avaya Aura® Conferencing server restore. (For more information, see Restoring an server on page 522.)
2. On EMServer1, restore the database. (For more information, see Restoring the database on page 525.)
3. On MS1Server1, restore the Avaya Media Server. (For more information, see Restoring an Avaya Media Server on page 528.)

Restoring an Avaya Aura® Conferencing server

The restore of a server's operating system and configuration data (that is, “server” data) consists of re-installing and commissioning the server and utilizing the previously backed up server configuration data to restore the server. For instructions on installation and commissioning an Avaya Aura® Conferencing server, see *Deploying Avaya Aura® Conferencing 7.2*.

Important:

The information stored for a particular server is specific to that server. Do not use administration data (or any Platform data or Application data) for a server other than the server from which the data was originally backed up.

This chapter contains the details regarding the execution of the `restoreSvr` script, which restores the server data. This server data includes the Avaya Aura® Conferencing data for

EMServer1 and the backups of the database for the server hosting both database applications.

You must re-install and commission all servers with the Platform data used as the remote administration date.

You can restore from:

- a local drive. (For more information, see Restoring an server from a local drive on page 523.)
- a USB drive. (For more information, see Restoring an server from a USB drive on page 525.)
- a remote disk. (For more information, see Restoring an server from a remote disk on page 524.)

Related topics:

Restoring an Avaya Aura Conferencing server from a local drive on page 523
Restoring an Avaya Aura Conferencing server from a remote disk on page 524
Restoring an Avaya Aura Conferencing server from a USB drive on page 525

Restoring an Avaya Aura® Conferencing server from a local drive

Before you begin

- You are a user with the SSA role (for example, ntsysadm).
- You have all of the required tar.gz files for restore in /var/mcp/backup/local.

About this task

Use this procedure to restore an Avaya Aura® Conferencing server from a local drive.

Procedure

1. Log on to the server using an account with the SSA role through SSH.
2. Enter `restoreSvr -local`.
3. Enter the password (if required).
4. Enter the appropriate number to select a restore tar.gz file from the list.
5. Enter `Y`.
6. Repeat Steps 4 and 5 as necessary.

Result

A summary of the restore results appears.

Restoring an Avaya Aura® Conferencing server from a remote disk

Before you begin

- You are a user with the SSA role (for example, ntsysadm).
- SSH is installed and running on the remote machine, and the server data was backed up successfully.

About this task

Use this procedure to restore an Avaya Aura® Conferencing server from a remote disk.

The restore script uses the previously configured backup parameters to identify the following information:

- IP address of the remote backup server
- folder on the remote backup server where the backup tar.gz files are located
- username to use for remote SSH commands
- previously generated SSH keys

Note:

You will probably need to regenerate the SSH keys used for remote backup/restore operations. For more information, see Configuring remote backup parameters on page 510.

Procedure

1. Log on to the server using an account with the SSA role through SSH.
2. Enter `restoreSvr -remote`.
3. Enter the pass phrase for SvrBkup Job identity.
4. Enter the appropriate number to select a restore tar.gz file from the list.
5. Enter `Y`.
6. Repeat Steps 4 and 5 as necessary.

Result

A summary of the restore results appears. To check the logs mentioned in the summary report, you must log on with root privileges.

Important:

Ensure that the restore operation was successful.

Restoring an Avaya Aura® Conferencing server from a USB drive

Before you begin

- You are a user with the SSA role (for example, ntsysadm).
- You inserted a USB drive into an available USB port.

About this task

Use this procedure to restore an Avaya Aura® Conferencing server from a USB drive.

Note:

When you specify the `-usbdrive` command line parameter to the specified restore, the backup sets (tar files) are read from the root directory of a locally attached USB storage device (for example, a hard drive or thumb drive). To avoid ambiguity, you can only attach one USB storage device. If you attach two or more USB storage devices, you receive an error, and the backup operation aborts.

Procedure

1. Log on to the server using an account with the SSA role through SSH.
2. Enter `restoreSvr -usbdrive`.
3. Enter the password (if required).
4. Enter the appropriate number to select a restore tar.gz file from the list.
5. Enter `Y`.
6. Repeat Steps 4 and 5 as necessary.

Result

A summary of the restore results appears.

Restoring the database

You can recover the database using one of the following methods:

- resyncing either the primary database or the secondary database that has failed with the other remaining complementary database (secondary or primary, respectively). This is the normal method of recovery when the server has been lost.
- restoring a previous backup of the database. This method is used when one of the following conditions exists:

- both the primary database and the secondary database have been lost
- data has been deleted by accident from a replicated system

The following scenarios pertain to **replicated databases**:

- To recover only the primary database (that is, use the existing secondary database to repopulate the primary database). Follow the procedure “Resyncing the database in *Deploying Avaya Aura® Conferencing 7.2* to resync the database from secondary to primary.
- To recover only the secondary database (that is, use the existing primary database to repopulate the secondary database). Follow the procedure “Resyncing the database in *Deploying Avaya Aura® Conferencing 7.2* to resync the database from secondary to primary.
- To restore the contents of the database as it existed on a certain date. See Restoring the primary database from a backup file on page 526 to restore the data from a previous database backup file.
- If both the primary and secondary databases have been lost, you must also restore the data from a backup file. Follow the procedure Restoring the primary database from a backup file on page 526 and then resync the database from primary to secondary. For more information, see “Resyncing the database” in *Deploying Avaya Aura® Conferencing 7.2* to resync the database from secondary to primary.

For **non-replicated databases**, you must restore the database from a backup file. Follow the procedure Restoring the primary database from a backup file on page 526.

Note:

If the data/backup you want to restore was taken as part of a failed software update (such as MCP_17.1.0.0_2013-06-15-2100 to MCP_17.1.0.0_2013-06-30-2100), follow the procedure “Downgrading a system” in *Deploying Avaya Aura® Conferencing 7.2*.

Related topics:

Restoring the primary database from a backup file on page 526

Restoring the primary database from a backup file

Before you begin

- You are a user with the DBA role (for example, ntdbadm).
- You have the backup file in one of the following folders:
  - /var/mcp/db/backup
  - /var/mcp/db/backup/latest
  - /var/mcp/db/backup/AUTO_history

- The primary Element Manager server has the load (in the /var/mcp/loads folder) that matches the database backup that you want to restore.
- The Avaya Aura® Conferencing software load currently running was also the load that was running when the backup was created.
- The database is installed already on the server(s) hosting the database. For more information, see *Deploying Avaya Aura® Conferencing 7.2* to reinstall the database software on all the servers hosting the database.

Important:

If the Avaya Aura® Conferencing software load currently running is not the load that was running when the backup was created, you must downgrade the system. Follow the instructions in “Downgrading a system” in *Deploying Avaya Aura® Conferencing 7.2* before restoring the primary database from a backup file.

About this task

Use this procedure to restore the primary database from a backup file.

Important:

This procedure can cause possible loss of data and interruption of service. Only trained personnel should perform this procedure.

Note:

Before performing this procedure, keep in mind the following information:

- During this process, all network components will be connected to the secondary database. As a result, the database will be in read-only mode. Databases writes will not be permitted.
- If the backup file you want to restore is stored in a remote location, retrieve that backup file and place it in the /var/mcp/db/backup folder. If needed, you can restore the database backup from the server backup.

Procedure

1. Log on to the server that hosts the primary database using an account with the DBA role (ntdbadm).
2. Enter `cd /var/mcp/run/MCP_17.0/mcpdb_0/bin/util ./dbRestore.pl <backupName>`where `<backupName>` is the name of the tar.gz file (with or without the tar.gz extension).

   Note:

   If `mcpdb` is NOT the name of the database (the value for the db.neName parameter from the installprops.txt file), replace `mcpdb_0` with `<your db.neName>_0` in the command.

Note:

Ignore all of the compiler warning messages. These messages are not service affecting.

3. If the database is set up in a redundant configuration, follow the procedure in "Resyncing the database" in *Deploying Avaya Aura® Conferencing 7.2* to resync the database from primary to secondary.
4. Restart all Network Elements so they will be in sync with the data in the restored database.

Result

The database is restored.

Restoring an Avaya Media Server

Before you begin

- You are a user with the SSA role (for example, ntsysadm).
- Element Manager Console is available.
- You have a local administrator logon (that is, admin, admin1, admin2, admin3, admin4, or admin5) on Element Manager Console.
- You have the Avaya Media Server backup file in one of the following folders:
  - /var/mcp/ma/MAS/platdata/EAM/Backups
  - /var/mcp/ma/MAS/platdata/EAM/Backups/latest
  - /var/mcp/ma/MAS/platdata/EAM/Backups/AUTO_history
- You know which Avaya Media Server network element is running on the Avaya Media Server.
- The Avaya Media Server is installed already on the server(s). For more information, see *Deploying Avaya Aura® Conferencing 7.2* to install the Avaya Media Server. The Avaya Media Server software load currently running must be the same software load that was running when the backup was created.

About this task

Use this procedure to restore an Avaya Media Server.

Procedure

1. Log on to Element Manager Console locally.
2. In Element Manager Console, stop the Avaya Media Server network element.

3. Log off Element Manager Console.
4. Log on to the Avaya Media Server A server as ntsysadm or an account with the SSA role.
5. Enter `msRestore`.
6. Enter the password (if required).
7. Enter the number for the appropriate Avaya Media Server backup tar file.
8. Enter `Y`.
9. Log on to Element Manager Console locally.
10. In Element Manager Console, start the Avaya Media Server network element.

Result

The Avaya Media Server is restored.

Restoring FSI data

Restoring FSI baselines from a local drive

Before you begin

You are a user with the SSA role (for example, ntsysadm).

About this task

Use this procedure to restore FSI baselines from a local drive.

Procedure

1. Log on to the server using ntsysadm or an account with the SSA role.
2. Enter `restoreFSI -local`.
3. Enter the password (if required).
4. Enter the number for the appropriate backup file.
5. Enter `Y`.

Result

The FSI baseline is restored.

Restoring FSI baselines from a remote server

Before you begin

- You are a user with the SSA role (for example, ntsysadm).
- SSH is installed and running on the remote machine, and the server data was backed up successfully.

About this task

Use this procedure to restore FSI baselines from a remote server.

Procedure

1. Log on to the server using ntsysadm or an account with the SSA role.
2. Enter `restoreFSI -remote`.
3. Enter the password (if required).
4. Enter the number for the appropriate backup file.
5. Enter `Y`.

Result

The FSI baseline is restored.

Restoring FSI baselines from a USB drive

Before you begin

- You are a user with the SSA role (for example, ntsysadm).
- You inserted a USB drive into an available USB port.

About this task

Use this procedure to restore FSI baselines from a USB drive.

Note:

When you specify the `-usbdrive` command line parameter to the specified restore, the backup sets (tar files) are read from the root directory of a locally attached USB storage device (for example, a hard drive or thumb drive). To avoid ambiguity, you can only attach one USB storage device. If you attach two or more USB storage devices, you receive an error, and the backup operation aborts.

Procedure

1. Log on to the server using ntsysadm or an account with the SSA role.
2. Enter `restoreFSI -usbdrive`.
3. Enter the password (if required).
4. Enter the number for the appropriate backup file.
5. Enter `Y`.

Result

The FSI baseline is restored.

Chapter 32: Uninstalling software

Introduction to uninstalling software

The mcpInstaller script is used for new Avaya Aura® Conferencing installations only. If you need to reinstall or upgrade, use the procedures in this chapter to undeploy and uninstall current applications prior to running the mcpInstaller script.

Important:

After you have uninstalled the current applications, start the mcpInstaller script and select no at the prompt to resume from a previous installation. You must start from the beginning of the script.

Checklist for uninstalling Application Server software

The following checklist provides the workflow for uninstalling the Application Server software.

Table 48: Workflow for uninstalling the Application Server software

#	Task	Description	Notes	✔
1	Stop and undeploy all network element instances except for Element Manager instances.	See Stopping and undeploying a network element instance on page 534.		
2	Undeploy Element Manager.	See Stopping and undeploying Element Manager on page 534.		
3	Cleanup the Application Server database or Uninstall the Application Server.	See Cleaning up the Application Server database on page 535 or Uninstalling the		

#	Task	Description	Notes	✔
		database software on page 535 if a reinstallation is required.		

Stopping and undeploying a network element instance

About this task

Stop and undeploy a network element instance.

Procedure

1. In the navigation pane of the Element Manager Console, click **Feature Server Elements**, and select the <NE Type> and <NE> for the instance you want to stop. For example, to stop a Media Server network element instance, click **Media Servers and Clusters** > **Media Servers** and select the <Media Server NE> for the instance you want to stop.
2. Click **NE Maintenance**.
3. In the Maintenance dialog box, select the row for ID 0, and click **Stop**.
4. In the Maintenance dialog box, select the row for ID 1 (if it exists), and click **Stop**.
5. After the stop operation completes, select the row for ID 0, and click **Undeploy**.
6. Select the row for ID 1 (if it exists), and click **Undeploy**.

Stopping and undeploying Element Manager

Before you begin

If you have a secondary Element Manager, you must stop and undeploy from the Element Manager console.

About this task

Stop and undeploy the primary Element Manager.

Procedure

1. Log on to EMServer0 as `ntappadm` through ssh or directly at the server console.

2. Type `emUndeploy.pl`, and press **Enter**.
3. Type **y** to all prompts, and press **Enter**.

Result

The Element Manager instance 0 is now stopped and uninstalled.

Cleaning up the Application Server database

Before you begin

All Network Element instances must be stopped.

About this task

Cleanup the Application Server database.

Procedure

1. Log on to EMServer0 as ntappadm through ssh.
2. Type `dbUninstall.pl`, and press **Enter**.
3. Type `y` to all prompts, and press **Enter**.

Result

The Application Server database has been cleaned.

Uninstalling the database software

Uninstalling the database software is not usually necessary. A clean up of the database is generally sufficient.

Before you begin

Stop and undeploy all network element instances.

About this task

Use this procedure to uninstall the database software if a complete reinstallation of the software is required.

Procedure

1. Log on to EMServer0 as `ntappadm` through ssh.

2. Type `cd /var/mcp/install`, and press **Enter**.
3. Type `./mcpDbSwUninstall.pl –primary`, and press **Enter**.
4. Type `y` to all prompts, and press **Enter**.
5. For co-resident with redundancy and standalone with redundancy deployment types (non-simplex), type `./mcpDbSwUninstall.pl –secondary`, and press **Enter**.
6. Type `y` to all prompts, and press **Enter**.

Result

The application database software is uninstalled.

Checklist for uninstalling the Avaya Media Server software

The following checklist provide the workflow for uninstalling the Avaya Media Server software.

Table 49: Workflow for uninstalling the Avaya Media Server software

#	Task	Description	Notes	✔
1	Stop and undeploy the Media Server instances.	See Stopping a Network Element instance on page 472.		
2	Uninstall the Media Server software.	See Uninstalling the on page 536.		

Uninstalling the Avaya Media Server

Before you begin

Stop and undeploy the Media Server network elements.

About this task

Uninstall the Avaya Media Server software.

Procedure

1. Log on to `ntsysadm` through ssh or directly at the server console.

2. Enter **su -** to log on as root.
3. Type `mcpMsUninstall.pl`, and press **Enter**.
4. At the prompt to `Continue uninstall?`, type `y`, and press **Enter**.

Result

The message `Uninstall completed SUCCESSFULLY` appears. The Avaya Media Server software is now uninstalled.

Appendix A: Shutting down and starting the Avaya Aura® Conferencing system

Shutting down the Avaya Aura® Conferencing system

About this task

Use the following procedure to shut down the Avaya Aura® Conferencing system.

Procedure

1. Log on to the Element Manager Console using an account with admin privileges.
2. Stop all network element instances except for the primary Element Manager instance (EM_0).

   For more information about stopping network elements, see the procedure for stopping a network element instance.
3. Log on to the EM_0 server as ntappadm to stop the primary network element instance for EM_0.
   a. Type `cd /var/mcp/install`, and press **Enter**.
   b. Type `./emStop.pl`.
4. Log on to the primary database server as `ntsysadm` or an account with the SSA role through ssh or directly on the server console to stop the database and replication.
   a. Type `stopDB`, and press **Enter**.
   b. If prompted, type the password for the SSA account.
   c. Type `stopRep`, and press **Enter**.
5. Power off the server.

Starting the Avaya Aura® Conferencing system after a shutdown

Before you begin

The servers must be powered up.

About this task

Use the following procedure to start the Avaya Aura® Conferencing system after a shutdown.

Note:

To determine the current status of the database, on the command line, log on as `ntsysadm`, and type `statusOfDB`.

Procedure

1. If the secondary database was stopped, log on to the secondary database server (EMServer2), as `ntsysadm` or an account with the SSA role through ssh or directly on the server console.
   a. Type `startRep` to start replication, and press **Enter**.
   b. Type `startDB` to start the database, and press **Enter**.
2. If the primary database was stopped, log on to the primary database server (EMServer1), as `ntsysadm` or an account with the SSA role through ssh or directly on the server console.
   a. Type `startRep` to start replication, and press **Enter**.
   b. Type `startDB` to start the database, and press **Enter**.
3. Log on to the primary Element Manager (EMServer1) hosting Element Manager instance 0 (EM_0) as `ntappadm` or an account with the AA role through ssh or directly on the server console.
   a. Type `cd /var/mcp/install`, and press **Enter**.
   b. Type `./emStart.pl`, and press **Enter**.
4. From the Element Manager Console, start all network element instances.
   For more information about starting network elements, see the chapter for Deploying and starting the remaining Network Elements.

Comments? infodev@avaya.com

Appendix B: Migrating existing data to Avaya Aura Conferencing 7.2

Introduction to migrating your data

This appendix describes the process for installing the data migration tool and migrating your Avaya Aura® Conferencing 6.0 or Meeting Exchange 5.2 data to Avaya Aura® Conferencing 7.2.

If you are upgrading from Avaya Aura® Conferencing 6.0 or Meeting Exchange 5.2, you can repurpose your Dell™ PowerEdge™ R610 or IBM S8800 to use Avaya Aura® Conferencing 7.2 for a co-resident with redundancy or a co-resident simplex layout configuration.

Note:

A separate WebLM server is required if you want to maintain your current Meeting Exchange or Avaya Aura® Conferencing license while adding a new Avaya Aura® Conferencing 7.2 license.

Installing the data migration tool

The data migration tool is a Windows desktop application that runs under Windows XP or the Windows 7 Operating System.

Before you begin

- Windows XP or Windows 7 Operating System is installed.
- The minimum hardware requirements are met.
- Microsoft .NET Framework 4 Client Profile is installed on the target server.

About this task

Use the following procedure to install the data migration tool to your PC.

Procedure

1. Insert the CD containing the AAC Data Migration Tool 1.0.15.msi installer.

2. Double-click **AAC Data Migration Tool 1.0.15.msi** to start the installation.

   Note:

   If an older version of the installer already exists, you must remove it before continuing.

3. At the Welcome to the Avaya AAC Data Migration Tool Setup Wizard screen, click **Next**.
4. At the Select Installation Folder screen, click **Browse** to install the software to another folder.
5. Click **Just me** to ensure that the Data Migration Tool can only be used by you on this computer or click **Everyone** to allow anyone who uses this computer to use this tool.
6. Click **Next** to continue or to accept the default folder location.
7. At the Confirm Installation screen, click **Next.**
   After the installation completes, you see the message Avaya AAC Data Migration Tool has been successfully installed.
8. Click **Close**.

Next steps

Proceed to Exporting data from 5.2 or 6.0 on page 542.

Exporting data from Meeting Exchange 5.2 or Avaya Aura® Conferencing 6.0

Before you begin

- You have a Dell™ PowerEdge™ R610 server or an IBM S8800 server running Meeting Exchange 5.2.
- You have either the Windows XP or Windows 7 Operating System installed.
- Obtain the SQL Server Database credentials for your Meeting Exchange 5.2 system
- Obtain the user name and password for the Avaya Aura® Conferencing system.

About this task

Use the following procedure to export your existing data from Meeting Exchange 5.2 or Avaya Aura® Conferencing 6.0 to Avaya Aura® Conferencing 7.2.

Procedure

1. Click the **Start** menu, and select **Programs** > **Avaya** > **AAC Data Migration Tool**.
2. In the Welcome window, click **Export**.
3. In the Export dialog box, in the CRS server section, complete the following:
   - **Host name or IP address**: Type the hostname or IP address of the SQL server where the CRS database resides.
   - **Database username**: Type **sa**
   - **Database password**: Type the password that you configured during installation.
4. Click **Test Connection**.
5. In the Storage section, click the ellipsis (...) to specify a location to save your data.

   Note:

   Your exported data is backed up using the file name mxbackup.xml.
6. Click **Export**.
7. Click **Back to Main** to return to the main window.

Next steps

Install Avaya Aura® Conferencing 7.2, see Introduction to software installation on page 113 and then proceed to importing the user data to System Manager.

Checking connection between Avaya Aura® Conferencing and System Manager

For a successful import of the User information to System Manager, you need to verify that the Avaya Aura® Conferencing server is connected to System Manager.

About this task

Use this procedure to ensure there is a connection between Avaya Aura® Conferencing and Avaya Aura® System Manager prior to importing the data to System Manager.

Procedure

1. Log on to System Manager as admin.

2. On the System Manager console, click **Elements** > **Session Manager**.
3. In the navigation pane, click **System Status** > **SIP Entity Monitoring**.
4. In the All Monitored SIP Entities section, verify that your Avaya Aura® Conferencing server is visible.
5. Click **Log off**.

Importing data from Meeting Exchange 5.2 or Avaya Aura® Conferencing 6.0

The import process involves the following:

- Defines a Session Manager name and location.
- Defines a domain which is appended to the qualified username for Avaya Aura® Conferencing, for example, user1@domain.com.
- Imports Meeting Exchange conference data into Avaya Aura® Conferencing profiles.
- Prepares an XML file containing user information and imports users to System Manager using the System Manager bulk import process.
- Assigns system profiles for users, assigns participant codes, and moderator codes.

Before you begin

- You have exported the data from Meeting Exchange 5.2 or Avaya Aura® Conferencing 6.0.
- You have installed Avaya Aura® Conferencing 7.2.
- You have checked to ensure Avaya Aura® Conferencing is connected to the System Manager.

For more information, see Checking connection between and on page 543.

About this task

Warning:

If the Meeting Exchange or Avaya Aura® Conferencing 6.0 data contains duplication, conference names that are greater than 30 characters, or non-recognizable symbols, the Data Migration Tool applies the following changes:

- Duplicate entries where a combination of Participants and Dial Out is not unique are removed. All clients that reference duplicate conferences are changed to reference only one conference.
- Only alphanumeric data and the underscore (_) symbols are recognized. All other symbols are replaced with an underscore (_).
- Conference names are truncated at 30 characters.
- Duplicate user names are automatically corrected by appending a number to the name during the import process.
- Duplicate conference names are automatically corrected by appending a _renamed to the name during the import process.

Use the following procedure to import the Meeting Exchange 5.2 or Avaya Aura® Conferencing 6.0 data that you previously exported.

Procedure

1. Click the **Start** menu, and select **Programs** > **Avaya** > **AAC Data Migration Tool**.
2. In the Welcome window, click **Import**.
3. In the Import dialog box, in the AAC 7.0 Server section, complete the following:
   - **Host name or IP address**: Type the hostname or IP address of the Avaya Aura® Conferencing Provisioning (PROV) client.
   - **Username**: Type **admin**.
   - **Password**: Type the admin password.
4. Click **Test Connection**.
   If the connection is established, the message Connected OK appears immediately below the Test Connection button.
5. In the Storage section, click the ellipsis (...) to specify a location to save your Avaya Aura® Conferencing 6.0 or Meeting Exchange 5.2 data.
6. Click **Import**.
7. In the Specify Session Manager and Location dialog box, complete the following:
   - **Session Manager**: Type the Session Manager name used for Avaya Aura® Conferencing as specified in System Manager.
   - **Location**: Type a location for Session Manager.
8. Click **Next**.
9. In the Specify Domain name dialog box, complete the following:
   - **Domain Name**: Select a domain from the list.
   - **Time Zone**: Select a time zone from the list.

   If a domain name does not exist, complete the following:

- Select the **Specify Domain Name** check box if the domain name is not listed.
- **Domain name**: Type a domain name.
- **Time Zone**: Select a time zone from the list.

The domain name is used to create qualified user names for Avaya Aura® Conferencing. For example, user1@domain.com.

10. Click **Next**.
11. The Create Conferencing Profiles window appears with the Avaya Aura® Conferencing 6.0 Conference Names in the left pane and the Avaya Aura® Conferencing 7.0 Conferencing Profiles in the right pane. Click **Validate Data** prior to importing the data into Avaya Aura® Conferencing to check for duplicate names or invalid characters in names.
    The Validating Conference data window appears with the following message:
    ```
    The Data Migration Tool will attempt to apply the following rules
    automatically: Create conferencing profiles based on combination of Number
    of Participants and DialOut Enabled fields. Replace any special characters
    in conferencing profile names. You will be prompted to provide a
    replacement pattern. Truncate conferencing profile names where the length
    exceeds 30 characters. Correct duplicate conferencing profile names by
    adding a number at the end of the names. Do you wish to proceed?
    ```
12. In the Validating data dialog box, click **Yes** to proceed with data validation.
13. If an invalid special character is found, the Define replacement pattern dialog box appears. In the **Enter replacement pattern here** field, type a character that replaces the invalid special character, for example, underscore (_), and click **OK**.

    Warning:

    Invalid characters are automatically replaced with the pattern you provide.
14. In the Validating Conference data dialog box, at the message Conference validation complete, click **Close**.
    On the Import Conferences window, the bulk of the data moved to the right pane. If the original conference name changed, the comment field contains the change. Conference names with the word _renamed appended to the name are names that contained parameter duplication with other conferences. The renamed conference is updated in the user records to ensure the user references the correct conference. After duplicate conferences are found and removed, users reference only one instance of the conference.
15. On the Validating data dialog box, click **OK**.
16. The Create Conferencing Profiles window appears with the remaining Avaya Aura® Conferencing 6.0 Conference Names in the left pane and the Avaya Aura® Conferencing Conferencing Profiles in the right pane. Double-click a field to edit duplicate names or invalid characters.

    All fields can be edited, except for the Comment field.

17. Click **Validate Data**, and click **Yes** to proceed with data validation.
    The Validating Conference Data window appears.
18. Click **Close** when the `Client validation complete` message appears.
19. Click **OK**.
20. On the Import Conferences dialog box, if any duplicated conferences are found, they are renamed but not imported. You can manually import these conferences. Select the conferences in the left pane, and click **Import Selected** or **Import All**. The conferences on the left pane are moved to the right pane.
21. Click **Close**.
22. If conferences remain in the left pane, a message appears to identify conferences not imported. Click **Yes** to skip to the user import and proceed to the next step or click **No** to continue with conference import.
23. The Load System manager user accounts dialog box appears, click the **ellipsis (...)** to browse to the folder containing the System Manager user account information.

    Note:

    This is the path containing the stored set of XML files that were created when exporting users from System Manager.
24. On the User Accounts dialog box, click **Yes** and skip mapping to System Manager Accounts or **No** to perform a manual association.
25. If you selected no, the Select System Manager Account dialog box appears, double-click on a user account to manually perform user association, and click **OK**.
26. In the **Search** field, type a name or part of a name, surname, or email.

    Note:

    The search is case sensitive and display any matches as you type.
27. Select an account, and click **OK**.

    Note:

    If preparing an XML file for import, if the Meeting Exchange or Avaya Aura® Conferencing 6.0 user has a System Manager account associated with it then the System Manager user account information is updated with the conferencing profile from Meeting Exchange or Avaya Aura® Conferencing 6.0 and saved to the XML file.

    If there is a matching System Manager account, the following fields (in bold type) are updated:

    <commProfile xsi:type="ns9:MmcsCommProfileType" xmlns:ns9="http://xml.avaya.com/schema/import_mmcs">

    <**ns9:template**> </**ns9:template**>

<**ns9:securityCode**> </**ns9:securityCode**>

<**ns9:moderatorPin**> </**ns9:moderatorPin**>

<commProfile>

If there is no matching System Manager account, only the following fields (in bold) are updated:

<commProfile xsi:type="ns6:SessionManagerCommProfXML"mlns:ns6="http://xml.avaya.com/schema/import_sessionmanager>

<**ns6:primarySM**> </**ns6:primarySM**>

<**ns6:homeLocation**> </ **ns6:homeLocation**>

</commProfile>

<handle>

<**handleName**> </**handleName**>

<**domainName**> </**domainName**>

</handle>

Save the user data in an XML file based on the template XML file. You can save selected records or save all records to an XML file for System Manager.

28. On the Save As dialog box, type a name for the file such as BulkImport.xml and navigate to a location to save the file, and click **Save**.
    The Preparing Bulk Import file for System Manager window appears and indicates the number of clients that successfully saved.
29. Click **Close**.
30. Verify that there is a connection between Avaya Aura® Conferencing and System Manager prior to importing the data to System Manager, see Checking connection between and on page 543.
31. Log on to System Manager as admin to import the BulkImport.xml file into System Manager.

    Note:

    For more information about using the Bulk Import and Export, see *Administering Avaya Aura® System Manager*.
32. On the System Manager console, click **Services** > **Bulk Import and Export**.
33. In the navigation pane, click **Import** > **User Management** > **Users**.
34. On the Import users dialog box, in the File selection section, click **Browse**.
35. Select the BulkImport.xml file that you previously saved.
    You can monitor the status in the Manage job section.
36. Upon successful completion, return to the AAC Data Migration Tool.
37. On the System Manager Bulk Import Users dialog box, click **OK**.

38. Click **Assign Selected** or **Assign All**, to assign System Profile, Participant, and Moderator codes for the users.
39. Click **Close**.
40. Click **Back to Main** to return to the main window.
41. Exit the application.
    A Web browser window automatically opens and the log file containing the details of the data manipulations is saved in HTML format.

Result

The import is complete.

Appendix C: Re-IPing the Application Server

Introduction to re-IPing the Avaya Aura® Conferencing servers

This appendix provides the procedures to change the IP address on the Avaya Aura® Conferencing (AAC) 7.2 system. Avaya recommends that you use the job aid worksheet to assist in gathering your data and planning your systems for the re-IP process. For more information, see the Microsoft Excel job aid, *AAC 7.0 ReIP Job Aid.xlsm* at http://support.avaya.com.

Prerequisites

- Examine the system certificates to determine if new certificates are required.

  Important:

  Network elements require a new certificate if the certificate currently in use contains the old IP address or host name as the Subject AltName or the Common Name. If you want to update any other information, a new certificate is optional. However, Avaya recommends that you obtain a new certificate to keep your certificate information current.

- Obtain and install new certificates.

Preparing your data for re-IP

The job aid worksheet has the following three tabs:

- Server Data: Enter the old and new information for each server in the system that requires a re-IP
- Application Data: Populate all the old and new IP addresses in the system.
- Role Data: Capture all the user information for server access and administration information for each server in the system requiring a re-IP.

Related topics:

Preparing server data on page 552

Preparing application data on page 553
Preparing role data on page 555

Preparing server data

About this task

Use the following procedure to populate the server data for all servers undergoing an IP address change.

Procedure

1. Open the job aid worksheet, *AAC 7.0 reIP Job Aid.xlsm*, and click the **Server Data** tab.
2. If the hostname changes, type the Old Hostname and the New Hostname.
3. In the Internal OAM (Default) section, complete the following:
   a. Old IP address and the New IP address
   b. Old Subnet Prefix length and the New Subnet Prefix length (if the network prefix is different)
   c. Old Subnet Default Router and the New Subnet Default Router (if the default Gateway is different).

   Note:

   For co-resident with redundancy or co-resident simplex layouts where the Avaya Media Server components are co-resident with the Application Server components and the Media IP address is undergoing a re-IP, see Step 4 on page 552.
4. In the Media section, complete the following:
   a. Old IP address and the New IP address.
   b. Old Subnet Prefix length and the New Subnet Prefix length.
   c. Old Subnet Default Router and the New Subnet Default Router.
5. In the EM server section for EMServer1 and EMServer2, complete the following:
   a. Old External clock Source #1 and New External Clock Source #1.
   b. Old External clock Source #2 and New External Clock Source #2 (if applicable).
   c. Old Secondary Clock Source and New Secondary Clock Source.
6. In the NE Server section, complete the following:
   a. Old Primary Clock Source and New Primary Clock Source.
   b. Old Secondary Clock Source and New Secondary Clock Source.

Note:

If you have additional Network Element (NE) servers, copy and paste a new row in the spreadsheet.

If the EMServer1 and EMServer2 IP addresses changed and the network element server undergoing a reIP uses the Element Manager server IP address as the NTP source, then you must update the NTP configuration of the network element server to use the new EMServer1 and EMServer2 IP addresses when updating your network configuration. For more information, see Updating the hostname and clock source on page 560.

Next steps

Proceed to Preparing application data.

Preparing application data

About this task

Use the following procedure to populate the application data for all servers that are undergoing a re-IP.

Procedure

1. Open the job aid worksheet, *AAC 7.0 ReIP Job Aid.xlsm*.
2. Click the **Server Data** tab, and copy the Old IP address and New IP address data to the following cells on the **Application Data** tab.
   a. Old IP address
   b. New IP address
3. If Network Element (NE) service addresses change, perform the following:
   a. Log on to the Element Manager Console.
   b. In the navigation pane, click **Addresses**.
   c. Copy the addresses to the Old IP address column on the **Application Data** tab.
   d. In the New IP address column, type the new IP address for the NE service addresses.
   e. (Optional) Copy the Logical Name from the **Addresses** table to the Logical Name (optional) column on the **Application Data** tab.

      Note:

      If more rows are required, copy and paste new rows in the spreadsheet.

4. Click **Save IP Address List** to save the list to your PC with the filename IPAddr.txt.
5. Log on to EMServer1 as ntappadm through ssh or directly at the server console.
6. Transfer the IPAddr.txt file to the `/var/mcp/install` directory.
7. If the Element Manager Internal OAM service IP address changes, on the **Application Data** tab in the Element Manager section, complete the following:
   a. Old Service IP Address (Internal OAM)
   b. New Service IP Address (Internal OAM)
8. If the Application Server Internal OAM service IP address changes, on the **Application Data** tab in the Application Server section, complete the following:
   a. Old Service IP Address (Internal OAM)
   b. New Service IP Address (Internal OAM)
9. If the Accounting Manager Internal OAM service IP address changes, on the **Application Data** tab in the Accounting Manager section, complete the following :
   a. Old Service IP Address (Internal OAM)
   b. New Service IP Address (Internal OAM)
10. If a Web Conferencing Server exists in the system, on the **Application Data** tab in the Web Conferencing Server section, complete the following:
    a. Old Service IP Address
    b. New Service IP Address
11. On the **Application Data** tab in the Primary DB section, complete the following for EMServer1 and EMServer2:
    a. Old IP Address
    b. New IP Address
12. If a secondary database exists in the system, on the **Application Data** tab in the Secondary DB section, complete the following:
    a. Old IP Address
    b. New IP Address

Next steps

Proceed to preparing role data.

Preparing role data

About this task

Use the following procedure to type the passwords for the following accounts for each server undergoing a re-IP.

Procedure

1. Open the job aid worksheet, *AAC 7.0 ReIP Job Aid.xlsm*.
2. Click the **Role Data** tab and type the Old Server IP and the New Server IP for each server undergoing a re-IP.
3. For each server, type the password for the accounts with the following roles:
   a. System Security Administrator (SSA) role, such as ntsysadm.
   b. Application Administrator (AA) role, such as ntappadm.
   c. Security Audior (SA) role, such as ntsecadm.
   d. Backup Administrator (BA) role, such as ntbackup.
   e. Database Administrator (DBA), such as ntdbadm.
4. In the EM and Prov Console administrator column, type the administrator password that is used to log in to the Element Manager Console or Provisioning Manager for the following accounts:
   a. admin
   b. admin1
   c. admin2
   d. admin3
   e. admin4
   f. admin5

   Note:

   If more rows are required, copy and paste new rows in the spreadsheet.

   For more information about the accounts and roles, see Administrative user roles and preconfigured accounts on page 23.

Next steps

Proceed to Re-IPing an Avaya Aura® Conferencing system.

Checklist for reIPing an Avaya Aura® Conferencing system

The following checklist provides a high level view of the steps required to change the IP address of the Avaya Aura® Conferencing system.

Perform the procedure for each task in the order specified.

#	Task	Description	Notes	✔
1	Shutdown the Avaya Aura® Conferencing core applications.	See Shutting down Avaya Aura Conferencing core applications on page 557.		
2	Remove security hardening.	• For Access Control Language (ACL) setup, see Configuring Access Control List to system default on page 558.		
3	Update IP addresses for the server. **Note:** If the Avaya Aura® Conferencing system is moving to a different network, ensure the Avaya Aura® Conferencing system is connected to the new network before proceeding.	See Updating IP addresses for the server on page 559. **Important:** Perform this procedure for each server undergoing an IP address change.		
4	Update the hostname and clock source.	See Updating the hostname and clock source on page 560.		
6	Update Element Manager, Database,	See Updating Element Manager database and		

Comments? infodev@avaya.com

#	Task	Description	Notes	✔
	and Network Element IP addresses.	network element IP addresses on page 562.		
7	Update Hostnames, Element Manager and Network Element certificates.	See Updating hostnames Element Manager and network element certificates on page 563.		
8	Update the Application Data tab, If there are application server internal OAM serivce IP address changes.	• Type the Old Service IP Address (Internal OAM) • Type the New Service IP Address (Internal OAM)		
9	Shut down the application database to configure ACL. Restart the database	See Starting the application and the database on page 566.		
10	Reconfigure Single-Sign On (SSO).	See Configuring the application server network elements on on page 229.		

Related topics:

Shutting down Avaya Aura Conferencing core applications on page 557
Configuring Access Control List to system default on page 558
Updating IP addresses for the server on page 559
Updating the hostname and clock source on page 560
Updating Element Manager, database, and network element IP addresses on page 562
Updating hostnames, Element Manager, and network element certificates on page 563
Shutting down the application on page 565
Configuring ACL on page 565
Starting the application and the database on page 566

Shutting down Avaya Aura® Conferencing core applications

About this task

Use the following procedure to shut down the core applications before you perform a re-IP of the Application Server.

Procedure

1. Log on to the Element Manager Console using an account with admin privileges.
2. Stop all network element instances except for EM_0.

   For more information about stopping network elements, see the procedure for stopping a network element instance.
3. Log on to the Element Manager server hosting Element Manager instance 0 (EM_0) as `ntappadm` to stop the network element instance for EM_0.
4. Type `cd /var/mcp/install`, and press **Enter**.
5. Type `./emStop.pl`, and press **Enter**.

Next steps

Proceed to the procedures for configuring the Access Control List (ACL).

Configuring Access Control List to system default

About this task

Use the following procedure for each server in the system with Access Control List (ACL) previously configured.

Procedure

1. Log on to the server as ntsysadm through ssh or directly on the server console.
2. Type `iptcfg`, and press **Enter**.
3. At the prompt, `password for ntsysadm`, type the password, and press **Enter**.
4. On the IPTables configuration Options screen, perform the following:
   a. Type `7` to select **Restore System Default**, and press **Enter**.
   b. Type `y` to proceed, and press **Enter**.
   c. Type `9` to exit, and press **Enter**.
   d. Type `y` to proceed to exit, and press **Enter**.

Next steps

Proceed to updating IP addresses for the server.

Updating IP addresses for the server

About this task

Use the following procedure to change the IP address of the servers in your system. Perform this procedure for every server undergoing an IP address change.

Note:

If the Avaya Aura® Conferencing system is moving to a different network, ensure the Avaya Aura® Conferencing system is connected to the new network before proceeding.

Procedure

1. Log on to the database server as ntsysadm or an account with the SSA role through SSH or directly on the server console.
2. Type `stopDB` to stop the hosted database server instance, and press **Enter**.
3. Type `statusOfDB` to verify the database was stopped, and press **Enter**.
4. Type `mcpShowNwkConfig` to determine the network configuration, and press **Enter**.
5. Type `mcpModIPv4Subnet –name <Subnet name> [-nif <NIF name>] [-addr <IP address/Subnet Prefix length>] [-router <Subnet default router> [-addotheraddrs <addr1, addr2, ...>] [-delotheraddrs <addrs3, addrs4,...>]` where:
   - <*Subnet name*> is the name of the system default v4subnet, for example, sn0.
   - <*NIF name*> is the name of the network interface (NIF) where the new IP address resides. The syntax is <bond name>.
   - <*IP address*> is the new IP address for the Internal OAM.
   - <*Subnet Prefix length*> is the new Subnet prefix length for the Internal OAM. If the Internal OAM subnet prefix length did not change then use the old Subnet prefix length value.
   - <*Subnet default router*> is the new Subnet Default Router for Internal OAM. If the Internal OAM subnet default router did not change then use the old Subnet Default Router value.
   - <*addr1,addr2,..*> is the list of new IP addresses to be added to the network interface. Use it to add the new Media IP address.
   - <*addr3,addr4,..*> is the list of old IP addresses to be deleted from the network interface. Use it to delete the old Media IP address

Note:

Only the -name and -addr parameter are required. All other parameters are optional. Additional parameter information:

- Use the -addr <*new internal OAM IP address/new Subnet Prefix length*> parameter to update the internal OAM IP address.
- Use the -addotheraddrs <*new Media address*> parameter to add the new Media IP address, if required.
- Use the -delotheraddrs <*old Media address*> parameter to delete the old Media IP address.

6. Type `mcpShowNwkconfig` to verify modification of the network configuration, and press **Enter**.

Next steps

Proceed to updating the hostname and clock source.

Updating the hostname and clock source

About this task

Use the following procedure to update the hostname and clock source of the servers in your system. Perform this procedure for every server undergoing an IP address change.

Procedure

1. Log on to the database server as ntsysadm or an account with the SSA role through SSH or directly on the server console.
2. Type `su -` to log on as root, and press **Enter**.
3. Type `reconfigure.pl`, and press **Enter**.
4. Type the SAA password, if prompted, and press **Enter**.
5. Type <*new hostname*>.
6. At the prompt to confirm, type `y`, and press **Enter**.
7. At the prompt to use the default value for this timezone, type `y`, and press **Enter**.
8. At the prompt, `Do you wish to configure/display the Audit configuration?`, type `q`, and press **Enter**.
9. At the prompt, `Do you wish to configure/display Inactive Login Audit configuration?`, type `q`, and press **Enter**.

10. At the prompt, `Do you wish to configure/display the NTP configuration?`, type `c`, and press **Enter**.
11. Specify the clock source function of the server, select one of the following, and press **Enter**:
    - Option 1 if the server is EMServer1,
    - Option 2 if the server is EMServer2.
    - Option 3 if the server is a Network Element (NE) Server.
12. If you selected EMServer1 or EMServer2, configure the external clock source. At the `Select an option (E, I)` prompt, type `e`.
13. At the prompt, `How many external clock sources would you like to reference (1-2) [1]?`, perform one of the following:
    - If you have defined both the external clock sources (new External Clock Source #1 and new External Clock Source #2) in the job aid worksheet, type `1`, and press **Enter.**
    - If you have defined only one External Clock Source in the job aid worksheet, type `2`, and press **Enter**.

    Note:

    There must be at least one external clock source defined for an Element Manager server.
14. At the prompt, `New External Clock Source #1` type the new address.
15. At the prompt, `Would you like to configure symmetric key authentication for server New External Clock Source #1`?, type `n`.
16. Repeat Steps 14 on page 561 and 15 on page 561 for New External Clock Source #2, if used.
17. For Element Manager Server 1, at the prompt, `Enter the Machine Logical IP address of the Secondary Clock Source Server`, type the New Secondary Clock Source address, and press **Enter**.
18. For Element Manager Server 2, at the prompt, `Enter the Machine Logical IP address of the Primary Clock Source Server`, type the New Primary Clock Source address, and press **Enter**.
19. At the prompt to verify the NTP configuration, type `y`.
20. For network element servers perform the following:
    a. At the prompt, `Enter the Machine Logical IP address of the Primary Clock Source Server`, type the New Primary Clock Source address, and press **Enter**.

b. At the prompt, `Enter the Machine Logical IP address of the Secondary Clock Source Server`, type the New Secondary Clock Source address, and press **Enter**.
c. At the prompt to verify the NTP configuration, type `y`, and press **Enter**.

21. At the prompt, `Grub password configuration`, type `q` and press **Enter**.
22. At the prompt, `SysLog Configuration`, type `q`, and press **Enter**.

Next steps

Proceed to update the Element Manager, database and network element IP addresses.

Updating Element Manager, database, and network element IP addresses

About this task

Use this procedure to update the IP addresses for Element Manager, database, and network elements.

Procedure

1. Log on to the database server as ntsysadm or an account with the SSA role through SSH or directly on the server console.
2. Type `su -` to log on as root, and press **Enter**.
3. Type `/etc/init.d/./reconfigDbServer`, and press **Enter**.
4. Type `su ntdbadm`, and press **Enter**.
5. Type `restartDB`, and press **Enter**.
6. Type `exit`.
7. Log on to EMServer1 (hosting EM instance 0) as ntappadm or an account with the AA role through SSH or directly on the server console.

   Note:

   If the IP address for EMServer1 changed, use the new IP address; otherwise, use the old IP address.

8. Type `cd /var/mcp/install`, and press **Enter**.
9. Type `vi installprops.txt` to edit, and type the New IP address for the following (if changed):
   a. For EMServer1, in the **ne.mgmt.ip** field, type the New IP address in the Internal OAM network of the EM Server 1.

b. For the server hosting the Primary database, in the **db.host** field, type the New IP address in the Internal OAM network of the Primary Database.
c. For the server hosting the Secondary database, in the **db.secHost** field, type the New IP address in the Internal OAM network of the Secondary Database.

10. Type `./dbInstall.pl –fo`, and press **Enter**. The script displays the database settings.
    a. At the prompt, `Continue with these settings? (Y/N) [N]`, type `y`, and press **Enter**.
    b. At the prompt, `Perform "Deploy Files Only" operation to Secondary DB (Y/N) [N]`, type `y`, and press **Enter**.
11. Type `./emDeploy.pl`, and press **Enter**.
    The script displays the Element Manager settings.
12. At the prompt, `Continue with these settings? (Y/N) [N]`, type `y`, and press **Enter**.
13. Type `./addrListUpdate.pl –i IPAddr.txt`, and press **Enter**.
14. Type `./emStart.pl`, and press **Enter**.

Next steps

Proceed to updating hostname, Element Manager, and network element certificates.

Updating hostnames, Element Manager, and network element certificates

About this task

Use the following procedure to update the network element certificates, hostname, and Element Manager.

Procedure

1. On the management PC, open the browser.
2. In the address bar, type `https://<EM service IP address>:12121`, where <IP address> is the EM Internal OAM Service IP address. (This is the logical IP address of the server running Element Manager Console.)

   Note:

   If the IP address for the EM service changed, use the new EM Internal OAM Service IP address; otherwise, use the old EM service IP address.
3. Press **Enter**.

A Web page appears displaying the IP address you entered.

4. On the <IP address> page, click **Launch Element Manager Console**.
5. Log on to the Element Manager console as admin.
6. Navigate to servers.
7. To update the hostname for a server, perform the following:
   a. Select the server, and click **Edit (-/+)**.
   b. Type the new hostname for the server, and click **Apply**.
8. For newly created Element Manager certificates, perform the following:
   a. On the Element Manager console, click **Feature Server Elements** > **Element Manager**.
   b. On the configuration window, select the Element Manager, and click **Edit (-/+)**.
   c. Update the Internal OAM HTTPS Certificate, as required.
9. For newly created Provisioning Manager certificates, perform the following:
   a. On the Element Manager console, click **Feature Server Elements** > **Provisioning Managers**.
   b. On the configuration window, select the Provisioning Manager, and click **Edit (-/+)**.
   c. Update Prov Internal OAM HTTPS Certificate, PA HTTPS Certificate, and SIP Certificate as required
   d. Repeat substeps 9.a on page 564 through 9.c on page 564 for every Provisioning Manager in the system.
10. For newly created Avaya Media Server certificates, perform the following:
    a. On the Element Manager console, click **Media Server and Clusters** > **Media Servers**.
    b. On the configuration window, select the Media Server and click **Edit (-/+)**.
    c. Update the SIP Certificate and SOAP Certificate.
    d. Repeat substeps 10.a on page 564 through 10.c on page 564 for every Avaya Media Server in the system.
11. To restart Element Manager, perform the following:
    a. Log on to the server hosting EMServer instance 0 through ssh or the server console. At the logon prompt, type `ntappadm` or logon to an account with the AA role assigned.
    b. Type `cd /var/mcp/install`, and press **Enter**.
    c. Type `./emStop.pl`, and press **Enter** to stop Element Manager.
    d. Type `./emStart.pl`, and press **Enter** to start Element Manager.
12. On the Element Manager Console, deploy and start all network element instances.

Note:

When you first start Media Server network elements after a system IP address change, you see an alarm that the Configured IP address is not valid. This alarm only appears because of the system IP address change. Restart the Media Server network element to clear the alarm.

13. Verify the state of all network element instances.

Next steps

Proceed to configuring shutting down the application.

Shutting down the application

About this task

After a server IP address change, shut down the application database before you update the Access Control List (ACL) configuration.

Procedure

1. Log on to the Element Manager Console through the EM service address on the Internal OAM network using the admin account.
2. On the Element Manager Console, stop all network element instances except the EM_0 instance.
3. Log on to the server hosting EMServer instance 0 through ssh or the server console. At the logon prompt, type `ntappadm` or log on to an account with the AA role assigned.
4. Type `cd /var/mcp/install`.
5. Type `./emStop.pl`.

Next steps

Proceed to configuring ACL.

Configuring ACL

After a server IP address change, update the Access Control List (ACL) configuration if the system uses ACL.

Before you begin

You have a copy of the *Avaya Aura® Conferencing Security Hardening* document.

Procedure

To update the ACL configuration after an IP address change, see the instructions in the *Avaya Aura® Conferencing Security Hardening* document.

Next steps

Proceed to starting the application.

Starting the application and the database

About this task

Use the following procedure to start the primary Element Manager, database, and other network elements.

Procedure

1. Log on to the server hosting EM instance 0 either through ssh or the server console. At the logon prompt, type `ntappadm` or logon to an account with the AA role assigned.
2. Type `cd /var/mcp/install`, and press **Enter**.
3. Type `./emStart.pl`, and press **Enter**.
4. Log on to the Element Manager Console as admin.
5. Start all network element instances, see deploying and starting the remaining Network Elements.

Next steps

Proceed to configuring the application server network elements on System Manager.

Appendix D: Using OpenSSL for Certificate Signing Requests

Introduction

If creating certificates signed by a third party CA, the administrator must have the tools to generate RSA private keys, Certificate Signing Requests (CSRs), and be able to import the private key and signed certificate into a PKCS#12 file. The OpenSSL package that is included as part of the Avaya Aura® Conferencing platform provides tools to accomplish these tasks.

Important:

This appendix describes one approach to using these tools to perform the tasks. However, there are other ways of performing these tasks. The Enterprise CA or Public CA that signs the certificate request can have other tools or procedures that are required by the policy of a specific CA.

Generating a private key

About this task

Use the following procedure to generate a new RSA private key to use with a Certificate Signing Request (CSR).

Procedure

On a system that has OpenSSL installed, type **`openssl genrsa -des3 -out <private key filename>.key 2048`**, and press **Enter**.

Note:

The value 2048 represents the bit length of the key. For certificates created via OpenSSL, the bit length is typically 2048. You can choose other values such as 1024 or 4096. The value is dependent on the security policy of your network.

Result

A file with the name <private key filename>.key containing the encrypted key is created.

Next steps

Proceed to Generating a Certificate Signing Request.

Generating a Certificate Signing Request

Before you begin

You must have previously generated or have access to an RSA private key that is associated with the certificate.

About this task

Use the following procedure to create a Certificate Signing Request (CSR) to send to the appropriate CA for signing.

Procedure

On the system that has OpenSSL installed, type **`openssl req –new –key <private key filename>.key -out <csr filename>.csr -subj "/C=US/O=My Org/CN=<FQDN>"`**, and press **Enter**.

Note:

The <FQDN> is the only part that is required for certificates used by Avaya Aura® Conferencing. For all other fields of the subject name of the certificate, check with your Enterprise Public Key Infrastructure group or the Public Certificate Authority where you send the request for signing.

Result

A file with the name <csr filename>.csr containing the Certificate Signing Request is created.

Next steps

Proceed to creating a PKCS#12 file.

Creating a PKCS#12 file

Before you begin

You must have access to the following:

- the private key
- the pass phrase that protects the private key
- the certificate that has been signed by the CA

About this task

Use the following procedure to create a PKCS#12 file containing the signed certificate and private key pair.

Procedure

On the system that has OpenSSL installed, type **`openssl pkcs12 –export –out <certificate filename>.p12 –inkey <private key filename>.key -in <certificate filename>.crt`**.

Result

A file with <certificate filename>.p12 containing the certificate and private key is created.

Removing the passphrase key file

About this task

Optional: For Document Conversion Server installation. Use the following procedure to remove a passphrase from the passphrase protected key file.

Procedure

On a system that has OpenSSL installed, type `openssl rsa -in <protected private key filename>.key -out <unprotected private key filename>.key`, and press **Enter**.

Result

A passphrase protected key file is removed.

Appendix E: Downgrading a system

Introduction to downgrading your system

This section provides the details for two types of downgrades:

- downgrading the database only (after the replicated database upgrade failed)
- an entire system (database and all network elements) to a previous Maintenance Release (MR)/patch (for redundant and non-redundant systems)

Note:

The MR patch for an upgrade of the database is backwards compatible so downgrading to a previous MR/patch is typically not required. In the situation of a database failure and to determine if a database downgrade is necessary, contact the Avaya support Web site at http://support.avaya.com to open a service request. In most cases, the problem that caused the upgrade to fail can be fixed and the upgrade can be attempted again.

Prerequisites for performing a downgrade

Review the prerequisites and notes in the following table prior to performing a downgrade.

Table 50: Prerequisites and notes

#	Prerequisites and notes	Description
1	If a Maintenance Release (MR)/patch upgrade failed, determine where the problem occurred.	• There is a problem with a Network Element other than the database. Downgrade the Network Element to a previous MR/patch load. • There is data corruption in the database and you have a database backup for the current MR/patch load, see the database backup and restore section in the *Maintaining and Troubleshooting Avaya Aura® Conferencing.* • A replicated database failed and no other components have been upgraded, see Checklist for downgrading when a replicated database upgrade fails on page 574.

#	Prerequisites and notes	Description
2	Prior to performing a downgrade, compose a list of application network element names and IP addresses. Include all applications for keeping track of when the applications change from active to standby and back again.	On the Element Manager console, view the status of the instance (for example, Active or Standby) from the Maintenance window for the Network Element instance.
3	Review the warnings and notes prior to starting the downgrade process.	**Warning:** During the downgrade process, any data written to the secondary database (registrations) is lost. **Note:** The database access layer (used by all of the Network Elements that connect to the database) is designed for the NE instance to only setup communications with a database that has the same (or higher) load version as the Network Element, for example, MCP_15.0.6.0. This ensures that the downgrade process can downgrade the database and the NE instances in a singular (one-by-one) fashion and that the NEs connect to the database with the current load/version installed. The following distinctions are made between the two Maintenance Release (MR) loads during the downgrade process: • 15.0.Y.Y: The MR you are currently deploying (MR that you upgraded to) • 15.0.X.X: The MR that you are downgrading to
4	Ensure you have access to the three roles required for performing the downgrade procedures.	• Root: Access root by logging on as `ntsysadm` through ssh and typing **su -**. • AA role: Log on as `ntappadm`. • DBA role: Log on as `ntdbadm`. For more information about these roles, see Administrative user roles and preconfigured accounts on page 23.
5	Identify your deployment type: • Redundant system: co-resident with redundancy or	• For co-resident with redundancy or standalone with redundancy deployments, see Checklist for downgrading a system—co-resident with

#	Prerequisites and notes	Description
	standalone with redundancy layout type • Non-redundant system: co-resident simplex or standalone simplex	redundancy or standalone with redundancy layout on page 575. - For co-resident with redundancy or standalone with redundancy deployments, also see Downgrading the on page 579. • For co-resident simplex or standalone simplex deployments, see Checklist for downgrading a system—co-resident simplex or standalone simplex layout on page 582.
6	You can only downgrade a database to a version that has been successfully deployed in the past. Review the following list of example database deployments.	Prior to a downgrade: • MCP_15.0.6.0_2012-03-02-2201 mcpInstall.pl: an initial deployment of the database load. • MCP_15.0.6.0_2012-03-25-2201 mcpUpgrade.pl: creates a backup of the MCP_15.0.6.0_2012-03-02-2201 with its current contents (before the upgrade is performed). • MCP_15.0.6.0_2012-03-25-2201 mcpUpgrade.pl: creates a backup of the MCP_15.0.6.0_2012-03-25-2201 database with its current contents (before the upgrade is performed). After you downgrade the database: • MCP_15.0.6.0_2012-03-02-2201: the downgrade restores the database using the backup taken when the database was upgraded to the MCP_15.0.6.0_2012-03-25-2201 load. • MCP_15.0.6.0_2012-03-25-2201: the downgrade restores the database using the backup taken when the database was upgraded to the MCP_15.0.6.0_2012-03-25-2201 load. **Note:** An attempt to downgrade the database to a different version would fail (because there is no associated backup for restoring the database).
7	The version of the software load being downgraded must exist on the Element Manager.	

Checklist for downgrading when a replicated database upgrade fails

Use the following checklist when the upgrade of the replicated database failed and no other components have been upgraded.

#	Task	Description	Notes	✔
1	Drop database replication	See Dropping database replication on page 577.	10 minutes	
2	Downgrade the secondary database (see steps 2a through 2c):		Total time: 30 minutes (approximately)	
2a	Restore the 15.0.X.X install scripts/files.	See Restoring install scripts on page 583.	10 minutes	
2b	Verify the 15.0.X.X database backup file exists in the `/var/mcp/db/backup` directory on the server hosting the secondary database.	See Verifying the database backup file on the secondary database on page 578.	10 minutes	
2c	Restore the 15.0.X.X database backup to the secondary database.	See Restoring the database backup file to the secondary database on page 578.	10 minutes	
3	Resync the Database	See Resyncing the database on page 581.	90 minutes	

Checklist for downgrading a system—co-resident with redundancy or standalone with redundancy layout

The following checklist provides a high level overview of the downgrade process for co-resident with redundancy or standalone with redundancy layouts (redundant system).

#	Task	Description	Notes	✔
1	Log on to the 15.0.Y.Y Element Manager Console and stop all Personal Agent and Provisioning Agent Managers running on the primary and secondary servers. This prevents any additional provisioning changes from being made to the 15.0.Y.Y database or data. In the full rollback scenario, the primary database stays on the 15.0.Y.Y release/schema until the end of the rollback process, and then the secondary database (which was restored with the old 15.0.X.X database backup) is used to populate (resync) the primary database to the 15.0.X.X release/schema. Also, to disallow any provisioning changes to the 15.0.Y.Y primary database, the Personal Agent and Provisioning Agent Manager components are stopped.	See Stopping a Network Element instance on page 472.	5 minutes	
2	Drop database replication	See Dropping database replication on page 577.	10 minutes	
3	Downgrade the secondary database (see steps 3a through 3c):		Total time: 30 minutes (approximately)	
3a	Restore the 15.0.X.X install scripts/ files.	See Restoring install scripts on page 583.	10 minutes	
3b	Verify the 15.0.X.X database backup file exists in the `/var/mcp/db/backup` directory on the server hosting the secondary database.	See Verifying the database backup file on the secondary database on page 578.	10 minutes	

#	Task	Description	Notes	✔
3c	Restore the 15.0.X.X database backup to the secondary database.	See Restoring the database backup file to the secondary database on page 578.	10 minutes	
4	Downgrade the Avaya Media Server software for every Avaya Media Server.	See Downgrading the on page 579.	—	
5	Downgrade the following Network Elements (NE): • Provisioning Manager • Personal Agent Manager (if any) • Accounting Manager • Application Server • Media Server (if any) • Web Conferencing Management Server (if any) • Web Conferencing Server (if any)	See Downgrading the Network Elements on page 580.	5 minutes for each Network Element.	
6	Downgrade the Element Manager to the old 15.0.X.X load.	See Downgrading the Element Manager on page 581.	5 minutes	
7	Resync the Database	See Resyncing the database on page 581.	90 minutes	
8	The two databases are now replicated and the downgrade process is complete.			

Related topics:

Stopping a Network Element instance on page 472
Dropping database replication on page 577
Verifying the database backup file on the secondary database on page 578
Restoring the database backup file to the secondary database on page 578
Downgrading the Avaya Media Server on page 579
Downgrading the Network Elements on page 580
Downgrading the Element Manager on page 581
Resyncing the database on page 581

Stopping a Network Element instance

About this task

Use this procedure to stop a Network Element instance.

Procedure

1. Log on to Element Manager Console.
2. In the navigation pane of Element Manager Console, select **Feature Server Elements**> ***<Network Element type>*** > ***<Network Element instance you want to stop>*** > **NE Maintenance**.
3. In the Maintenance dialog box, select the row that has a value of the target instance in the ID column.
4. Click **Stop**.
   The Maint state changes from “None” to “Stopping,” indicating that the stop operation is in progress. When the stop operation is complete, the following state changes occur:
   - The Maint state changes back to “None.”
   - The Admin state changes from “Online” to “Offline.”

Result

The Network Element instance is stopped.

Dropping database replication

About this task

Use the following procedure to drop database replication.

Procedure

1. Log on to the primary database as `ntdbadm` or an account with the DBA role.
2. Type `cd /var/mcp/run/MCP_15.0/<dbname>_0/bin/util`.
3. Type `./cleanupReplication.pl`.
4. At the prompt, `Continue with dropping Database replication?`, type `y`, and press **Enter**.

Next steps

Proceed to downgrading the secondary database.

Verifying the database backup file on the secondary database

About this task

Use the following procedure to verify the 15.0.X.X. database backup file exists in the `/var/mcp/db/backup` directory on the server hosting the secondary database.

Procedure

1. Log on to the secondary database as `ntdbadm` or an account with the DBA role.
2. Type `cd /var/mcp/db/backup`, and press **Enter**.
3. Type `ls -lrt`. If the 15.0.X.X database backup file is not there, you can sftp the file from the server hosting the primary database, as follows:
   a. Type `sftp <primary_db_IP>`, where: <primary_db_IP> is the IP address of the server hosting the primary database.
   b. Type the ntdbadm password.
   c. Type `cd /var/mcp/db/backup`.
   d. Retrieve the <15.0.X.X_database_backup_file>.
   e. Type `exit`.
4. Type `ls -lrt`, and ensure the size of the <15.0.X.X_database_backup_file> is the same size as the file on the server hosting the primary database.

Next steps

Proceed to restoring the 15.0.X.X. database backup to the secondary database.

Restoring the database backup file to the secondary database

About this task

Use the following procedure to restore the 15.0.X.X. database backup to the secondary database.

Procedure

1. Type `cd /var/mcp/run/MCP_15.0/<dbname>/bin/util`.
2. Type `./dbRestore.pl <backupfile>`, and press **Enter**.

Comments? infodev@avaya.com

Note:

Backup files are located at `/var/mcp/db/backup`.

The total time required is dependant on the platform and size of the database being restored.

Next steps

Proceed to downgrading the Avaya Media Server software for every Avaya Media Server.

Downgrading the Avaya Media Server

The two Avaya Media Server loads involved in the downgrade process are referred to as the following:

- 7.5.0.YYY: the Avaya Media Server that is currently deployed or the Avaya Media Server that you upgraded to.
- 7.5.0.XXX: the Avaya Media Server that is being downgraded to.

About this task

Use the following procedure to downgrade the servers containing the Avaya Media Server software.

Procedure

1. Log on to the Avaya Media Server as root.
2. Type `mcpMsUninstall.pl`, and press **Enter**.
   You have uninstalled the 7.5.0.YYY load.
3. Type `mcpInstall.pl` and select the **7.5.0.XXX** load.
   You have installed the 7.5.0.XXX load.
4. Type `msRestore.pl`, and press **Enter**.
5. Select the backup file to restore.

   Note:

   Backup files are located in `/var/mcp/ma/MAS/platdata/EAM/Backups`.
6. Repeat this procedure for every Avaya Media Server requiring a downgrade.

Result

You have successfully downgraded the Avaya Media Server software.

Downgrading the Network Elements

About this task

Use this procedure to downgrade the following Network Elements (NE):

- Provisioning Manager
- Personal Agent Manager (if any)
- Accounting Manager
- Application Server
- Media Server (if any)
- Web Conferencing Management Server (if any)
- Web Conferencing Server (if any)

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements**.
2. Navigate to the **NE Maintenance** window for each Network Element to be stopped.

   Note:

   Provisioning Manager and Personal Agent Manager were previously stopped in the procedure for Stopping a Network Element instance.
3. In the Maintenance dialog box for a Network Element, select the row for ID 0.
4. Click **Stop**.
5. In the Instance window for a Network Element, select the row for ID 0.
6. Click **Edit (-/+)**.
7. Select the old load (15.0.X.X) from the list.
8. Click **Apply**.
9. In the NE maintenance window for a Network Element, select the row for ID 0, and click **Deploy**.
10. In the NE maintenance window for a Network Element, select the row for ID 0, and click **Start**.
11. Repeat these procedures for all Network Elements with instance 0.
12. If there is a second instance (ID 1), repeat the procedures for all Network Elements with instance 1.

Note:

Ensure the downgraded instance is up and running before downgrading other Network Elements or instances.

Downgrading the Element Manager

About this task

Use the following procedure to downgrade the Element Manager to the old 15.0.X.X load.

Procedure

1. Log on to the primary Element Manager server (EMServer1) as `ntappadm` or an account with the AA role.
2. Type `cd /var/mcp/install`, and press **Enter**.
3. Type `./emUpgrade.pl`, and press **Enter**.

Result

Downgrading for all the Network Element instances are complete.

Resyncing the database

About this task

Use the following procedure to resync the database.

Procedure

1. Log on to the secondary Element Manager (EMServer2) as `ntdbadm` or an account with the DBA role.
2. Type `cd /var/mcp/run/MCP_15.0/<dbname>_1/bin/util`, and press **Enter**.
3. Type `./resync.pl`, and press **Enter**.

Result

The two Databases are now replicated and the downgrade process is complete.

Example

The following is an example of the output from an resync.pl script execution on a secondary database.

```
WARNING: This script should be executed during off-hours when Provisioning and
Registration traffic is low. In addition, while this script is executing, there is a
period of time that the database goes into a read-only state. Thus, during this
period, NO REGISTRATION or PROVISIONING changes are allowed. Note that the Session
Manager will queue all changes to Registrations within its local memory/cache (during
this operation), and the Registrations will be written to the Database once the
resync successfully completes. If this script DOES NOT RUN TO COMPLETION, then the
DB could be left in a READ-ONLY state. Again, if the DB is in a READ-ONLY state, then
ALL PROVISIONING CHANGES WILL FAIL until the DB mode is changed MANUALLY. For this
case, please execute the activate AppUserDBprivs.pl script (in this same directory)
to ensure the DB is not "stuck in" a READ-ONLY state.
**************************************************************************
Continue with this script?(Y/N): [N]y ----------------------------- ReSync Type:
Resync From Secondary To Primary Primary DB IP: 192.168.209.126 Secondary DB IP:
192.168.209.194 Operation to Perform: Resync Continue with these settings?(Y/N):[N]y
```

Checklist for downgrading a system—co-resident simplex or standalone simplex layout

The following checklist provides a high level overview of the downgrade process for co-resident simplex or standalone simplex layouts (non-redundant).

#	Task	Description	Notes	✔
1	Stop all Network Element instances. • Provisioning Manager • Personal Agent Manager (if any) • Accounting Manager • Application Server • Media Server (if any)	See Stopping a Network Element instance on page 472.	10 minutes	

#	Task	Description	Notes	✔
	• Web Conferencing Management Server (if any) • Web Conferencing Server (if any)			
2	Downgrade the database (see steps 2a and 2b)		30 minutes total	
2a	Restore the 15.0.X.X install scripts/files and deploy old database load file only.	See Restoring install scripts on page 583.	5 minutes	
2b	Restore the old database backup to the database.	See Restoring the old database backup to the database on page 584.	25 minutes	
3	Downgrade the Avaya Media Server software for every Avaya Media Server.	See Downgrading the on page 579.	—	
4	Downgrade the Element Manager to the old 15.0.X.X load.	See Downgrading the Element Manager on page 581.	5 minutes	
5	Downgrade remaining Network Elements	See Downgrading the Network Elements on page 580.	5 minutes for each Network Element.	
6	The downgrade is complete.			

Related topics:

Downgrading the Avaya Media Server on page 579
Downgrading the Network Elements on page 580
Downgrading the Element Manager on page 581
Restoring install scripts on page 583
Restoring the old database backup to the database on page 584

Restoring install scripts

About this task

Use the following procedure to restore the 15.0.X.X. install scripts.

Procedure

1. Log on to Element Manager (EMServer1) as `ntappadm` or an account with the AA role.

2. Type `cd /var/mcp/install`, and press **Enter**.
3. Type `vi install.props.txt` to change the ne.load=<loadname>. Where <loadname> is the previously deployed 15.0.X.X loadname.
4. Type `vi install.props.txt` to edit and change the ne.load=<loadname>. Where <loadname> is the previously deployed 15.0.X.X loadname.
5. Type `./dbInstall.pl –fo` to deploy the old database load file (Deploy files only option), and press **Enter**.
6. At the prompt to `Continue with these settings? (Y/N) [N]`, type `y`, and press **Enter**.
7. At the prompt to `Perform Deploy Files Only operation to Secondary DB also? (Y/N) [Y]`, type `y` or press **Enter** to accept the default.

Restoring the old database backup to the database

About this task

Use the following procedure to restore the old database backup to the database.

Procedure

1. Log on to the server hosting the database as `ntdbadm` or an account with the DBA role.
2. Type cd `/var/mcp/run/MCP_15.0/<dbname>/bin/util`.
3. Type `./dbRestore.pl <backupfile>`, and press **Enter**.

   Note:

   Backup files are located at `/var/mcp/db/backup`.

   The total time required is dependant on the platform and size of the database being restored.
4. After the restore is complete, restart all Network Elements so they will be in sync with the data in the restored database.

Next steps

Proceed to downgrading the Element Manager.

Downgrading the Avaya Media Server

The two Avaya Media Server loads involved in the downgrade process are referred to as the following:

- 7.5.0.YYY: the Avaya Media Server that is currently deployed or the Avaya Media Server that you upgraded to.
- 7.5.0.XXX: the Avaya Media Server that is being downgraded to.

About this task

Use the following procedure to downgrade the servers containing the Avaya Media Server software.

Procedure

1. Log on to the Avaya Media Server as root.
2. Type `mcpMsUninstall.pl`, and press **Enter**.
   You have uninstalled the 7.5.0.YYY load.
3. Type `mcpInstall.pl` and select the **7.5.0.XXX** load.
   You have installed the 7.5.0.XXX load.
4. Type `msRestore.pl`, and press **Enter**.
5. Select the backup file to restore.

   Note:

   Backup files are located in `/var/mcp/ma/MAS/platdata/EAM/Backups`.
6. Repeat this procedure for every Avaya Media Server requiring a downgrade.

Result

You have successfully downgraded the Avaya Media Server software.

Downgrading the Element Manager

About this task

Use the following procedure to downgrade the Element Manager to the old 15.0.X.X load.

Procedure

1. Log on to the primary Element Manager server (EMServer1) as `ntappadm` or an account with the AA role.

2. Type `cd /var/mcp/install`, and press **Enter**.
3. Type `./emUpgrade.pl`, and press **Enter**.

Result

Downgrading for all the Network Element instances are complete.

Downgrading the Network Elements

About this task

Use this procedure to downgrade the following Network Elements (NE):

- Provisioning Manager
- Personal Agent Manager (if any)
- Accounting Manager
- Application Server
- Media Server (if any)
- Web Conferencing Management Server (if any)
- Web Conferencing Server (if any)

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements**.
2. Navigate to the **NE Maintenance** window for each Network Element to be stopped.

   Note:

   Provisioning Manager and Personal Agent Manager were previously stopped in the procedure for Stopping a Network Element instance.
3. In the Maintenance dialog box for a Network Element, select the row for ID 0.
4. Click **Stop**.
5. In the Instance window for a Network Element, select the row for ID 0.
6. Click **Edit (-/+)**.
7. Select the old load (15.0.X.X) from the list.
8. Click **Apply**.
9. In the NE maintenance window for a Network Element, select the row for ID 0, and click **Deploy**.

10. In the NE maintenance window for a Network Element, select the row for ID 0, and click **Start**.
11. Repeat these procedures for all Network Elements with instance 0.
12. If there is a second instance (ID 1), repeat the procedures for all Network Elements with instance 1.

Note:

Ensure the downgraded instance is up and running before downgrading other Network Elements or instances.

Appendix F: DNS and Avaya Aura Conferencing

DNS and Avaya Aura® Conferencing

Typically, customers who purchase and implement the Avaya Aura® Conferencing solution also support Domain Name Server (DNS) lookup in their deployment. So, in most cases, DNS is used at a solution level for Avaya Aura® Conferencing. However, there are a small number of customers who purchase and implement Avaya Aura® Conferencing in a deployment that does not support DNS lookup. It is more likely that small to medium sized enterprises may not use DNS at a solution level for Avaya Aura® Conferencing. These customers, who do not implement DNS lookup, must manually ensure that the mapping between Fully Qualified Domain Names (FQDN) and IP addresses is accurate and up-to-date.

In the Avaya Aura® Conferencing solution, a table called **/etc/hosts** manages the mapping between domain names and IP addresses.

Updating the host table entries

Note:

Perform this procedure only if the DNS client is not configured on the server.

The FQDN assigned to each Web Conferencing Service IP must be mapped to a corresponding IP address. Any server hosting a managed element instance that communicates with a Web Conferencing Service IP requires mapping.

Entries in the `/etc/hosts` table are managed by using the **`hostTableConfig`** alias. You must be logged on to an account with the SSA role (for example, ntsysadm).

Before you begin

- You must know the mapping of the service FQDN to IP address for each Web Conferencing Service IP.
- If the Web Conferencing Service IP is located within the DMZ, ping the IP address of each server to confirm communications between all components.

Note:

If your firewall blocks ICMP, you cannot verify communications between all components using ping.

About this task

Use the following procedure to create the mapping of FQDN to IP address on the Avaya Aura® Conferencing servers.

Procedure

1. Log on to the server hosting a Web Conferencing Server using an account with the SSA role (for example, ntsysadm).
2. Type `hostTableConfig -a <IP_Address> <FQDN>` for every IP address that requires mapping.

   Where IP_Address is the IP address to map to the specific Web Conference service FQDN.
3. Repeat Step 2 for each server hosting the following Network Elements:
   - Application Server
   - Provisioning Manager
   - Personal Agent Manager
   - Web Conferencing Management Server
   - Web Conferencing Server
   - Recording Server(s)

Note:

Systems external to Avaya Aura® Conferencing must be able to translate the Web Conferencing Server FQDN into an IP address for routing. Contact your network engineers to configure entries on your DNS servers.

Next steps

Proceed to configuring the meeting event processor for the Web Conferencing Management Server.

Glossary

Application Server (AS)	The application server hosts the Meetme and Adhoc conference applications, and handles the SIP signaling from clients.
Avaya Media Server	The Avaya Media Server hosts conferences and relays media.
Guest	A guest is an unprovisioned user. The guest has the same privileges as a participant but cannot be promoted to presenter or moderator.
AV MeetMe conference	A planned Web conference supporting audio and video.
Bandwidth	Requested bandwidth: This is the bandwidth that is requested at the time of initiating a conference call. This bandwidth request may be negotiated down to a lower bandwidth, or can be thinned by Avaya Aura® Conferencing at some point during the conference. Negotiated bandwidth: This is a bandwidth that the server allocates to the client and is based on your system configuration and the total available network bandwidth. Actual bandwidth: This is the bandwidth that is used for a session as determined by the Avaya Media Server.
Database (DB)	The database stores configuration information for all Network Elements, such as long and short names, server IP address, and historical OM data.
Dropped sessions	Dropped sessions are the number of sessions that dropped by a system due to bandwidth management issues.
Down sessions	Down sessions are the number of sessions where bandwidth is downgraded because of proactive or reactive thinning.
Communication Manager	A key component of Avaya Aura®. It delivers rich voice and video capabilities and provides a resilient, distributed network for media gateways and analog, digital, and IP-based communication devices. It includes advanced mobility features, built-in conference calling, contact center applications and E911 capabilities.
Document Conversion Server	The Document Conversion Server (DCS) is a windows server that is a document converter and converts PowerPoint, PDF and other document types into formats compatible with Web conferencing.

Element Manager (EM)	Client receives almost all information from the Element Manager using OMI methods. The client sends an OMI request to Element Manager. Element Manager processes this request and determines what to do with it. To get the data for client Element Manager, a request is sent to the database or to other network elements, such as the Application Server or the Web Conferencing Server.
Gap	The gap is the difference between the negotiated and actual bandwidth. For example: A request for bandwidth is initiated for a video or audio call (requested bandwidth). The Media Server responds with bandwidth and bandwidth is applied (negotiated bandwidth). Bandwidth continually changes during a call due to factors such as codec, packetization, and time. Therefore, a gap between the actual and negotiated bandwidth occurs.
Geographic Redundancy	The capability to implement multiple server instances, such as Session Manager, in geographically distinct data centers.
Hybrid Conference	A hybrid conference includes Web and Audio sessions.
IPv4	The fourth revision in the development of IP, and the first version of the protocol to be widely deployed.
KPI client	Client receives almost all information from the Element Manager using OMI methods. Usually to get some information client sends an OMI request to Element Manager. Element Manager processes this request and decides what to do with it. To get the data for client Element Manager sends a request to database or to another network elements, such as the Application Server or the Web Collaboration Server.
License	There are two types of system licenses: Audio and Video. A unique license is required for each Avaya Aura® Conferencing provisioned user. The License key is installed on the Web License Manager (WebLM) server which is co-resident with System Manager.
Moderator	A moderator is a provisioned user and has full control of the conference using either Telephone User Interface (TUI) and User Interface (UI) commands on one of the supported clients.
Open Management Interface (OMI) call	SOAP based Web Services provides operations required for Avaya Aura® Conferencing.
Operator	An operator controls every aspect of a conference in the same manner as the moderator. An operator does not attend the conference but can be called upon by issuing a Telephony User Interface (TUI) code, if assistance is required.
Participant	Participants are people who attend conference calls. A participant can access a conference using an Avaya Aura® Conferencing user account

	or log in as guest. A participant can be promoted by the moderator to be a presenter or a moderator but cannot change the state of the conference.
Presenter	A presenter is a provisioned user. The presenter has the same privileges as a participant but has been promoted to presenter to allow presentation of content using Web collaboration.
R-factor	R-factor is a measure of audio quality; the lower the number, the poorer the audio quality. R-factor uses a scale of 0 to 100.
Session Completion Ratio	The percentage of rejected sessions compared to the total number of sessions. A session can be rejected for different reason, such as, not enough Bandwidth or not enough licenses.
Simple Object Access Protocol (SOAP)	Protocol specification for exchanging structured information in the implementation of Web Services in computer networks.
Standalone Web conference	A user starts a standalone Web conference using the Collaboration Agent client before starting an AV MeetMe conference. After an AV MeetMe conference is started, the standalone Web conference is merged with the AV MeetMe conference and is no longer in a standalone state.
Web Conferencing Server (WCS)	This server handles user actions and media during Web collaboration.
Web Service (WS)	A software system designed to support interoperable machine-to-machine interaction over a network.

Index

A

AAC Platform 129
  verifying 129
Access Control List 566
ACL 376, 386, 566
  configuring 376
ACL rules 377–380, 382, 385
adhoc 237
adhoc conference 76
alarm forwarding 295, 303, 305
  disabling 305
  enabling 303
  SAL gateway 303, 305
  system manager 295
Allowing administrator sudo access 374
Apple Safari 24
application server 79, 533
  uninstall workflow 533
audio 71
  network impact 71
audio delays 72, 73
  with media cascading 73
  without media cascading 72
audio queue 75
Audio SRTP 265, 266, 270
  configuring 265
  modifying the settings 266
Audio/Video in Collaboration Agent ... 337, 339, 343, 344, 347, 349, 351, 353, 355–357, 365, 488
  adding a Flash Media Gateway cluster 351
  configuring a coresident deployment 343
  configuring the Flash Media Gateway 349
  creating the client configuration file 353
  hardening 357
  installation checklist 337
  installing the client software 355
  installing the Management Portal software 347
  installing the server software 344
  starting the Flash Media Gateway 353
  upgrading 365, 488
  verifying integration 356
Audio/Video in Collaboration Agent installation files 342
  copying 342
  extracting 342
authentication files 375
  loading 375
Avaya 96x1 SIP telephones 400
  configuring 400
Avaya Aura Conferencing Platform 437, 446
  patching 446
  patching the primary servers for the main site ... 437
Avaya Aura Conferencing server 505, 522
  backing up 505
  restoring 522
Avaya Flare Experience for iPad Devices 398
  configuring 398
Avaya Flare Experience for Windows 397
  configuring 397
avaya media server 80, 82
  redundancy 80
Avaya Media Server 134, 177, 178, 448, 502, 579, 585
  adding 177
  adding a network element 178
  backing up 502
  downgrading 579, 585
  installation 134
  upgrading 448
Avaya Media Servers 445, 473
  locking an instance 445, 473
  stopping an instance 445, 473
Avaya Mentor videos 18

B

back up 497, 518
backup parameters 510, 515
  configuring individual remote backup parameters 515
  configuring remote backup parameters 510
bandwidth management 69
bandwidth monitoring 96
bandwidth reduction 87
BIOS 119
  modifying clock 119
BIOS boot order 367
BIOS password 367
bulk provisioning 284

C

CA certificates 163, 169
capacity 69

cascading 258, 260
configuring 258
configuring a regional cascading location 260
media server cascading 258
configuring 258
centralized hosting 87
certificates 168, 169, 171–176, 331
third party 168
third party CA 169
change IP address 556
checklist ... 99, 108, 153, 273, 274, 313, 333, 410, 421, 556
LDAP integration 313
Audio/Video in Collaboration Agent 333
before you begin 99, 410, 421
installation 108
IP address change 556
Recording feature in a co-resident deployment . 274
Recording feature in a dedicated Recording server deployment 273
Transport Layer Security 153
Chrome 24
co-resident simplex 27
deployment layout 27
co-resident with redundancy 27
deployment layout 27
co-resident with redundancy with DMZ 53
servers 53
target capacities 53
codecs 259, 260
cascading trunks 259, 260
Communication Manager 310, 311
conference types 76
conferencing profile 246, 249, 250
Configuring a file system baseline 388
Configuring Avaya Media Server DSCP 394
Configuring operating system password and account policies 370
Configuring the post-login warning banner 369
Configuring the pre-login warning banner 369
coresident 33, 34
specifications 33, 34
no dmz access 33
with dmz access 34
coresident deployments 343
configuring Audio/Video in Collaboration Agent . 343
Creating new user-specific accounts 372

D

data migration 541, 542, 544
exporting 542
importing 544
data migration tool 541
installing 541
database 476, 499, 525
backing up 499, 525
starting 476
DCS 193
Windows OS 193
Deleting pre-configured OS administrator accounts . 375
Dell PowerEdge R610 25
deployment layout 27
co-resident simplex 27
co-resident with redundancy 27
enterprize DMZ 27
standalone 27
standalone simplex 27
deployment layouts 32
enterprise dmz 32
design considerations 67
dial out 76
display numbers 241, 242
adding 241
deleting 242
dmz 33, 34, 62
coresident 33, 34
specifications 33, 34
DMZ 186–188, 190
from 190
to 188
DNS 589
DNS client 494
configuring 494
document conversion server 40, 202, 204, 487
specifications 40
upgrading 487
Document Conversion Server 193, 197, 200, 201, 205, 207, 449
adding on Element Manager 205
configuring the SNMP service 197
disabling SSL/TLS 207
installing 200
restricting access to 201
upgrading 449
documentation 105
document set 105
downloading 105
domain 246
adding 246
domain name 589
domains 245
downgrading 571, 574, 575, 577, 578, 580–586
database replication 577

introduction 571
non-redundant 582
co-resident simplex 582
standalone simplex 582
prerequisites 571
redundant system 575
co-resident with redundancy 575
standalone with redundancy layout 575
replicated database failure 574

E

Element Manager 392
changing the SNMP community string 392
Element Manager console 147
local login 147
Element Manager Console 391
configuring local administration login rules 391
configuring local administration password policies 391
Element Manager primary network element instance 432
stopping 432
Enabling Tomcat webserver access and error logs for the Element Manager 388
End Entity 160, 358
enrollment password 298
system manager 298
enterprise dmz 32
deployment layouts 32
enterprize DMZ 27
deployment layout 27
erlang-b model 84
event conference server 40
specifications 40
event conferencing 64, 237, 257

F

failover 215
feature packs 455, 457
installing 455
overview 457
Firefox 24
Fixing remote host SSH keys 394
Flare Experience for iPad Devices 397
Flare Experience for Windows 397
Flash Media Gateway 43, 349, 353, 359–362
configuring 349
configuring a secure SIP TLS connection to Session Manager 361
creating a VeriSign-signed certificate 359
securing the JMX connection and RTMPS connection 360
securing the RTMPS connection to AViCA clients 362
servers 43
specifications 43
starting 353
Flash Media Gateway cluster 351
adding 351
FSI baselines 518

G

Google Chrome 24

H

hardening 367
Hardening the database 372
hardware environment 120
host tables 589
hosting locations 86, 92
with media cascading 92
without media cascading 86
HP DL360 G7 server 111
power management settings 111
HP DL360 G7 Server 106–108
back view 106
environmental specifications 107
front view 106
physical specifications 108
HP Proliant DL360 G7 25

I

IBM S8800 25
identity certificate 160–162, 358
End Entity 160
Firefox 162
Flash Media Gateway 358
Internet Explorer 161
import.dat 387
install scripts 583
installation files 427, 467
copying 427, 467
extracting 427, 467
intelligent workbook 20, 116, 140
populating tags 140
Internet Explorer 24
IP address change 551, 556
IP addresses 139

gathering 139

J

Java 195, 196
JMX connection 360
Flash Media Gateway 360

L

LDAP directory integration 316, 317
LDAP integration 313, 314, 319, 321, 325–328, 330
passcodes encryption 327
license key 151
Linux 113, 116
Avaya Media Server 113
Element Manager Console 113
installing 113, 116
Linux patching 113
patching 113
Linux operating system 129
verifying 129
load balancer 289, 291
local logon 391
configuring administration login rules 391
configuring administration password policies 391
locations 254, 260, 261
associating web collaboration resources 254
configuring a regional cascading location 260
configuring media cascading locations 261
log forwarding 297, 298, 300, 301
checklist 297
configuring 298
disabling 301
enabling 300

M

MAC OS 24
macros 200
media cascading 42
servers 42
media cascading locations 261
configuring 261
media cascading server 42
specifications 42
media server 38, 380, 502
backing up 502
specifications 38
media server clusters 179, 279
configuring Recording in a co-resident deployment 279
modifying 179
media servers 445, 473, 477
locking an instance 445, 473
starting an instance 477
stopping an instance 445, 473
unlocking an instance 477
meetme 76, 237
Microsoft Office 2013 198
activating the license 198
Microsoft Outlook Add-in 401–403
centralized software deployment 403
ClickOnce deployment 402
deploying 401
Microsoft Visual C++ 2008 199
installing 199
Microsoft Windows updates 195
configuring 195
Mozilla Firefox 24
multiple hosting locations 93
with media cascading 93

N

network delay 96
network element 485
patching 485
upgrading 485
network element instance 443, 444, 447, 493
deploying 493
stopping 443
undeploying 444
upgrading 447
Network Element instance 472, 476, 577
starting 476
stopping 472, 577
network elements 218, 219
web conferencing 218
web conferencing management 219
network impact 71, 74
audio 71
video 74
network planning 67
non-hosting locations 92
with media cascading 92
NTP clock 123
configuration 123

O

operating system warning banner 368

P

packet time selection 96
passcodes encryption 327
passphrase key file 569
password 126
  initial logon 126
patches .. 127, 437, 442, 446, 463, 470, 474, 479, 484, 485, 492
  Avaya Aura Conferencing Platform 446
  Avaya Aura Conferencing Platform for the main site 437
  database 479, 492
  Element Manager 484
  installing 463, 485
  MCP database 484
  operating system 437, 446, 470, 474
  target server platform patch 127
  upgrading the database 437, 442
patching 480
  Avaya Aura Conferencing software 480
peak participants 84
performance 29
  specifications 29
Personal Agent Manager 390
  configuring audit logging 390
  configuring Tomcat webserver access logs 390
planning 67, 68
  QoS 68
Provisioning Client 221, 391
  configuring local administration login rules 391
  configuring local administration password policies 391
Provisioning Manager 389
  configuring audit logging 389
  configuring Tomcat webserver access logs 389

Q

QoS 68
  planning 68

R

recording 37, 259, 273, 282
  codecs 259
  specifications 37
  trunks 259
  user provisioning 282
Recording 275, 278–282
  configuring a media server cluster in a co-resident deployment 279
  configuring for a user 282
Recording feature 286
  configuring the backup server 286
recording media server 130
Recording setting 281
  configuring 281
redundancy 79, 81
regional cascading location 260
  configuring 260
related resources 18
  Avaya Mentor videos 18
  training 18
remote backup parameters 510, 515
  configuring 510, 515
Removing the default staging certificates 393
Resetting the GRUB password 371
restore 521
resync 436
RTMPS connection 360, 362
  Flash Media Gateway 360
  securing between Flash Media Gateway and AViCA clients 362

S

Safari 24
SAL 303, 305
secure access gateway 303
secure access link 303, 305
secure access link gateway 303, 305
security hardening 367
servers 30, 42, 43, 53
  co-resident with redundancy with DMZ 53
  Flash Media Gateway 43
  media cascading 42
  specifications 30
service level agreement 75
service packs 463
  installing 463
service URI 237
Setting operating system inactive account auditing ..368
shared bandwidth management 96
shut down 539
single sign-on 231
SIP domains 245
sla 75
SNMP service 197
  configuring 197
software installation 113
  checklist 113
specifications 29, 30, 33, 34, 37–40, 42, 43

dmz 33, 34
document conversion server 40
event conference server 40
Flash Media Gateway 43
media cascading server 42
media server 38
performance 29, 37
servers 30
standalone simplex 37
recording 37
standalone with redundancy 37
web conferencing management server 39
web server 39
SRTP 266
modifying the audio settings 266
standalone 27, 37–40
deployment layout 27
simplex 37
specifications 37
specifications 38–40
document conversion server 40
event conference server 40
media server 38
web conferencing management server 39
web server 39
with redundancy 37
specifications 37
standalone recording 275
standalone simplex 27, 60
deployment layout 27
starting the system 540
support 18
contact 18
synchronization 245
syslog server 125
configuration 125
system components 466
upgrading and patching 466
system manager 297, 298, 300, 301
system manager domain 246
adding 246
system requirements 52, 55–57, 60, 62
co-resident simplex layout 56
co-resident simplex with DMZ layout 57
Co-resident with redundancy layout 52
Co-resident with redundancy with DMZ layout 55
standalone simplex layout 62
standalone with redundancy layout 60
system status 224
verifying 224

T

target capacities 53
co-resident with redundancy with DMZ 53
third party CA 169, 567
third party certificates 168
TLS 207, 361
configuring for the Flash Media Gateway 361
disabling 207
training 18
related resources 18

U

upgrade 429–431, 439–441, 443, 451
database replication 429, 443
upgrading 365, 423, 438, 480, 483, 488
Element Manager 438, 483
Audio/Video in Collaboration Agent 365, 488
Avaya Aura Conferencing software 480
Element Manager 438, 483
MCP database 483
standalone deployment 423
upgrading a co-resident deployment 412
checklist 412
user accounts and passwords 126
verifying 126
user template 238, 239
users 282–284
bulk provisioning 283, 284
configuring the Recording feature 282
modifying 283

V

Verifying the warning banners 370
video 74
network impact 74
bandwidth 74
intra-frame coding 74
jitter 74
latency 74
motion mode 74
packet loss 74
sharpness mode 74
VMOS 74
video class of service 240
videos 18
Avaya Mentor 18

W

wan bandwidth 85
WAN bandwidth 85, 86
estimating bandwidth for video streams 85
estimating bandwidth for web conferencing 86
WCMS 435, 436
resync 436
web browser 24
web collaboration 397
web collaboration resources 254
associating with a location 254
web conferencing 182
modifying the meeting event processor for a management server 182
web conferencing management server 39
specifications 39
Web conferencing server 181
configuring 181
web server 39
specifications 39
Windows 7.0 24
Windows OS 193
Windows XP 24
without Avaya Media Server 87