



Upgrading and Patching Avaya Aura® Contact Center

Release 7.1
Issue 07.09
April 2024

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE). THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/licenseinfo) UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE

TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction	12
Purpose	12
Intended audience	12
Related resources	12
Avaya Aura® Contact Center documentation	12
Viewing Avaya Mentor videos	16
Support	17
Chapter 2: Changes in this release	18
Features	18
Ability to deploy Avaya Workspaces at any stage	19
Avaya Aura® Contact Center Release 7.1 Feature Pack 2 Post GA Patches supports Microsoft Windows 11	19
Avaya Aura® Contact Center Release 7.1 Feature Pack 2 Post GA Patches supports Microsoft Windows Server 2019	19
Avaya Aura® Contact Center Release 7.1 supports Microsoft Windows Server 2016	19
Disabling encryption not required for Contact Center upgrades	20
Ignition Wizard enhancements	20
NTP configuration of the Avaya Workspaces nodes	20
Support for Avaya Workspaces	20
Support for Avaya Workspaces High Availability	20
Workspaces HA Configurator	20
Avaya Workspaces features for Release 7.1.2.2	20
Other changes	21
Documentation update for Avaya Workspaces upgrades	22
Updated third-party software for the Avaya Workspaces cluster	22
Interoperability with the latest WebLM releases	22
VMware support	22
End of support for Internet Explorer	22
Windows operating system support	23
Avaya Aura® Media Server interoperability	23
Interoperability with Avaya Aura®	23
Chapter 3: Overview	24
Avaya Aura® Contact Center upgrades and migrations	24
Supported migrations	26
Backup locations	31
Migration of Avaya Aura® Midsize Business Template 5.2 to Avaya Aura® Unified Communications platform	32
Release Pack Installer	34
Update Manager	34
Migrating Contact Center campus HA solutions	34

Using a standby server to perform a migration on the same server hardware.....	34
Expanding a SIP-enabled Aura solution with a single server to support more agents.....	35
Expanding a CS 1000 AML-based solution with a single server to support more agents.....	36
Avaya Aura® Media Server on Linux.....	37
Avaya Aura® Media Server upgrades, migrations, and patches.....	38
Administration Client Transport Layer Security.....	41
Migrating security certificates.....	41
Database encryption considerations.....	42
Avaya Aura® Contact Center firewall considerations.....	43
Agent Desktop upgrades.....	43
Migrating custom Report Creation Wizard reports.....	44
Prerequisites.....	44
Chapter 4: Common server preparation procedures.....	45
Downloading the most recent documentation.....	45
Installing Microsoft Windows Server 2016 or Windows Server 2019.....	46
Navigating the Microsoft Windows Server 2016 or Windows Server 2019 interface.....	48
Installing the most recent supported operating system service packs.....	49
Connecting to the contact center subnet.....	50
Adding a server to a domain.....	50
Downloading the most recent Contact Center patches to the server.....	51
Disabling unused network adapters.....	52
Enabling Microsoft Remote Desktop connection.....	52
Disabling Admin Approval Mode for Windows Server administrators.....	52
Creating a shared location for security configuration.....	53
Securing the Windows server.....	54
Part 1: Voice and Multimedia Contact Server without Avaya Aura® Media	
Server migrations and patches.....	55
Chapter 5: Voice and Multimedia Contact Server without Avaya Aura® Media	
Server migration.....	56
Voice and Multimedia Contact Server without Avaya Aura® Media Server migration	
prerequisites.....	57
Voice and Multimedia Contact Server without Avaya Aura® Media Server migration	
procedures.....	58
Backing up the Database Integration Service configuration.....	62
Backing up the Avaya Aura® Contact Center Release 7.1 databases.....	63
Preparing custom RCW reports for migration.....	64
Backing up the Avaya Aura® Contact Center CCMA data.....	65
Backing up the Voice and Multimedia Contact Server Release 6.x databases.....	66
Backing up the Avaya Aura® Contact Center CCMS database.....	67
Backing up the Avaya Aura® Contact Center CCT database.....	68
Backing up the Avaya Aura® Contact Center CCMM database.....	68
Disabling Windows Server Automatic Maintenance.....	69

Installing the Voice and Multimedia Contact Server without Avaya Aura® Media Server software for Avaya Aura® Unified Communications platform.....	70
Configuring the Voice and Multimedia Contact Server without Avaya Aura® Media Server software for Avaya Aura® Unified Communications platform.....	73
Installing the Voice and Multimedia Contact Server software for CS1000.....	82
Configuring Voice and Multimedia Contact Server software for CS1000.....	84
Enabling Windows Server Automatic Maintenance	92
Backing up the new Avaya Aura® Contact Center Release 7.1 databases.....	93
Turning off Web Services security.....	93
Restoring the Database Integration Service configuration.....	94
Restoring the Voice and Multimedia Contact Server Release 7.1 databases.....	95
Restoring the Voice and Multimedia Contact Server databases.....	96
Restoring Contact Center Manager Administration data.....	98
Upgrading the Contact Center Manager Administration data.....	100
Starting Contact Center services.....	104
Configuring the Contact Center Manager Administration system components.....	106
Configuring the Contact Center Multimedia new details.....	107
Configuring Multimedia data management.....	107
Configuring settings for Multimedia Complement for Elite server migration.....	108
Converting custom RCW reports to Contact Center R7.1 format.....	109
Commissioning the Contact Center solution.....	110

Chapter 6: Voice and Multimedia Contact Server without Avaya Aura® Media

Server patch installation.....	111
Voice and Multimedia Contact Server without Avaya Aura® Media Server patch installation prerequisites.....	111
Disabling Windows Server Automatic Maintenance.....	112
Installing Voice and Multimedia Contact Server without Avaya Aura® Media Server Release Packs, Feature Packs and Service Packs.....	112
Installing Voice and Multimedia Contact Server without Avaya Aura® Media Server software patches.....	114
Enabling Windows Server Automatic Maintenance	114

Part 2: Voice Contact Server migrations and patches..... 116

Chapter 7: Voice Contact Server migration.....	117
Voice Contact Server migration prerequisites.....	118
Voice Contact Server migration procedures.....	118
Backing up the Database Integration Service configuration.....	122
Backing up the Avaya Aura® Contact Center Release 7.1 databases.....	122
Preparing custom RCW reports for migration.....	123
Backing up the Avaya Aura® Contact Center CCMA data.....	124
Backing up the Voice Contact Server Release 6.x databases.....	125
Backing up the Avaya Aura® Contact Center CCMS database.....	126
Backing up the Avaya Aura® Contact Center CCT database.....	127
Disabling Windows Server Automatic Maintenance.....	127

Installing the Voice Contact Server software for Avaya Aura® Unified Communications platform.....	128
Configuring the Voice Contact Server software for Avaya Aura® Unified Communications platform.....	131
Installing the Voice Contact Server software for CS1000.....	139
Configuring Voice Contact Server software for CS1000.....	142
Enabling Windows Server Automatic Maintenance	149
Backing up the new Avaya Aura® Contact Center Release 7.1 databases.....	150
Restoring the Database Integration Service configuration.....	150
Restoring the Voice Contact Server Release 7.1 databases.....	151
Restoring the Voice Contact Server databases.....	152
Restoring Contact Center Manager Administration data.....	154
Upgrading the Contact Center Manager Administration data.....	156
Starting Contact Center services.....	160
Configuring the Contact Center Manager Administration system components.....	162
Converting custom RCW reports to Contact Center R7.1 format.....	163
Commissioning the Contact Center solution.....	164
Chapter 8: Voice Contact Server patch installation.....	165
Voice Contact Server patch installation prerequisites.....	165
Disabling Windows Server Automatic Maintenance.....	165
Installing Voice Contact Server Release Packs, Feature Packs and Service Packs.....	166
Installing Voice Contact Server software patches.....	167
Enabling Windows Server Automatic Maintenance	168
Part 3: Multimedia Contact Server migrations and patches.....	170
Chapter 9: Multimedia Contact Server migration.....	171
Multimedia Contact Server migration prerequisites.....	171
Multimedia Contact Server migration procedures.....	172
Backing up the Avaya Aura® Contact Center Release 7.1 databases.....	175
Backing up the Multimedia Contact Server Release 6.x database.....	175
Disabling Windows Server Automatic Maintenance.....	176
Deploying the Avaya Workspaces OVA.....	177
Installing the Multimedia Contact Server software.....	179
Configuring the Multimedia Contact Server software.....	182
Enabling Windows Server Automatic Maintenance	188
Turning off Web Services security.....	189
Restoring the Multimedia Contact Server database.....	189
Configuring the Contact Center Multimedia new details.....	191
Configuring Multimedia data management.....	191
Commissioning the Contact Center solution.....	192
Chapter 10: Multimedia Contact Server patch installation.....	193
Multimedia Contact Server patch installation prerequisites.....	193
Disabling Windows Server Automatic Maintenance.....	193
Installing Multimedia Contact Server Release Packs, Feature Packs and Service Packs.....	194

Installing Multimedia Contact Server software patches.....	195
Enabling Windows Server Automatic Maintenance	196
Part 4: Voice and Multimedia Contact Server with Avaya Aura® Media Server migrations and patches.....	198
Chapter 11: Voice and Multimedia Contact Server with Avaya Aura® Media Server migration.....	199
Voice and Multimedia Contact Server with Avaya Aura® Media Server migration prerequisites.....	200
Voice and Multimedia Contact Server with Avaya Aura® Media Server migration procedures.....	201
Backing up the Database Integration Service configuration.....	205
Preparing custom RCW reports for migration.....	206
Backing up the Avaya Aura® Contact Center Release 7.1 databases.....	207
Backing up the Avaya Aura® Media Server database.....	208
Backing up the Voice and Multimedia Contact Server Release 6.x databases.....	209
Preparing the Avaya Media Server on Windows Content Store.....	210
Backing up the Avaya Media Server database.....	211
Backing up the Avaya Aura® Contact Center CCMA data.....	212
Backing up the Avaya Aura® Contact Center CCMS database.....	213
Backing up the Avaya Aura® Contact Center CCT database.....	214
Backing up the Avaya Aura® Contact Center CCMM database.....	214
Disabling Windows Server Automatic Maintenance.....	215
Installing the Voice and Multimedia Contact Server with Avaya Aura® Media Server software for Avaya Aura® Unified Communications platform.....	216
Configuring the Voice and Multimedia Contact Server with Avaya Aura® Media Server software for Avaya Aura® Unified Communications platform.....	219
Enabling Windows Server Automatic Maintenance	228
Backing up the new Avaya Aura® Contact Center Release 7.1 databases.....	229
Turning off Web Services security.....	229
Restoring the Database Integration Service configuration.....	230
Restoring the Voice and Multimedia Contact Server Release 7.1 databases.....	231
Logging on to Avaya Aura® Media Server Element Manager.....	232
Restoring the Avaya Aura® Media Server database	233
Resetting the Avaya Aura® Media Server IP address in Element Manager.....	234
Restoring the Avaya Aura® Media Server default license.....	234
Restoring the Voice and Multimedia Contact Server databases.....	235
Restoring Contact Center Manager Administration data.....	236
Upgrading the Contact Center Manager Administration data.....	238
Migrating the Avaya Media Server database.....	242
Completing the Avaya Aura® Media Server on Linux Content Store.....	243
Starting Contact Center services.....	244
Configuring the Contact Center Manager Administration system components.....	246
Configuring the Contact Center Multimedia new details.....	247

Configuring Multimedia data management.....	247
Configuring settings for Multimedia Complement for Elite server migration.....	248
Converting custom RCW reports to Contact Center R7.1 format.....	249
Commissioning the Contact Center solution.....	250
Chapter 12: Voice and Multimedia Contact Server with Avaya Aura® Media Server upgrade and patch installation.....	251
Voice and Multimedia Contact Server with Avaya Aura® Media Server patch installation prerequisites.....	252
Disabling Windows Server Automatic Maintenance.....	252
Installing Voice and Multimedia Contact Server with Avaya Aura® Media Server Release Packs, Feature Packs and Service Packs.....	253
Installing Voice and Multimedia Contact Server software patches.....	255
Installing Avaya Aura® Media Server patches on Linux.....	256
Enabling Windows Server Automatic Maintenance	257
Part 5: Avaya Aura® Media Server upgrades, migrations, and patches.....	258
Chapter 13: Avaya Aura® Media Server overview.....	259
Avaya Aura® Media Server upgrades, migrations, and patches.....	259
Chapter 14: Avaya Aura® Media Server to Avaya Aura® Media Server migration.....	263
Backing up the Avaya Aura® Media Server database.....	263
Installing the Linux server.....	264
Adding a Linux user group and user.....	267
Installing Avaya Aura® Media Server software on Linux.....	267
Configuring the Linux server for Avaya Aura® Media Server.....	269
Logging on to Avaya Aura® Media Server Element Manager.....	270
Restoring the Avaya Aura® Media Server database	271
Configuring the Avaya Aura® Media Server system parameters.....	271
Configuring Avaya Aura® Media Server name resolution.....	273
Resetting the Avaya Aura® Media Server IP address in Element Manager.....	273
Restoring the Avaya Aura® Media Server default license.....	274
Configuring the Linux Avaya Aura® Media Server in CCMA.....	274
Removing the existing Avaya Aura® Media Server from CCMA.....	275
Restarting Contact Center License Manager.....	276
Chapter 15: Avaya Media Server to Avaya Aura® Media Server migration.....	278
Preparing the Avaya Media Server on Linux Content Store.....	278
Backing up the Avaya Media Server database.....	279
Installing the Linux server.....	280
Adding a Linux user group and user.....	282
Installing Avaya Aura® Media Server software on Linux.....	283
Configuring the Linux server for Avaya Aura® Media Server.....	284
Migrating the Avaya Media Server database.....	285
Completing the Avaya Aura® Media Server on Linux Content Store.....	286
Logging on to Avaya Aura® Media Server Element Manager.....	287
Configuring the Avaya Aura® Media Server system parameters.....	288

Configuring Avaya Aura® Media Server name resolution.....	289
Configuring the Linux Avaya Aura® Media Server in CCMA.....	289
Removing the existing Avaya Media Server from CCMA.....	290
Chapter 16: Co-resident Avaya Aura® Media Server replacement.....	292
Prerequisites.....	292
Uninstalling co-resident Avaya Aura® Media Server from the Windows server.....	292
Chapter 17: Avaya Aura® Media Server OVA upgrade and patch installation.....	294
Prerequisites to Avaya Aura® Media Server patch installation.....	294
Updating Avaya Aura® Media Server OVA to Release 7.1	294
Installing Avaya Aura® Media Server patches on Linux.....	295
Installing the Avaya Aura® Media Server patches in High Availability.....	296
Part 6: Network Control Center Server migrations and patches.....	298
Chapter 18: Network Control Center server migration.....	299
Network Control Center Server migration prerequisites.....	299
Network Control Center Server migration procedures.....	300
Backing up the Avaya Aura® Contact Center Release 7.1 databases.....	303
Backing up the Avaya Aura® Contact Center CCMA data.....	303
Backing up the Avaya Aura® Contact Center Network Control Center database.....	304
Disabling Windows Server Automatic Maintenance.....	305
Installing the Network Control Center Server software.....	306
Configuring the Network Control Center Server software.....	309
Enabling Windows Server Automatic Maintenance	315
Backing up the new Avaya Aura® Contact Center Release 7.1 databases.....	316
Restoring the Network Control Center Release 7.1 databases.....	316
Restoring the Network Control Center Server database.....	318
Restoring Contact Center Manager Administration data.....	319
Upgrading the Contact Center Manager Administration data.....	321
Starting Contact Center services.....	325
Configuring the Contact Center Manager Administration system components.....	327
Commissioning the Contact Center solution.....	327
Chapter 19: Network Control Center Server patch installation.....	329
Network Control Center Server patch installation prerequisites.....	329
Disabling Windows Server Automatic Maintenance.....	329
Installing Network Control Center Server Feature Packs and Service Packs.....	330
Installing Network Control Center Server software patches.....	331
Enabling Windows Server Automatic Maintenance	332
Part 7: AML to SIP migrations.....	334
Chapter 20: AML to SIP Migration.....	335
Turning off Web Services security.....	336
Migrating the Voice and Multimedia databases to the SIP-enabled server.....	337
Restoring the Multimedia Contact Server database.....	338
Checking the Server Configuration settings on the new SIP-enabled server.....	339

Configuring Multimedia settings on the new SIP server.....	340
Restoring Contact Center Manager Administration data.....	341
Upgrading the Contact Center Manager Administration data.....	343
Completing CCMA and CCMM configuration on the new SIP-enabled server.....	347
Updating the CCMS and CCT configuration data.....	349
Generating the CCMS Workflow Compliance report.....	350
Part 8: Common procedures.....	352
Chapter 21: Common procedures for patching.....	353
Hot patching for Mission Critical High Availability.....	353
Hot patching for hot standby High Availability.....	355
Starting SMMC.....	358
Chapter 22: Avaya Workspaces upgrades.....	359
Deploying the Avaya Workspaces OVA.....	360
Configuring Avaya Workspaces during the initial installation.....	362
Configuring Avaya Workspaces using the Update Configurator.....	365
Downloading Contact Center Workspaces Patch Installer.....	366
Installing Avaya Workspaces patches.....	367
Chapter 23: Deploying Avaya Workspaces High Availability.....	369
Avaya Workspaces High Availability deployment on a physical server.....	369
Configuring Avaya Workspaces High Availability for a physical deployment using the Workspaces HA Configurator tool.....	370
Avaya Workspaces High Availability deployment on a virtual server.....	372
Deploying additional virtual machines for Avaya Workspaces High Availability.....	372
Configuring Avaya Workspaces High Availability for a virtual deployment using the Workspaces HA Configuration tool.....	374

Chapter 1: Introduction

This document contains the procedures to migrate customer information and install patches for Avaya Aura® Contact Center 7.1.x.

Purpose

This document contains migrating, upgrading, and patching procedures.

Intended audience

This document is intended for people who perform upgrades or who patch server software.

Related resources

Avaya Aura® Contact Center documentation

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

Title	Document purpose	Audience
Overview		

Table continues...

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

Table continues...

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

Table continues...


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

Table continues...

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

Finding documents on the Avaya Support website

Procedure

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.
This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.
For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click  to display the search results.

Viewing Avaya Mentor videos

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

About this task

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

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

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

In the right pane, the page displays a list of available videos.

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

 **Note:**

Videos are not available for all products.

Support

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

Chapter 2: Changes in this release

The following sections detail what has changed in *Upgrading and Patching Avaya Aura® Contact Center* Release 7.1.x.

Features

New features in the Release 7.1 base build

See the following sections for information about new features in Release 7.1 base build:

- [Avaya Aura Contact Center Release 7.1 supports Microsoft Windows Server 2016](#) on page 19
- [Ignition Wizard enhancements](#) on page 20
- [Support for Avaya Workspaces](#) on page 20

New features in Release 7.1 Service Packs 1 and 2

There are no new features in Release 7.1 Service Packs 1 and 2.

New features in Release 7.1 Service Pack 3

See the following sections for information about new features in Release 7.1 Service Pack 3:

- [Support for Avaya Workspaces High Availability](#) on page 20
- [Workspaces HA Configurator](#) on page 20

New features in Release 7.1 Feature Pack 1

See the following section for information about new features in Release 7.1 Feature Pack 1: [NTP configuration of the Avaya Workspaces nodes](#) on page 20.

New features in Release 7.1 Feature Pack 2

See the following sections for information about new features in Release 7.1 Feature Pack 2:

- [Ability to deploy Avaya Workspaces at any stage](#) on page 19
- [Disabling encryption not required for Contact Center upgrades](#) on page 20

New features in Release 7.1 Feature Pack 2 Post GA Patches

See the following sections for information about new features in Release 7.1 Feature Pack 2 Post GA Patches:

- [Avaya Aura Contact Center Release 7.1 Feature Pack 2 Post GA Patches supports Microsoft Windows 11](#) on page 19
- [Avaya Aura Contact Center Release 7.1 Feature Pack 2 Post GA Patches supports Microsoft Windows Server 2019](#) on page 19

New features in Release 7.1.2 Service Pack 2

See the following section for information about new features in Release 7.1.2 Service Pack 2: [Avaya Workspaces features for Release 7.1.2.2](#) on page 20.

Ability to deploy Avaya Workspaces at any stage

From Release 7.1 Feature Pack 2, you can deploy and configure the Avaya Workspaces cluster at any stage after you upgrade to the latest release. Using the Update Configurator, you can deploy the Avaya Workspaces cluster either during initial installation and configuration of the Contact Center release, or as a Day 2 operation.

Avaya Aura® Contact Center Release 7.1 Feature Pack 2 Post GA Patches supports Microsoft Windows 11

From Release 7.1 Feature Pack 2 Post GA Patches, Avaya Aura® Contact Center supports Microsoft Windows 11 for Avaya Agent Desktop, Contact Center Manager Administration, Contact Center Multimedia Administration, and Communication Control Toolkit.

Avaya Aura® Contact Center Release 7.1 Feature Pack 2 Post GA Patches supports Microsoft Windows Server 2019

Avaya Aura® Contact Center Release 7.1 Feature Pack 2 Post GA Patches supports the Microsoft Windows Server 2019 operating system. Customers that upgrade to Avaya Aura® Contact Center Release 7.1 Feature Pack 2 Post GA Patches and want to use Windows Server 2019 must perform a fresh installation on a new Microsoft Windows Server 2019. For more information about restoring the database to the new server, see *Upgrading and Patching Avaya Aura® Contact Center*.

Avaya Aura® Contact Center Release 7.1 supports Microsoft Windows Server 2016

The Avaya Aura® Contact Center Release 7.1 base build adds support for the Microsoft Windows Server 2016 operating system. Customers upgrading to Avaya Aura® Contact Center 7.1 on Windows Server 2016 must migrate to a new Microsoft Windows Server 2016 server.

Disabling encryption not required for Contact Center upgrades

Release 7.1 Feature Pack 2 removes the requirement to disable encryption when upgrading Contact Center, which decreases the overall time of the upgrading process.

Ignition Wizard enhancements

From Release 7.1 the following enhancements of Ignitions Wizard are implemented:

- Ignition Wizard now supports chained certificates
- Ignition Wizard now allows to remove the imported certificates
- Password complexity rules of Ignition Wizard are now aligned with Security Manager
- Ignition Wizard now has enhanced validation and reset options

NTP configuration of the Avaya Workspaces nodes

From Release 7.1 Feature Pack 1, you can synchronize your Avaya Workspaces nodes with the Contact Center environment using Network Time Protocol (NTP) servers. Set up the NTP servers before deploying or upgrading your Contact Center Release 7.1. You can use from one to three NTP servers, however, Avaya recommends that you use three. You can configure time synchronization settings in the new Other settings tab while configuring Avaya Workspaces in Ignition Wizard (for fresh installs) or in the Update Configurator (for upgrades).

Support for Avaya Workspaces

From Release 7.1, Contact Center supports Avaya Workspaces — a client for voice, video, email and webchat contact types.

Support for Avaya Workspaces High Availability

From Release 7.1 Service Pack 3, Avaya Aura® Contact Center supports Avaya Workspaces High Availability for fault tolerant and resilient contact center solutions. You can configure Avaya Workspaces High Availability for solutions that support both Mission Critical High Availability and Avaya Workspaces. For data resiliency and disaster recovery, you can also configure Geographic High Availability for Avaya Workspaces.

Workspaces HA Configurator

From Release 7.1 Service Pack 3, you can use Workspaces HA Configurator — a new tool for configuration, repair and administration of Avaya Workspaces High Availability.

Avaya Workspaces features for Release 7.1.2.2

Release 7.1.2.2 introduces the following Avaya Workspaces features for Avaya Aura® Contact Center (AACC) and Avaya Contact Center Select (ACCS). For more information about Avaya Workspaces features, see *Using Avaya Workspaces for AACC and ACCS*.

Consult, transfer, and conference options for web chat

You can consult with another agent during a chat interaction. Messages between agents are whispered so the customer does not see them.

If the other agent agrees, you can do one of the following when ending the consultation:

- Transfer the web chat to the other agent.
- Start a conference.

Observe web chat

A supervisor can observe a chat interaction from the My Agents widget.

Whisper coaching during web chat

While observing a chat interaction, the supervisor can start coaching. During the coaching session, the supervisor can whisper guidance to the agent. The customer does not see whispered messages.

Barge in to web chat

A supervisor can barge in to the chat interaction and communicate with the customer directly.

Email approval

A supervisor can approve or reject an email and add review comments. The agent can edit the email and add comments if it is rejected.

Reschedule email

You can postpone work on an email and reschedule it for a later time. This is a useful option if you need more time to gather information before completing the email.

Email transfer enhancements and new forwarding option

Previously, you could only transfer an email interaction to a skillset. Now, you can also transfer the email to another agent. In addition, you can also forward an email to any email address.

Multiple keyword search

You can use multiple keywords when searching through email templates and suggested content.

Customer history view

Customer history information for all contact types (voice and multimedia) is now displayed together in the same table.

Other changes

This section lists other changes for Release 7.1.x. Outdated information has been removed.

Other changes in Release 7.1 Feature Pack 2

See the following sections for information about other changes in Release 7.1 Feature Pack 2:

- [Documentation update for Avaya Workspaces upgrades](#) on page 22

- [Updated third-party software for the Avaya Workspaces cluster](#) on page 22

Other changes in Release 7.1.2 Service Pack 2

See the following sections for information about other changes in Release 7.1.2 Service Pack 2:

- [Interoperability with the latest WebLM releases](#) on page 22
- [VMware support](#) on page 22
- [End of support for Internet Explorer](#) on page 22
- [Windows operating system support](#) on page 23
- [Avaya Aura Media Server interoperability](#) on page 23
- [Interoperability with Avaya Aura](#) on page 23

Documentation update for Avaya Workspaces upgrades

From Release 7.1 Feature Pack 2, the Avaya Workspaces upgrades chapter has been added to *Upgrading and Patching Avaya Aura® Contact Center*. The new chapter provides more detailed information about upgrading and patching Avaya Workspaces in physical and virtual environments. See [Avaya Workspaces upgrades](#) on page 359.

Updated third-party software for the Avaya Workspaces cluster

Release 7.1 Feature Packs 1 and 2 include upgrades to a number of third-party components for the Avaya Workspaces cluster. Examples of components that have been upgraded to more recent versions include Kubernetes, Docker, Istio, and Kafka.

Interoperability with the latest WebLM releases

In Release 7.1.2.2, the latest versions of WebLM 8.1.3.x and 10.1.x are supported.

VMware support

Contact Center Release 7.1.2.2 supports ESXi 7.0 and 8.0 Update 2. Earlier VMware versions, including 6.5 and 6.7, are no longer supported.

See the [VMware website](#) for general lifecycle policy information.

End of support for Internet Explorer

Microsoft ended support for the Internet Explorer (IE) web browser in June 2022.

Many Contact Center applications, such as Contact Center Manager Administration (CCMA), Contact Center Multimedia (CCMM), and Communication Control Toolkit (CCT) require the IE engine. To run these applications, you must use Microsoft Edge in IE mode. If you are using Windows 10, IE can be disabled but cannot be removed from your computer. With Windows 11, you do not need to install the IE browser because Edge already includes the IE engine.

Windows operating system support

The following Microsoft operating systems are no longer supported:

- Windows 7 and 8.1
- Windows Server 2012 R2 and earlier versions

See the [Microsoft website](#) for lifecycle policy information.

Avaya Aura® Media Server interoperability

Contact Center now supports Avaya Aura® Media Server Release 10.1.x. Release 8.0.x is also supported.

Interoperability with Avaya Aura®

Avaya Aura® Contact Center Release 7.1.2.2 supports interoperability with Avaya Aura® Release 8.1.3, 10.1.x, and 10.2.

Chapter 3: Overview

Avaya Aura® Contact Center Release 7.1.x is supported on the Microsoft Windows Server 2016 and 2019 operating systems, Standard and Data Center editions. Your Microsoft Windows Server operating system and server must meet the requirements specified in *Avaya Aura® Contact Center Overview and Specification*.

To upgrade your solution to Avaya Aura® Contact Center Release 7.1.x without changing your operating system release, install the latest Avaya Aura® Contact Center software using the Contact Center Release Pack Installer (RPI). To upgrade your solution from a previous release with a different operating system, you must install the Windows Server 2016 or 2019 operating system, install Avaya Aura® Contact Center Release 7.1.x software, and then migrate your existing information to Windows Server.

After the migration, see *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* or *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000* for information about post-migration steps.

If you change the server name or the IP address of your server after upgrading, you must configure all servers with the new information. See *Avaya Aura® Contact Center Server Administration*.

SIP-enabled Avaya Aura® Contact Center solutions include and use Avaya Aura® Media Server.

Note:

- Avaya Aura® Contact Center and Avaya Aura® Media Server have independent patches, service packs, upgrade and patching procedures, and naming conventions.
- When upgrading to a minor or major release of Avaya Aura® Contact Center, you must schedule a maintenance window because Contact Center services are not available during upgrade or migration. However, if you have an HA solution, you can hot patch some Feature Packs, Service Packs and patches using Avaya RPI. To determine if the update supports hot patching, read the latest release notes and readme files. For more information, see [Hot patching for Mission Critical High Availability](#) on page 353 and [Hot patching for hot standby High Availability](#) on page 355.

Avaya Aura® Contact Center upgrades and migrations

You cannot upgrade directly from Avaya Aura® Contact Center Release 6.x on Windows Server 2008 to Avaya Aura® Contact Center Release 7.1.x on Windows Server 2016 or 2019. You can

migrate agent and statistical information from your existing Avaya Aura® Contact Center Release 6.x solution to Avaya Aura® Contact Center Release 7.1.x.

All Avaya Aura® Contact Center minor releases use the application of Release Packs, Feature Packs, or Service Packs as the upgrade method. Download and read the Release Notes for additional instructions to successfully upgrade Avaya Aura® Contact Center.

When you upgrade or migrate to Avaya Aura® Contact Center 7.1.x, you can choose to deploy and configure Avaya Workspaces. You must ensure that your solution hardware specifications meet the minimum requirements for Avaya Workspaces. Avaya Workspaces is supported on the following SIP-enabled Contact Center server types:

- Voice and Multimedia Contact Server with Avaya Aura® Media Server
- Voice and Multimedia Contact Server without Avaya Aura® Media Server
- Multimedia Contact Server

For more information about Avaya Workspaces hardware requirements, see *Avaya Aura® Contact Center Overview and Specification*.

When you are upgrading to Avaya Aura® Contact Center Release 7.0 Feature Pack 2 or later, the following limitations apply:

- If you are upgrading from Avaya Aura® Contact Center Release 7.0 or Release 7.0 Service Pack 1, you cannot upgrade directly to Avaya Aura® Contact Center Release 7.0 Feature Pack 2 or later. You must upgrade to Release 7.0 Feature Pack 1 before upgrading to Release 7.0 Feature Pack 2 or later.
- The mmReport user is recreated with the default password when you upgrade to Release 7.0 Feature Pack 3 or later. If you have previously changed the mmReport user password, you must change the password using the CCMM Administration utility after the upgrade is complete. This ensures that CCMM reporting is not impacted when you upgrade.

For a migration, install a new server with the most recent version of Contact Center and import the data from a previous Contact Center version.

The following steps describe the migration process.

1. On the existing Contact Center server, back up the databases to a secure network location.
2. On Windows Server 2016 or 2019, install Avaya Aura® Contact Center Release 7.1.x software.
3. Restore the old Contact Center databases to the new Avaya Aura® Contact Center Release 7.1.x server, converting the old databases where necessary.
4. Commission Avaya Aura® Contact Center Release 7.1.x.

You can migrate your existing Avaya Aura® Contact Center Release 6.x customer information to Avaya Aura® Contact Center Release 7.1.x.

! Important:

The following caveats apply to Avaya Aura® Contact Center Release 7.1.x upgrades and migrations:

- Do not upgrade your operating system from a previous release to Windows Server 2016 or 2019. Avaya Aura® Contact Center is not supported on an upgraded operating system.
- When you migrate configuration information from the old server to the new server, do not run the two application servers simultaneously. Both applications are configured the same way, so they attempt to access and control the same resources. Continuing to run the old applications in the new Contact Center can result in unpredictable behavior.
- When you are migrating your existing Avaya Aura® Contact Center, the Admin database must not be restored.
- If many web services are configured in the Database Integration Wizard (DIW), installations can time out while compiling these web services. An installation times out after 30 minutes. You can compile approximately 5500 web services in 30 minutes. If there are more than 5500 web services configured in the DIW, you must remove some web services before the feature pack or service pack install and import them after the installation completes. For more information about DIW, see *Avaya Aura® Contact Center Server Administration*.
- If you use local WebLM licensing, the WebLM password is reset to the default password after you upgrade Avaya Aura® Contact Center.

Supported migrations

You can migrate the information from previous versions of Avaya Aura® Contact Center to the new Avaya Aura® Contact Center Release 7.1.x server types by following the software migration procedures. Migration procedures move historical, statistical, and configuration information from a previous release to the new release of Contact Center.

The following Contact Center components and servers can migrate to a Voice and Multimedia Contact Server without Avaya Aura® Media Server:

- Migrate data from an existing Release 6.x co-resident server with Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit, and Contact Center Multimedia to a new Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server Release 7.1.x.
- Migrate data from an existing Release 6.x Contact Center Manager Server server, Contact Center Manager Administration server, Communication Control Toolkit server, and Contact Center Multimedia server to one new Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server Release 7.1.x.
- Migrate data from an existing Release 6.x Avaya Aura® Contact Center No Switch Configured Multimedia only server to a new Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server Release 7.1.x.

- Migrate data from an existing Release 6.x Avaya Aura® Contact Center Multimedia Complement for Elite server to a new Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server Release 7.1.x.
- Migrate a Release 7.0 Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server to a new Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server Release 7.1.x.
- Migrate a Release 7.1.x Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server to a new server. For example, to move Voice and Multimedia Contact Server without Avaya Aura® Media Server software from one server to a new larger and faster server.

Existing server	New Server
Avaya Aura® Contact Center Release 6.x on Windows Server 2008 R2.	Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server Release 7.1.x on Windows Server 2016 or Windows Server 2019. Server components: <ul style="list-style-type: none"> • Contact Center Manager Server (CCMS) • Contact Center Manager Server Utility • Contact Center License Manager (LM) • Contact Center Manager Administration (CCMA) • Communication Control Toolkit (CCT) • Contact Center Multimedia (CCMM)
Avaya Aura® Contact Center No Switch Configured Multimedia only server Release 6.x on Windows Server 2008 R2.	
Avaya Aura® Contact Center Multimedia Complement for Elite server Release 6.x on Windows Server 2008 R2.	
Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server Release 7.0 on Windows Server 2012 R2.	
Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server Release 7.1.x on Windows Server 2016 or Windows Server 2019.	

The following Contact Center components and servers can migrate to a Voice Contact Server:

- Migrate data from an existing Release 6.x co-resident server with Contact Center Manager Server, Contact Center Manager Administration, and Communication Control Toolkit to a new Avaya Aura® Contact Center Voice Contact Server Release 7.1.x.
- Migrate data from an existing Release 6.x Contact Center Manager Server server, Contact Center Manager Administration server, and Communication Control Toolkit server to one new Avaya Aura® Contact Center Voice Contact Server Release 7.1.x.
- Migrate a Release 7.0 Avaya Aura® Contact Center Voice Contact Server to one new Avaya Aura® Contact Center Voice Contact Server Release 7.1.x.
- Migrate a Release 7.1.x Avaya Aura® Contact Center Voice Contact Server to a new server. For example, to move Voice Contact Server software from one server to a new larger and faster server.

Existing server	New Server
Avaya Aura® Contact Center Release 6.x on Windows Server 2008 R2.	Avaya Aura® Contact Center Voice Contact Server Release 7.1.x on Windows Server 2016 or Windows Server 2019. Server components: <ul style="list-style-type: none"> • Contact Center Manager Server (CCMS) • Contact Center Manager Server Utility • Contact Center License Manager (LM) • Contact Center Manager Administration (CCMA) • Communication Control Toolkit (CCT)
Avaya Aura® Contact Center Voice Contact Server Release 7.0 on Windows Server 2012 R2.	
Avaya Aura® Contact Center Voice Contact Server Release 7.1.x on Windows Server 2016 or Windows Server 2019.	

The following Contact Center components and servers can migrate to a Multimedia Contact Server:

- Migrate data from an existing Release 6.x Contact Center Multimedia server to one new Avaya Aura® Contact Center Multimedia Contact Server Release 7.1.x.
- Migrate a Release 7.0 Avaya Aura® Contact Center Multimedia Contact Server to one new Multimedia Contact Server Release 7.1.x.
- Migrate a Release 7.1.x Avaya Aura® Contact Center Multimedia Contact Server to a new server. For example, to move Multimedia Contact Server software from one server to a new larger and faster server.

Existing server	New Server
Avaya Aura® Contact Center Release 6.x on Windows Server 2008 R2.	Avaya Aura® Contact Center Multimedia Contact Server without Avaya Aura® Media Server Release 7.1.x on Windows Server 2016 or Windows Server 2019. Server components: <ul style="list-style-type: none"> • Contact Center Multimedia (CCMM)
Avaya Aura® Contact Center Multimedia Contact Server Release 7.0 on Windows Server 2012 R2.	
Avaya Aura® Contact Center Voice Contact Server Release 7.1.x on Windows Server 2016 or Windows Server 2019.	

The following Contact Center components and servers can migrate to a SIP-enabled Voice and Multimedia Contact Server with Avaya Aura® Media Server:

- Migrate data from an existing Release 6.x single-server with Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit, Contact Center Multimedia and Avaya Media Server to a new Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server Release 7.1.x.
- Migrate data from an existing Release 6.x Contact Center Manager Server server, Contact Center Manager Administration server, Communication Control Toolkit server, Contact Center Multimedia server, and Avaya Media Server server to one new Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server Release 7.1.x.
- Migrate a Release 7.0 Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server to one new Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server Release 7.1.x.

- Migrate a Release 7.1.x Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server to a new server. For example, to move Voice and Multimedia Contact Server with Avaya Aura® Media Server software from one server to a new larger and faster server.

Existing server	New Server
Avaya Aura® Contact Center Release 6.x on Windows Server 2008 R2.	Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server Release 7.1.x on Windows Server 2016 or Windows Server 2019. Server components: <ul style="list-style-type: none"> • Contact Center Manager Server (CCMS) • Contact Center Manager Server Utility • Contact Center License Manager (LM) • Contact Center Manager Administration (CCMA) • Communication Control Toolkit (CCT) • Contact Center Multimedia (CCMM) • Avaya Aura® Media Server (Linux version on a Hyper-V instance)
Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server Release 7.0 on Windows Server 2012 R2.	
Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server Release 7.1.x on Windows Server 2016 or Windows Server 2019.	

The following Contact Center components or servers can migrate to an Avaya Aura® Contact Center Network Control Center Server:

- Migrate data from an existing Network Control Center Server to a new Avaya Aura® Contact Center Network Control Center Server Release 7.1.x.
- Migrate a Release 7.0 Avaya Aura® Contact Center Network Control Center Server to an Avaya Aura® Contact Center Network Control Center Server Release 7.1.x.
- Migrate a Release 7.1.x Avaya Aura® Contact Center Network Control Center Server to a new server. For example, to move Network Control Center Server software from one server to a new larger and faster server.

Existing system	New server
Avaya Aura® Contact Center Network Control Center Release 6.x on Windows Server 2008 R2.	Avaya Aura® Contact Center Network Control Center Release 7.1.x on Windows Server 2016 or Windows Server 2019. Server components: <ul style="list-style-type: none"> • Contact Center Manager Server (CCMS) • Contact Center License Manager (LM) • Contact Center Manager Administration (CCMA)
Avaya Aura® Contact Center Network Control Center Release 7.0 on Windows Server 2012 R2.	
Avaya Aura® Contact Center Network Control Center Release 7.1.x on Windows Server 2016 or Windows Server 2019.	

The following migrations are supported:

- Avaya Aura® Media Server on Windows to Avaya Aura® Media Server on Windows.
- Avaya Aura® Media Server on Linux to Avaya Aura® Media Server on Linux

Migrating Avaya Aura® Media Server from Windows to Linux or from Linux to Windows is not supported. Replacing an Avaya Aura® Media Server Windows server with an Avaya Aura® Media Server Linux server is supported.

Migrating Avaya Aura® Contact Center from CS 1000 to the Avaya Aura® Unified Communications platform is supported. Migrating Avaya Aura® Contact Center from a SIP-enabled CS 1000 to the Avaya Aura® Unified Communications platform is not supported. Migrating Avaya Aura® Contact Center from the Avaya Aura® Unified Communications platform to CS 1000 is not supported.

! Important:

When you migrate configuration information from the old server to the new server, do not run the two application servers simultaneously. Both applications are configured the same way, so they attempt to access and control the same resources. Continuing to run the old applications in the new Contact Center can result in unpredictable behavior.

Summary of migration options

The following table summarizes the supported migration paths and the configuration options to which you can migrate:

From release	From PABX type	Migrate to AACC R7.1.x AML (CS 1000)?	Server types for R7.1.x AML (CS 1000)	Migrate to AACC R7.1.x SIP (Aura)?	Server types for R7.1.x SIP (Aura)
AACC R6.x	SIP	N	—	Y	Voice and Multimedia Contact Server with Avaya Aura® Media Server OR Voice and Multimedia Contact Server without Avaya Aura® Media Server & Avaya Aura® Media Server OR Voice Contact Server & Avaya Aura® Media Server & Multimedia Contact Server

Table continues...

From release	From PABX type	Migrate to AACC R7.1.x AML (CS 1000)?	Server types for R7.1.x AML (CS 1000)	Migrate to AACC R7.1.x SIP (Aura)?	Server types for R7.1.x SIP (Aura)
AACC R6.x	AML	Y	Voice and Multimedia Contact Server without Avaya Aura® Media Server OR Voice Contact Server & Multimedia Contact Server	Y	Voice and Multimedia Contact Server with Avaya Aura® Media Server OR Voice and Multimedia Contact Server without Avaya Aura® Media Server & Avaya Aura® Media Server OR Voice Contact Server & Avaya Aura® Media Server & Multimedia Contact Server

Backup locations

A backup location is a physical network location used to store backup data or migration data. Before a migration, you must create a backup location to store backup data or migration data.

Use the Database Maintenance Utility to create a backup location. A backup location consists of the following elements:

- Drive letter
 - Currently unassigned in Windows (you cannot use existing, already mapped Windows drive letters)
 - Created during use (for example, to store backup data or migration data)
 - Removed after use
 - Used only with the Database Maintenance Utility
- UNC path
 - Use a valid uniform naming convention (UNC) path (for example, \cc_server\cc_share\cc_backup)
- Username
 - Windows account that connects to the location specified by the UNC path
 - Must include the computer name or IP address in the account name (for example, cc_server\administrator)

- Password
 - This is the password of the Windows account entered in the username above, which connects to the location specified by the UNC path

When the Database Maintenance application performs a database backup of Contact Center applications, it creates a folder called “AACCDDBBackup” in the backup location. To restore this backup on a different server (for example, to migrate to a new server), you must create a new backup location as part of the restore procedure. Exclude the folder created by the server application backup from the UNC path, as shown in the following examples:

- When performing a backup on an Avaya Aura® Contact Center server, you create a backup location with a UNC path of \\SERVER01\SharedFolder01\
- The backup creates a backup folder with the path \\\SERVER01\SharedFolder01\AACCDDBBackup
- To restore this backup on a new Avaya Aura® Contact Center server, the UNC path you enter to create the new backup location is \\SERVER01\SharedFolder01\
- The restore on the new server pulls the data from \\\SERVER01\SharedFolder01\AACCDDBBackup

Avaya Aura® Contact Center Release 7.1.x supports full database backups, so you can back up and restore all databases at once. If you are migrating or upgrading to Release 7.1.x from a previous release, you must back up all old databases. Store the old database backups in the same backup location because all databases are restored from this location at the same time.

Migration of Avaya Aura® Midsize Business Template 5.2 to Avaya Aura® Unified Communications platform

This section outlines how to migrate from Avaya Aura® Contact Center with an Avaya Aura® Midsize Business Template 5.2 to Avaya Aura® Contact Center with Avaya Aura® Unified Communications platform.

To proceed, perform the following actions:

- you must use the Avaya Aura® Contact Center Database Maintenance utility to backup the Avaya Aura® Contact Center (with MBT 5.2) database.
- Ensure the database is available at a network location to use with the new Avaya Aura® Contact Center Release 7.1 server. The backup location is used for restoring the database.
- Download all recent Avaya Aura® Contact Center patches to the new server.

If the database backup is from a co-resident server, multiple databases can be restored together. Otherwise, you must perform individual database restores from CCT, CCMS, and CCMM. When migrating or upgrading CCMM, do not restore “Offline” content.

To migrate from Avaya Aura® Contact Center with an Avaya Aura® Midsize Business Template 5.2 to Avaya Aura® Contact Center with Avaya Aura® Unified Communications platform, perform the following steps:

1. Install Avaya Aura® Contact Center Release 7.1 software on the new server.

During the installation select the most recent patches.

Avaya recommends that you use the same hostname and IP address details as the existing Avaya Aura® Contact Center (with MBT 5.2) server.

2. After the install, reboot the server.
3. Use the Avaya Aura® Contact Center Database Maintenance utility to restore the backup Avaya Aura® Contact Center (with MBT 5.2) database from the network location with the following parameters:

Parameter	Value
Network Location	Media Type
First application database to be restored	CCT
Restore contents	Data

4. Click **Restore**.
5. After the CCT database restore is complete, use the Avaya Aura® Contact Center Database Maintenance utility to restore the backup Avaya Aura® Contact Center (with MBT 5.2) database from the network location with the following parameters:

Parameter	Value
Network Location	Media Type
First application database to be restored	CCMS
Restore contents	Data

6. If you are using Contact Center Multimedia, after the CCMS database is restored, use the Avaya Aura® Contact Center Database Maintenance utility to restore the backup Avaya Aura® Contact Center (with MBT 5.2) database from the network location with the following parameters:

Parameter	Value
Network Location	Media Type
First application database to be restored	CCMM
Restore contents	Data

7. Use the CCMS - Server Configuration utility to update the configuration for the new Avaya Aura® Contact Center server.

Check the server IP, Outbound Voice and Computer Telephony Integration (CTI) proxies are valid for your system.

8. After the configuration is complete, click **Apply All**.
9. Reboot the server.

Release Pack Installer

Use the Contact Center Release Pack Installer (RPI) for installing Release Packs, Feature Packs, and Service Packs, and associated patch bundles.

Release Pack, Feature Pack, and Service Pack ZIP files include the Release Pack Installer (RPI) executable. The RPI ensures that you do not need to manually un-install software patches before upgrading Contact Center.

It also ensures that third party software updates remain consistent, and facilitates roll-back to a previous patch lineup.

Update Manager

Use the Contact Center Update Manager to view the patches currently on a Contact Center server. You can use Update Manager to install and uninstall patch bundles in the correct order. You must install patches for each server application in order of patch number, for example; 01, 02, 03.

You cannot use Update Manager to install Release Packs, Feature Packs, or Service Packs; you must use the Contact Center Release Pack Installer (RPI).

Migrating Contact Center campus HA solutions

When migrating from a solution with campus High Availability (HA), you take all backups from the active servers. Restore backups only to the new active server and then commission HA on Avaya Aura® Contact Center Release 7.1.x. If you need to synchronize the Contact Centers, you first stop shadowing and then synchronize with the active servers. After the synchronization is complete, commission HA using a fresh backup and restore of the active server.

Using a standby server to perform a migration on the same server hardware

About this task

A Contact Center using redundant servers has the option of migrating on the same server hardware. Therefore, you can use the standby server to migrate the Avaya Aura® Contact Center Release 6.x master to Avaya Aura® Contact Center Release 7.1.x. As an administrator, only consider this option if:

- You can accept the risk of operating the Contact Center in a non-redundant mode for the period of the migration.
- The existing Avaya Aura® Contact Center server hardware meets all the requirements for Release 7.1.x.

- You understand and accept the difficulties of reverting to the original configuration after both servers are migrated to Avaya Aura® Contact Center Release 7.1.x.

! Important:

Before deciding to perform a migration on a redundant Contact Center using the same hardware, consider the points above and the sequence of actions required to migrate the Contact Center. This option results in operating without redundancy for the period of the migration, and greatly complicates reverting to the previous release of Contact Center.

The following is an outline of how to migrate a redundant Contact Center on the same hardware:

1. Take the existing standby server offline. If it is a Contact Center Release 6.x server, you must first stop shadowing.
2. Install the Windows Server 2016 or Windows Server 2019 operating system on the server. Do not upgrade the operating system.
3. Install the Avaya Aura® Contact Center Release 7.1.x software on the server.
4. Commission the Avaya Aura® Contact Center Release 7.1.x server to be the active server.
5. Back up the data from the active server, and restore it on the Avaya Aura® Contact Center Release 7.1.x server.
6. Synchronize the Avaya Aura® Contact Center Release 7.1.x database.
7. Take the Contact Center server offline.
8. Install the former active server with Avaya Aura® Contact Center Release 7.1.x and commission it as a standby server.
9. Commission High Availability on the new servers.

Expanding a SIP-enabled Aura solution with a single server to support more agents

About this task

This section outlines what to do if you have a Voice and Multimedia Contact Server with Avaya Aura® Media Server, and if you want to enable more active agents than the single server can support.

*** Note:**

You must obtain new license files with increased agent counts and at least two new servers.

The expanded solution contains a Voice Contact Server, a Multimedia Contact Server, and, depending on the number of agents, one or more Avaya Aura® Media Servers.

Procedure

1. Obtain an Avaya Aura® Contact Center license file with the new increased agent count and an instance license for each new Avaya Aura® Media Server.

2. Obtain a Windows server suitable for the Multimedia Contact Server software and new agent count.
3. Obtain a Linux server suitable for the Avaya Aura® Media Server software and new agent count.
4. Backup all the Voice and Multimedia Contact Server databases on the existing server.
5. In CCMA, remove the local Avaya Aura® Media Server as a media services provider.
6. Uninstall Avaya Aura® Media Server from the existing server.
7. Uninstall CCMM software from the existing server. The existing server is now a Voice Contact Server.
8. Configure the Voice Contact Server to use the new license file with the increased agent count.
9. Install the Multimedia Contact Server software on the new Windows server.
10. Restore the CCMM database to the Multimedia Contact Server.
11. Reconfigure the CCMM Dashboard and General Settings on the Multimedia Contact Server to use the Voice Contact Server.
12. On the Voice Contact Server, in CCMA, re-add the Multimedia Contact Server as the CCMM server and refresh the other server types.
13. Install and commission the Avaya Aura® Media Server software on the new Linux server.
14. Reconfigure the Avaya Aura® Media Server media files.
15. Configure Avaya Aura® Media Server to trust the Voice Contact Server.
16. Reconfigure CCMA on the Voice Contact Server to use the new Avaya Aura® Media Server details.
17. Re-install all the Avaya Agent Desktops from the new Multimedia Contact Server.

Expanding a CS 1000 AML-based solution with a single server to support more agents

About this task

This section outlines what to do if you have a Voice and Multimedia Contact Server without Avaya Aura® Media Server, and if you want to enable more active agents than the single server can support. You must obtain a new license file with an increased agent count and one new server.

The expanded solution contains a Voice Contact Server and a Multimedia Contact Server.

Procedure

1. Obtain an Avaya Aura® Contact Center license file with the new increased agent count.

2. Obtain a server suitable for the Multimedia Contact Server software and the new agent count.
3. Backup all the Voice and Multimedia Contact Server databases on the existing server.
4. Uninstall CCMM software from the existing server. The existing server is now a Voice Contact Server.
5. Configure the Voice Contact Server to use the new license file with the increased agent count.
6. Install the Multimedia Contact Server software on the new server.
7. Restore the CCMM database to the Multimedia Contact Server.
8. Reconfigure the CCMM Dashboard and General Settings on the Multimedia Contact Server to use the Voice Contact Server details.
9. On the Voice Contact Server, in CCMA, re-add the Multimedia Contact Server as a CCMM server and refresh the other server types.
10. Re-install all the Avaya Agent Desktop clients from the new Multimedia Contact Server.

Avaya Aura® Media Server on Linux

Avaya Aura® Contact Center Release 7.1.x supports Avaya Aura® Media Server Release 8.0.x and 10.1 on the Linux operating systems.

Avaya Aura® Contact Center Release 7.1.x supports Avaya Aura® Media Server on Microsoft Windows Server 2016 or 2019, but only where Avaya Aura® Media Server software is installed co-resident with Avaya Aura® Contact Center.

The following migrations are supported:

- Avaya Aura® Media Server on Windows Server to Avaya Aura® Media Server on Windows Server
- Avaya Aura® Media Server on Linux to Avaya Aura® Media Server on Linux

Important:

Migrating from Avaya Aura® Media Server on Linux to Avaya Aura® Media Server on Windows is not supported. Direct migration from Avaya Aura® Media Server on Windows to Avaya Aura® Media Server on Linux is also not supported.

Avaya Aura® Media Server supports High Availability on the Linux operating system, but not on the Microsoft Windows Server operating system.

Avaya Aura® Media Server upgrades, migrations, and patches

Avaya Aura® Media Server is a software based media processing platform. All SIP-enabled Avaya Aura® Contact Center solutions require one or more Avaya Aura® Media Server systems.

Each release of Avaya Aura® Contact Center integrates with a newer, enhanced version of Avaya Aura® Media Server:

- AACC 7.1.2.2 integrates with Avaya Aura® Media Server Release 8.0.x and 10.1.x.
- AACC Release 7.0 Feature Pack 3 integrates with Avaya Aura® Media Server Release 7.8.
- AACC Release 7.0 Feature Pack 2 integrates with Avaya Aura® Media Server Release 7.7.0.391.
- AACC Release 7.0 Feature Pack 1 integrates with Avaya Aura® Media Server Release 7.7.0.348.
- AACC Release 7.0 integrates with Avaya Aura® Media Server Release 7.7.
- AACC Release 6.4 integrates with Avaya Media Server Release 7.6.
- AACC Release 6.3 integrates with Avaya Media Server Release 7.5.
- AACC Release 6.2 integrates with Avaya Media Server Release 7.0.
- AACC Release 6.1/6.0 integrates with Media Application Server software.

You can upgrade or migrate Avaya Aura® Media Server software. The latest versions of Avaya Aura® Media Server are supported on Red Hat Enterprise Linux (RHEL) 64-bit servers. Therefore, if you are upgrading from a previous version of AACC to AACC Release 7.1.x and Avaya Aura® Media Server is installed standalone on a Linux server, you must migrate Avaya Aura® Media Server software. If you are upgrading from AACC 7.0.3 to AACC Release 7.1.x and you are using an Avaya Aura® Media Server OVA, you can upgrade Avaya Aura® Media Server software.

- For an upgrade, you reuse an existing RHEL 64-bit server with a previous version of software on it and upgrade the Avaya Aura® Media Server software on that same server. When you upgrade the Avaya Aura® Media Server OVA, the operating system is automatically updated.
- For a migration, you install a new RHEL 64-bit server with Avaya Aura® Media Server software and import the data from the previous server.

The Avaya Aura® Contact Center Release Notes contain information about known issues, patches, procedures, and workarounds specific to a release and patch line-up of Avaya Aura® Contact Center and Avaya Aura® Media Server. For more information about the Avaya Aura® Contact Center Release Notes, see <https://support.avaya.com>.

Avaya Aura® Contact Center and Avaya Aura® Media Server have independent patches, service packs, upgrade and patching procedures, and naming conventions.

Avaya Aura® Media Server supports High Availability only on the Linux operating system. Avaya Aura® Media Server does not support High Availability on the Microsoft Windows Server operating systems. All Avaya Aura® Media Server systems in a contact center solution must be the same

release. All Avaya Aura® Media Server systems in a High Availability pair or cluster must be the same release and patch level.

Upgrades

If you migrate Avaya Aura® Contact Center software to Release 7.1.x, you must also upgrade or migrate all media servers in the solution to either Avaya Aura® Media Server Release 8.0.x or 10.1.x. Ensure that you upgrade or migrate all Avaya Aura® Media Server systems in the solution to the same release.

The following table lists the supported Avaya Aura® Media Server upgrade options:

Existing version of Avaya Aura® Media Server	Direct upgrade	Notes
Media Application Server (AACC 6.0 or 6.1)	No	You must first upgrade to Media Server Release 7.6 and apply the most recent patches. Run the data preparation utility. Next, upgrade to Avaya Aura® Media Server Release 7.7 and apply the most recent patches. Finally, you must migrate to either Avaya Aura® Media Server Release 8.0.x or 10.1.x.
Avaya Media Server Release 7.0 (AACC 6.2)	No	You must first upgrade to Media Server Release 7.6 and apply the most recent patches. Run the data preparation utility. You must then upgrade to Avaya Aura® Media Server Release 7.7 and apply the most recent patches. Finally, you must migrate to Avaya Aura® Media Server Release 8.0.x or 10.1.x.
Avaya Media Server Release 7.5 (AACC 6.3)	No	
Avaya Media Server Release 7.6 (AACC 6.4)	No	Apply the most recent Media Server Release 7.6 patches and run the data preparation utility. You must then upgrade to Avaya Aura® Media Server Release 7.7 and apply the most recent patches. Finally, migrate to Avaya Aura® Media Server Release 8.0.x or 10.1.x.
Avaya Aura® Media Server Release 7.7 (AACC 7.0)	No	Apply the most recent Avaya Aura® Media Server Release 7.7 patches. You must then migrate to Avaya Aura® Media Server Release 8.0.x or 10.1.x.
Avaya Aura® Media Server Release 7.8 (AACC 7.0.3)	Yes	Apply the most recent Avaya Aura® Media Server Release 7.8 patches. You can then upgrade or migrate to Avaya Aura® Media Server Release 8.0.x or 10.1.x., depending on your installation.

The Avaya Aura® Media Server 8.0.x or 10.1.x OVA supports direct upgrades only on a fully-patched Avaya Aura® Media Server 7.7 or 7.8 server.

If your existing contact center solution is not using the Avaya Aura® Media Server OVA, then you must use the migration procedures. Avaya Media Server to Avaya Aura® Media Server migrations support migrating the Application Content data and do not support migrating the System Configuration data.

Upgrading from Avaya Aura® Media Server on Windows to Avaya Aura® Media Server on Linux is not supported. Similarly, you cannot upgrade from Avaya Aura® Media Server on Linux to Windows.

Before upgrading Avaya Aura® Media Server software, ensure that the existing server hardware can support the newer version of software.

Upgrading to Release 7.1.x

When you install Avaya Aura® Contact Center Release 7.1.x, you must also upgrade Avaya Aura® Media Server to the correct version. For more information about updating Avaya Aura® Media Server on Windows, see [Voice and Multimedia Contact Server with Avaya Aura Media Server upgrade and patch installation](#) on page 251. For information about Linux, see [Avaya Aura Media Server OVA upgrade and patch installation](#) on page 294.

Important:

Avaya Aura® Media Server includes enhancements to the music streaming feature. If you are using RSS or SHOUTcast streaming, you must reconfigure music streaming after the upgrade.

Migrations

The following Avaya Aura® Media Server migrations are supported:

- Avaya Aura® Media Server Release 7.7, 7.8, or 8.0.x on Windows to Avaya Aura® Media Server Release 8.0.x or 10.1.x on Windows Server 2016 or Windows Server 2019. When you migrate, the Linux version of Avaya Aura® Media Server is deployed on a Hyper-V instance on Windows Server.
- Avaya Aura® Media Server Release 7.7, 7.8, or 8.0.x on Linux to Avaya Aura® Media Server Release 8.0.x or 10.1.x on a Red Hat Enterprise Linux 64-bit server.

For the migration, install Avaya Aura® Media Server software on the new server. Then back up the data from the existing server and restore it on the new server.

Avaya Aura® Contact Center does not support the following:

- Migrating Avaya Aura® Media Server from Linux to the Microsoft Windows operating system.
- Migrating an Avaya Aura® Media Server database from Linux to Microsoft Windows.

Avaya Media Server to Avaya Aura® Media Server migrations support migrating the Application Content data but not the System Configuration data.

The following Media Server migrations support only Application Content migration:

- Media Server Release 7.5 or 7.6 on Windows 2008 to Avaya Aura® Media Server on Windows Server 2016 or 2019.
- Media Server Release 7.5 or 7.6 on Windows 2008 to Avaya Aura® Media Server on RHEL.
- Avaya Aura® Media Server Release 7.7 on Windows 2012 to Avaya Aura® Media Server on RHEL.

Media Server Release 7.5 or 7.6 on Linux to Avaya Aura® Media Server on RHEL.

- Media Server Release 7.6 OVA to the Avaya Aura® Media Server 8.0.x or 10.1.x OVA.

Patches

You can apply Avaya Aura® Media Server patches to resolve product issues. Some Avaya Aura® Media Server patches are simple Quick Fix Engineering (QFE) patches, and some patches are more complex. You must read each Avaya Aura® Media Server patch Readme file and the Avaya Aura® Contact Center Release Notes to determine the correct procedures for each patch.

Administration Client Transport Layer Security

Contact Center implements Transport Layer Security (TLS) version 1.2 as the default minimum version negotiated for secure communications. This is to avoid security vulnerabilities that exist in TLS 1.0.

Before migrating, check that the browsers you use for CCMA or Element Manager are configured to use TLS 1.2. This ensures that the administration clients work immediately after the migration, and that you can continue with your post-migration commissioning.

Migrating security certificates

If your existing Release 6.x Contact Center is a SIP-enabled Aura solution, or you have configured TLS security on any Contact Center services, then the existing server has security certificates in one or more of the security stores supported on earlier releases. Contact Center Release 7.1 uses a single certificate for both the Contact Center security store and the IIS security store.

As a result, you cannot migrate a Contact Center security store from Release 6.x to Release 7.1. If you are migrating a secure Contact Center system from Release 6.x, you must create a new security store on the Release 7.1 Contact Center server.

If you are migrating from a Release 7.x server and want to reuse the certificates from your existing system:

- The new system must have exactly the same name and use the same domain as the existing system.
- You can reuse only the certificate in the Contact Center security store.
- Migrating the Contact Center security store is a manual process.

Migrating the Contact Center security store

To migrate the Contact Center security store from an existing Release 7.x server to a new Release 7.1 server:

- On the existing server, use Security Manager to back up the security store to a directory. Ensure you record the password for the old security store.

- Archive the directory into a single file, for example a zip file.
- Save the archived file to a network location.
- After migrating to the new Release 7.1 server, copy the archived file to the new server and unpack the directory.
- Use Security Manager to restore the security store on the new server.

Configuring a minimum TLS version

From Release 7.0 Feature Pack 1, Contact Center implements Transport Layer Security (TLS) version 1.2 as the default minimum version negotiated for secure communications. This is to avoid security vulnerabilities that exist in TLS 1.0.

For backward compatibility and inter-operation with third-party or custom applications connecting to Contact Center, Administrators can set lower versions of TLS on certain communication channels.

If your Contact Center solution includes systems that support only lower TLS versions, ensure you set the minimum TLS version after migration. For more information on setting minimum TLS settings, see *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* or *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000*.

Database encryption considerations

Upgrades

You can upgrade your Contact Center solution with encrypted or not encrypted databases. The preliminary decryption of all databases is not required.

Note:

When downgrading Contact Center, you must decrypt all databases.

Migrations

When you migrate your Contact Center solution, you can restore Contact Center databases that are encrypted or are not encrypted.

If you want to restore an encrypted database to the new server, you must ensure that you use the same encryption key as the old server. You must also ensure that this existing key is activated before you perform the restore.

If you want to use a new encryption key on the new server, restoring an encrypted database is not supported. You must decrypt the Contact Center database on the old server before you perform the backup.

For more information about database encryption, see *Avaya Aura® Contact Center Server Administration*.

Avaya Aura® Contact Center firewall considerations

Avaya Aura® Contact Center supplies a customized Windows Firewall Security policy. After you install Avaya Aura® Contact Center, Avaya recommends that you do not make changes to the AACC Firewall Policy.

When you install a Service Pack on your Contact Center server, the Service Pack applies the most recent version of the AACC Firewall Policy; any changes previously made to the AACC Firewall Policy are therefore lost. If you make changes to the AACC Firewall Policy, you must manually track and manage these changes.

Agent Desktop upgrades

When you migrate or upgrade a server type that has CCMM, or apply a CCMM patch that includes changes for Agent Desktop, a new version of the Agent Desktop client is included.

For ClickOnce deployments, Agent Desktop prompts the agent to install the upgrade when the agent opens the client.

For MSI deployments, Avaya recommends that you install the newer version of the Agent Desktop client when migrating, upgrading, or patching the AACC server. Release Bundle zip files include an updated Agent Desktop MSI file, if applicable, in the `\Install Software\CCMM` folder. Alternately, you can update the AACC server and then open Agent Desktop on a client computer.

Contact Center supports backwards compatibility with the previous Feature Pack or Service Pack version of Agent Desktop. This allows you to upgrade the Contact Center server without the requirement to upgrade Agent Desktop in a single maintenance window. For example, if you upgrade to Release 7.0 Feature Pack 3, you can use the Release 7.0 Feature Pack 2 version of Agent Desktop. New Agent Desktop features added in the latest Contact Center release are not available until you upgrade Agent Desktop to that release. Backwards compatibility is not supported for major or minor releases. For example, if you upgrade to Release 7.1, you cannot use the Release 7.0 version of Agent Desktop.

Agent Desktop displays a message to inform you if the Agent Desktop version on the server is different to that on the client. For instructions on Agent Desktop silent installation using the MSI, see *Deploying Avaya Aura® Contact Center DVD for Avaya Aura® Unified Communications* or *Deploying Avaya Aura® Contact Center DVD for Avaya Communication Server 1000*. The MSI uninstalls the previous version of the client, you do not need to uninstall it manually.

When you upgrade Avaya Aura® Contact Center, the previous versions of .NET are removed. The .NET Framework updates are cumulative with previous minor versions; when you install a newer version of .NET Framework, the previous minor versions remain.

Migrating custom Report Creation Wizard reports

Custom historical reports built with Report Creation Wizard (RCW) in earlier releases are not compatible with SSRS reports on Contact Center Release 7.1.

You can migrate custom historical reports from the existing server to the new server. First use the report migration utility on the existing server to convert the existing reports from Crystal format. The report migration utility creates a zip file of your custom reports. Then copy the zip file to the new server, and use RCW to import the custom reports.

Important:

You cannot migrate custom reports that were not built with RCW. You must rebuild these reports on the new server using RCW or Microsoft® SQL Server® 2012 Report Builder.

If the custom reports use custom formulas on the existing server, the formulas do not migrate with the custom reports.

Contact Center creates a placeholder formula for each custom formula. The placeholder displays an asterisk character on the migrated report. If possible, the placeholder formula includes the original Crystal Syntax formula text as a comment. You must edit the placeholder formulas, entering valid SSRS expressions for the formula text, to complete the migration. The placeholder formula is limited to 32,000 characters, so it is possible that very long formulas can be truncated.

Document all the custom formulas on the existing server, to assist with re-creating them on the new server after migrating the Contact Center databases.

Prerequisites

- Download the most recent documentation from the Avaya website (<http://support.avaya.com>).
- Read *Avaya Aura® Contact Center Overview and Specification* to ensure that your configuration meets the Contact Center Release 7.1 requirements.
- Understand the features you purchased and have a license file.
- Know on which computer to upgrade each Contact Center component.
- Ensure you have the Contact Center DVD.
- If your current solution integrates with Proactive Outreach Manager, you must update POM to align with the release that is supported with Release 7.1.

Chapter 4: Common server preparation procedures

This chapter provides the common procedures to prepare the servers that you need to install the Avaya Aura® Contact Center server software. You must perform the procedures in this chapter on each Windows Server you plan to use.

If the server is to be used in a domain, Avaya recommends that you add the server to the domain before installing Contact Center software.

You can change the name of an Avaya Aura® Contact Center server, but because this is time consuming, Avaya recommends that you configure the server final production name before installing Contact Center software.

If you plan to follow the Microsoft server hardening guidelines, complete those procedures before installing Avaya Aura® Contact Center.

You can use any account with local administrative rights to install Avaya Aura® Contact Center. You can use any account with local administrative rights to upgrade and patch Avaya Aura® Contact Center; you do not need to always use the same account to perform these tasks. You can delete or disable the install account at any time, without impacting Avaya Aura® Contact Center operation.

Important:

You must disable the Admin Approval Mode security feature on the Contact Center server. This ensures that accounts with local administrative rights get full privileges for running applications on the Contact Center server.

This chapter describes the common procedures for Windows Server. If you are installing Avaya Aura® Media Server on Linux see [Avaya Aura Media Server upgrades, migrations, and patches](#) on page 258.

Complete the procedures in this section in sequential order.

Downloading the most recent documentation

Before you begin

- Access the Avaya website at <http://support.avaya.com>.
- Download the most recent version of Acrobat Reader.

About this task

Download the most recent documentation to ensure you have the most recent updates. Updates in the documentation accurately reflect the most recent changes in the software.

Procedure

1. Log on to the Avaya website.
2. Compare the versions of the documentation on the site with the versions you have.
3. If the version number on www.avaya.com is later than your version, download the most recent version of the document.
4. Review the Avaya website for release notes and readme files.

Installing Microsoft Windows Server 2016 or Windows Server 2019

Before you begin

- Ensure that you have a newly-formatted server on which to install Microsoft Windows Server 2016 or Windows Server 2019. The server must meet the specifications in *Avaya Aura® Contact Center Overview and Specification*.
- Do not upgrade your operating system from a previous release. Contact Center is not supported on an upgraded operating system.
- Configure all servers for RAID as described in *Avaya Aura® Contact Center Overview and Specification*.
- Ensure that you have a DVD for Microsoft Windows Server 2016 or 2019 Standard or Data Center edition.
- Ensure that you have a Microsoft Windows Server 2016 or 2019 operating system product key.
- Ensure that you know the IP addresses for the contact center subnet.

About this task

Install the Microsoft Windows Server 2016 or Windows Server 2019 Standard or Data Center operating system and configure it to support Contact Center server software.

The following table lists the main inputs to consider while installing the operating system:

Name	Description
Computer name	Do not use spaces or underscores or exceed 15 characters. The name must start with an alphabetic character. Server names must adhere to RFC1123. Avaya recommends that you configure the server's final production name before installing Contact Center software. The computer name must match the DNS name. It is case sensitive.

Table continues...

Name	Description
Disk drives	Format the partitions as required for the server. For more information, see <i>Avaya Aura® Contact Center Overview and Specification</i> .
Domain name	Configure as required for your site. You must check to ensure the DNS domain name (including case) matches the server name if the server is added to a domain after configuration.
Licensing modes	Select Per server licensing mode. Accept the five default concurrent connections.
Network components	Configure the IP address, WINS, and DNS for one or two network cards as appropriate. Contact Center does not support IPv6.
Network connections	If the server has more than one NIC/adaptor, ensure contact center subnet is displayed first in the network adapter binding order.
Hard Disk Partitions	Configure C: drive as the primary drive. Configure the other drives on your server to meet the requirements according to <i>Avaya Aura® Contact Center Overview and Specification</i> for the server.

Perform this procedure on each server before you install Contact Center server software on the server.

Procedure

1. Insert the Microsoft Windows Server 2016 or Windows Server 2019 Standard or Data Center DVD into the DVD drive.
2. Turn on the power to the server.
The server begins to boot up.
3. On the Windows Setup page, select a language from the **Language to install** list.
4. Select a **Time and currency format** from the list.
5. Select **Keyboard or input method** from the list.
6. Click **Next**.
7. Click **Install now**.
8. On the Activate Windows window, enter the operating system product key.
9. Click **Next**.
10. Select a version of Windows Server 2016 or Windows Server 2019 Standard or Data Center that includes the **Desktop Experience** option.
11. Click **Next**.
12. Read and accept the terms of the license agreement.
13. Click **Next**.
14. Select **Custom: Install Windows only (advanced)** to install a clean new installation of the operating system.

15. Select the disk partition on which you want to install Windows Server 2016 or Windows Server 2019.

You can use the partition management options to configure the partitions on your server.

16. Click **Next**.

The installation proceeds and automatically restarts the server several times.

17. After completing the installation, log in to the server as Administrator.

You must enter and confirm the Administrator password.

18. After logging in, configure the time zone settings for your server.

19. Specify the server IP address for your Network Interface Card (NIC).

20. Configure your computer name and domain.

21. **(Optional)** Change the DVD drive letter to E: to ensure the correct drive letters are free for the Contact Center application and database hard disk drives and partitions.

22. Configure the hard disk drives and partitions for this server using the Windows Server 2016 or Windows Server 2019 Computer Management - Disk Management utility.

23. Install other required drivers for your hardware configuration.

Navigating the Microsoft Windows Server 2016 or Windows Server 2019 interface

The following table describes some key Microsoft Windows Server 2016 and Windows Server 2019 user interface items.

User interface item	Description
Start menu	The Start menu button opens a list of shortcuts to the main administration interfaces of the server, including shortcuts to Contact Center applications. The Start menu displays the currently logged on user and provides some basic server logout and locking functions. This menu offers similar functionality as the Windows Server 2012 R2 Start and App pages. Note that Windows Server 2012 R2 is no longer supported.
Desktop	The Desktop screen contains the Windows Start button, Taskbar, Recycle Bin, and shortcuts to the Windows Explorer utility, among others. The Taskbar displays the Windows Notification Area and System Tray. The notification area is located on the right portion of the Taskbar next to the time.

Navigation tips:

- To display the **Start** menu, on the desktop, click the Windows **Start** button.
- To access the control panel, on the **Start** menu, click the **Control Panel** tile.

- To access administration tools, on the **Start** menu, click the **Windows Administrative Tools** tile.

The contents of your screens can vary depending on the roles, features, and applications installed on your server.

For more information about the Windows Server 2016 or Windows Server 2019 operating system, refer to the Microsoft support website and Microsoft product documentation.

 **Important:**

Instructions in the Contact Center documentation might vary depending on the Windows Server version you are using.

Installing the most recent supported operating system service packs

Before you begin

- Access the Avaya hotfixes list on the website <https://support.avaya.com>.
- Install and configure Microsoft Windows Server 2016 or 2019 on your server.
- Review the specifications for operating system service updates in *Avaya Aura® Contact Center Overview and Specification*.

About this task

Avaya recommends that you install the most recent supported operating system service packs. You must download the supported operating system service pack from the Avaya hotfixes list to ensure your Contact Center server software functions correctly with the supported operating system patches.

Procedure

1. Review the Contact Center Service Packs Compatibility and Security Hotfixes Applicability List to determine the most recent supported Avaya Aura® Contact Center patches or service packs.
2. Download the appropriate Windows Server patches for the Avaya Aura® Contact Center software installed on this server.
3. Install the most recent Windows Server service pack that is validated with Avaya Aura® Contact Center by following the Microsoft installation instructions.

Connecting to the contact center subnet

About this task

Connect the Contact Center server to the contact center subnet. The contact center subnet is the network on which the server software applications work together to route contacts and generate reports.

Procedure

1. Locate the slot assigned to the contact center subnet network interface card for the server. Make a note of the slot.
2. Connect the cable from the contact center subnet to the contact center subnet network interface card in the server in accordance with customer site networking guidelines.
3. Use the ping command to test the contact center subnet.

Adding a server to a domain

Before you begin

- Ensure that you have domain administrator privileges, or ask the Domain Administrator to assign you a domain user account for remote access.
- On the server, configure a preferred Domain Name System (DNS) server on the Network Interface Card (NIC).

About this task

Add the server to an existing domain.

Note:

Add the server to a Windows domain before installing Contact Center software. When joining the domain, ensure the server time and domain controller time are synchronized to the same time.

Ask your System Administrator to add a Domain Name System (DNS) static entry for this server. Each Contact Center server in a domain requires a DNS static entry.

Procedure

1. Log on to the server.
2. On the **Start** screen, select **Administrative Tools** > **Server Manager**.
3. In the left pane, select **Local Server**.
4. In the right pane, in the **Properties** section, double-click on the **Domain** value.
The **System Properties** dialog box appears.
5. In the **System Properties** dialog box, click the **Computer Name** tab.

6. Click **Change**.
7. In the **Member of** section, click the **Domain** option.
8. Type the domain name (you must provide the fully qualified domain name, which includes the prefix and suffix).
9. Click **OK**.
10. Type the domain administrator **User name** and **Password**.
11. Click **OK**.
12. Restart the server when you are prompted to do so.

Downloading the most recent Contact Center patches to the server

Before you begin

- Download and install the most recent and supported updates per Microsoft Windows Server 2016 or 2019.
- Know the location where plan to install each Contact Center server software package.
- Ensure that you use one administrator account on your server to uninstall and install software updates.

About this task

To ensure that you have the most current software, download the most recent Contact Center patches from <https://support.avaya.com> to the server you plan to install.

Procedure

1. Log on to the server using the administrator account.
2. Create a folder <Drive>:\Avaya-ProductUpdates\ to save the software updates, where <Drive> is the drive letter on which you want to save the Contact Center software updates.
3. Download the most recent service pack file.
4. Save and unzip the file on the Contact Center server in the Avaya-ProductUpdates folder.
5. If new patches are available for the latest service pack, download and save the patches in the Avaya-ProductUpdates folder.
6. Read the Contact Center Release Notes for the latest instructions.

Disabling unused network adapters

About this task

Disable all unused Network Adapters or NICs to improve network communications and prevent the erroneous configuration of unused NICs during Contact Center server commissioning.

Procedure

1. Log on to the server.
2. Navigate to **Start > Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings**.
3. Right-click on the unused network adapter and then click **Disable**.
4. Repeat this procedure for all unused network adapters.

Enabling Microsoft Remote Desktop connection

About this task

Enable Microsoft Remote Desktop connection as your remote access tool. Microsoft Remote Desktop provides remote access for support on the server.

Procedure

1. Log on to the server with administrator privileges.
2. On the **Start** screen, select **Control Panel > System and Security**.
3. In the **System** section, select **Allow remote access**.
4. Click the **Remote** tab.
5. Select **Allow remote connections to this computer**.
6. Click **Apply**.
7. Click **OK**.

Disabling Admin Approval Mode for Windows Server administrators

About this task

Windows Server implements a security feature known as User Account Control (UAC). By default, this feature causes applications run by local non built-in administrators to behave as if the applications had been run by standard users. Perform this procedure to ensure that local administrators get full privileges for running applications.

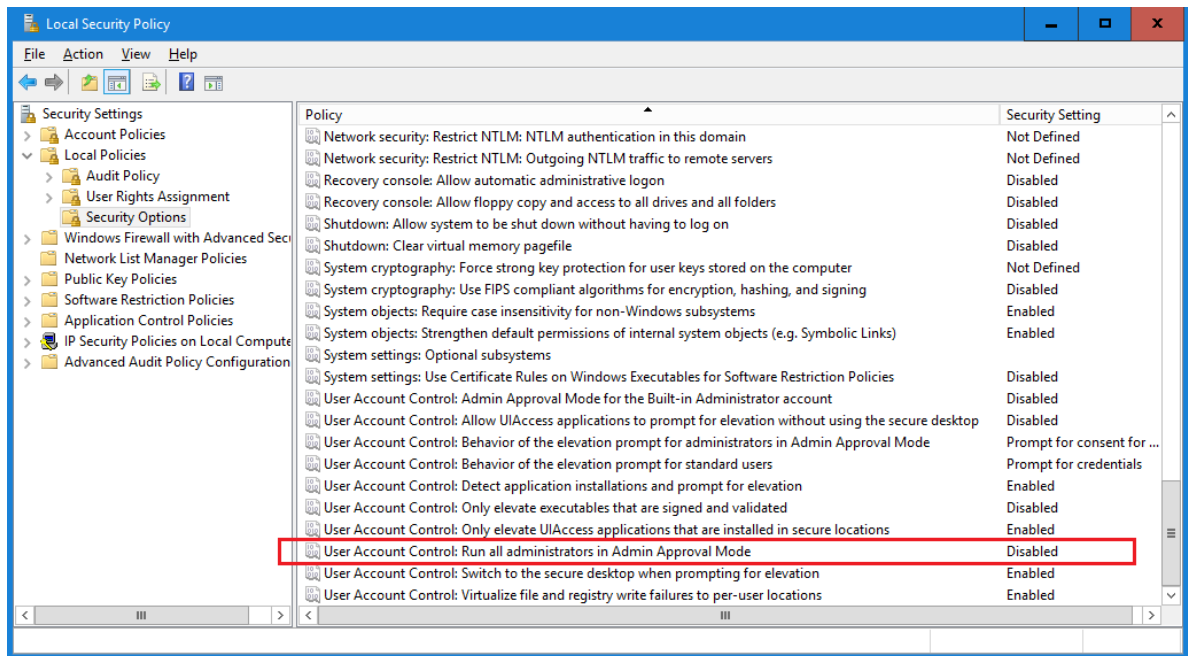
*** Note:**

This procedure describes how to disable Admin Approval Mode on the Contact Center server using one method only; there are additional methods available. For example, you can also administer User Account Control settings for the Contact Center server using a group policy.

Procedure

1. On the **Start** screen, select **Administrative Tools** > **Local Security Policy**.
2. Under **Security Settings**, expand **Local Policies**.
3. Select **Security Options**.
4. In the policy pane on the right, double-click on **User Account Control: Run all administrators in Admin Approval Mode**.
5. Click the **Local Security Setting** tab, and select **Disabled**.
6. Click **OK**.

If prompted, restart the server.



Creating a shared location for security configuration

About this task

If you want to enable security on the Contact Center server, and complete security configuration when installing Contact Center software, you must ensure that a shared network location exists on

the Contact Center server. You can then export the Certificate Signing Request (CSR) file to this location using the Contact Center Ignition Wizard.

Procedure

Create a shared network location on the Contact Center server.

Securing the Windows server

About this task

Apply optional security measures to your operating system to further secure your server.

Important:

Scanning software can degrade the performance and decrease the reliability of the system. Install virus scanning software only if the system connects to an exposed network or to the internet.

To maintain server performance, you must schedule virus scans during maintenance periods or low usage hours only.

Procedure

1. Harden the operating system using defined site procedures.
2. Install antivirus software if required.

If you install antivirus software, Avaya recommends that you exclude some contact center files and folders from real-time and scheduled scans. For more information, and for a list of files and folders to exclude, see *Avaya Aura® Contact Center Overview and Specification*.

Part 1: Voice and Multimedia Contact Server without Avaya Aura[®] Media Server migrations and patches

- [Voice and Multimedia Contact Server without Avaya Aura Media Server migration](#) on page 56
- [Voice and Multimedia Contact Server without Avaya Aura Media Server patch installation](#) on page 111

Chapter 5: Voice and Multimedia Contact Server without Avaya Aura® Media Server migration

This chapter describes how to migrate Avaya Aura® Contact Center Release 6.x to a new server running Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server Release 7.1.x. This chapter also provides information about migrating Voice and Multimedia Contact Server without Avaya Aura® Media Server from one server to another.

Existing server	New Server
Avaya Aura® Contact Center Release 6.x on Windows Server 2008 R2	Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server Release 7.1.x on Windows Server 2016 or 2019
Avaya Aura® Contact Center No Switch Configured Multimedia only server Release 6.x on Windows Server 2008 R2	
Avaya Aura® Contact Center Multimedia Complement for Elite server Release 6.x on Windows Server 2008 R2	
Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server Release 7.0 on Windows Server 2012 R2	
Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server Release 7.1.x on Windows Server 2016 or 2019	

This section describes how to migrate from an existing Avaya Aura® Unified Communications SIP enabled solution to a new Avaya Aura® Contact Center Release 7.1.x SIP enabled solution.

This section also describes how to migrate from an existing Avaya Communication Server 1000 AML-based solution to a new Avaya Aura® Contact Center Release 7.1.x AML-based solution.

You can use the procedures in this chapter to:

- Migrate data from your existing co-resident Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit and Contact Center Multimedia server to a new Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server.

- Migrate data from your existing Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit and Contact Center Multimedia to a single Voice and Multimedia Contact Server without Avaya Aura® Media Server.
- Migrate data from an existing Release 6.x Avaya Aura® Contact Center No Switch Configured Multimedia only server to a new Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server Release 7.1.x.
- Migrate data from an existing Release 6.x Avaya Aura® Contact Center Multimedia Complement for Elite server to a new Avaya Aura® Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server Release 7.1.x.
- Migrate a Voice and Multimedia Contact Server without Avaya Aura® Media Server to a new server. For example, to move Voice and Multimedia Contact Server without Avaya Aura® Media Server Release 7.1.x software from one server to a new and faster server.

A Voice and Multimedia Contact Server without Avaya Aura® Media Server includes the following server software:

- Contact Center Manager Server (CCMS)
- Contact Center Manager Server Utility
- Contact Center License Manager (LM)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center Multimedia (CCMM)
- Avaya Workspaces (optional)

Voice and Multimedia Contact Server without Avaya Aura® Media Server migration prerequisites

- Ensure that your hardware meets all requirements as described in *Avaya Aura® Contact Center Overview and Specification*.
- Prepare your new server for software installation. For more information see, [Common server preparation procedures](#) on page 45.
- If you are migrating from AAACC Release 6.x, archive contacts from the CCMM database.

Voice and Multimedia Contact Server without Avaya Aura® Media Server migration procedures

About this task

This task flow shows you the sequence of procedures you perform to migrate to an Avaya Aura® Contact Center Release 7.1 Voice and Multimedia Contact Server without Avaya Aura® Media Server.

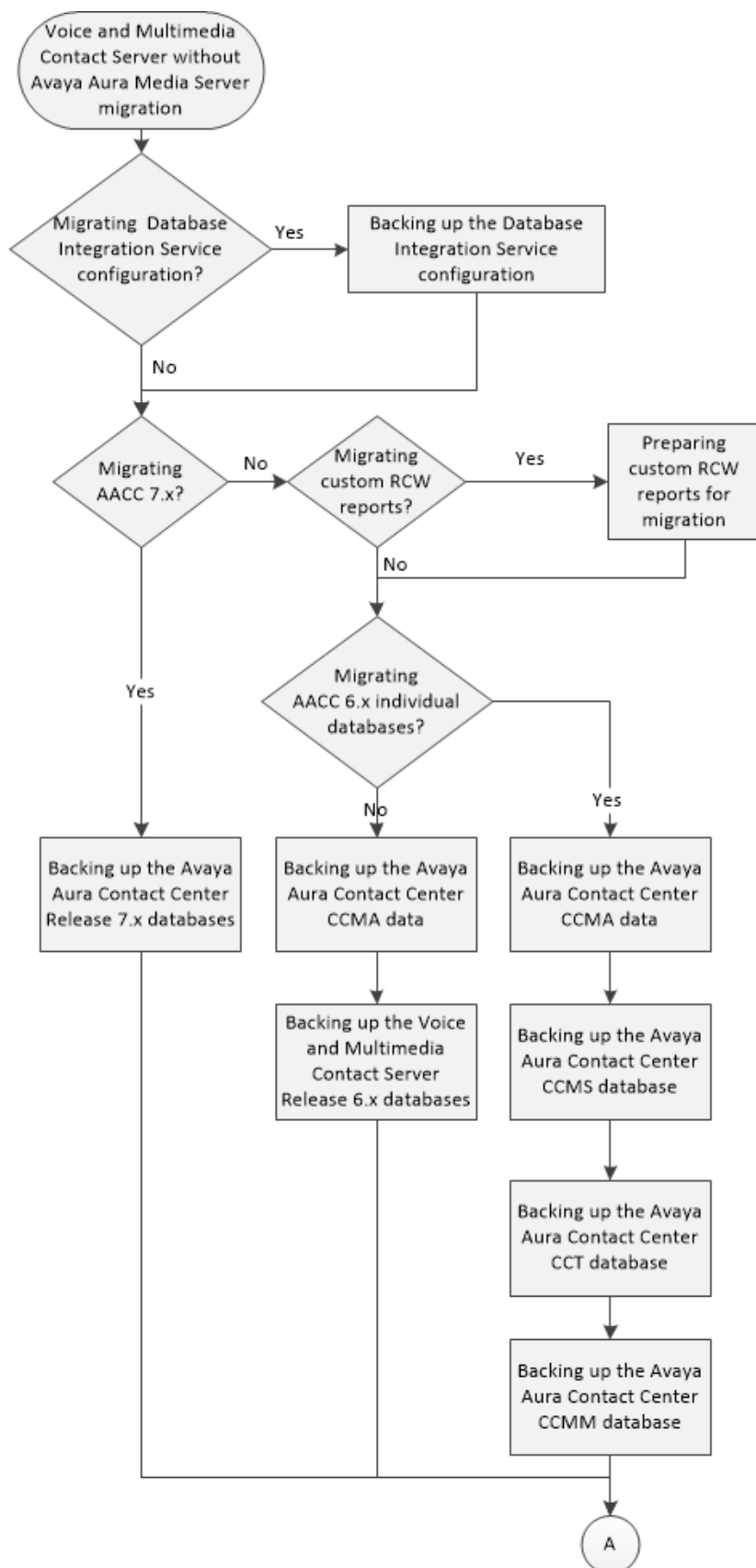


Figure 1: Voice and Multimedia Contact Server without Avaya Aura® Media Server migration

procedures

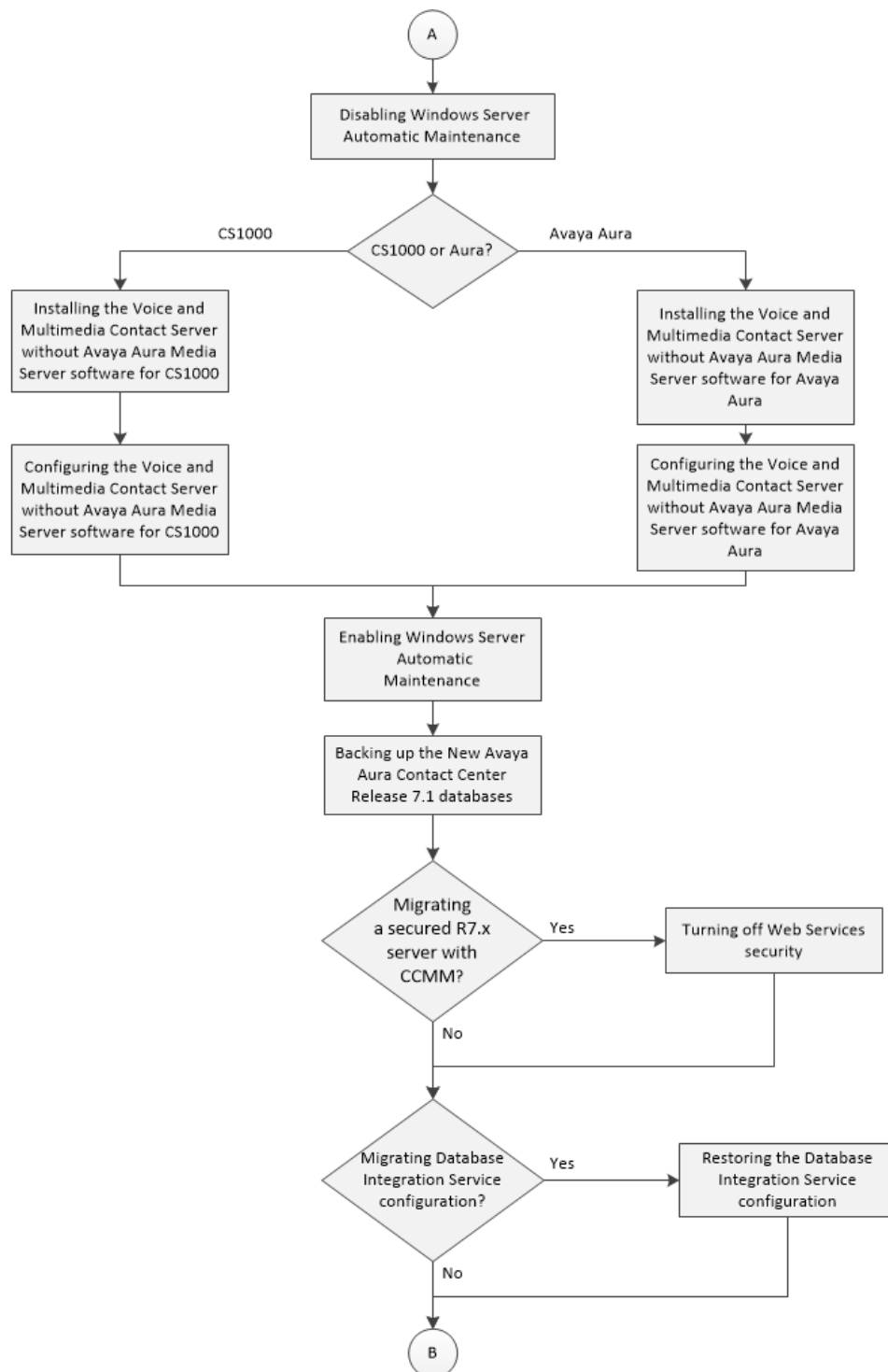


Figure 2: Voice and Multimedia Contact Server without Avaya Aura® Media Server migration procedures continued

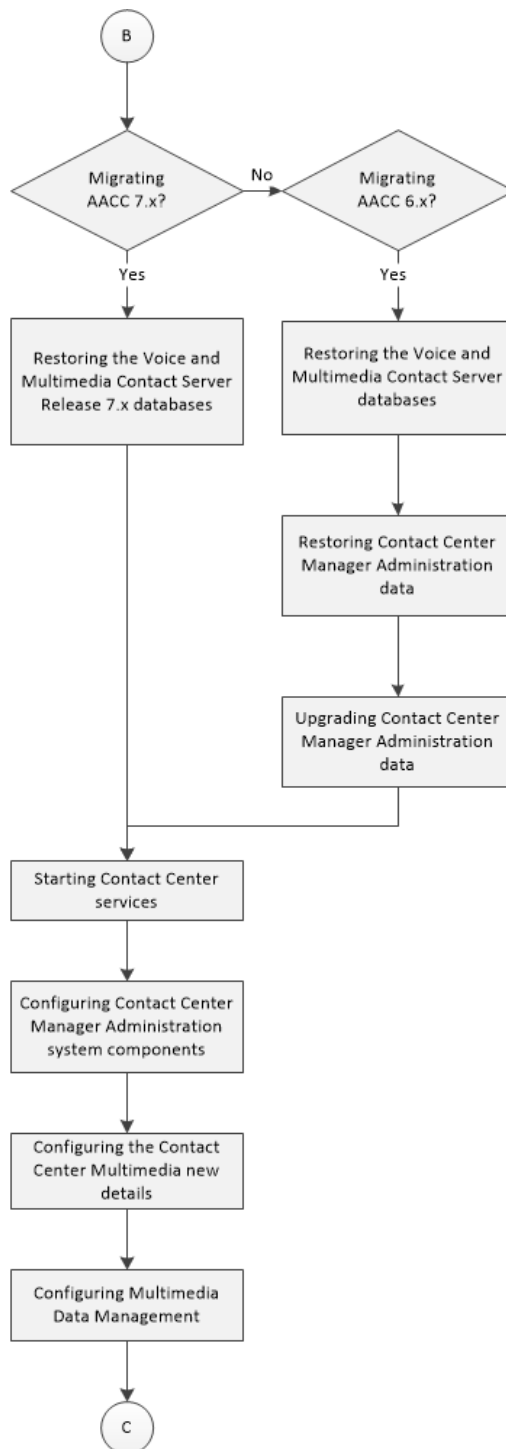


Figure 3: Voice and Multimedia Contact Server without Avaya Aura® Media Server migration procedures continued

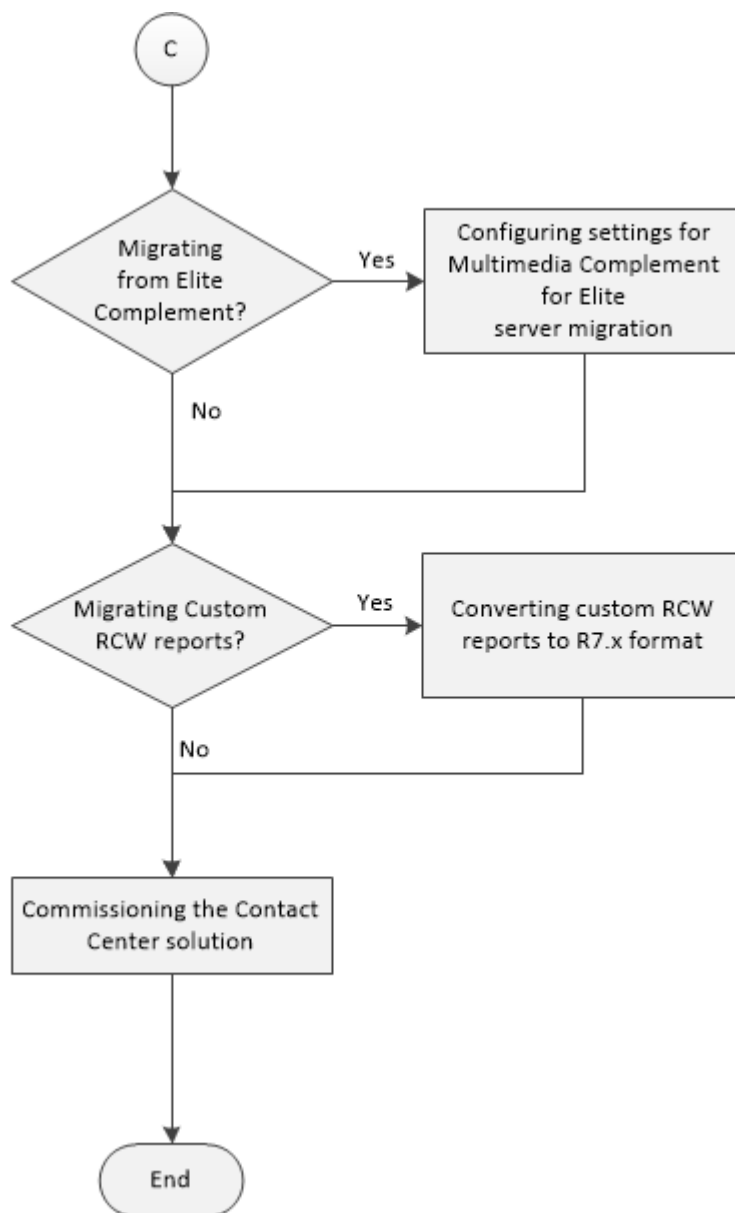


Figure 4: Voice and Multimedia Contact Server without Avaya Aura® Media Server migration procedures continued

Backing up the Database Integration Service configuration

Before you begin

- When you migrate the Database Integration Service to a new Contact Center server, you must manually re-configure any custom DSNs that you use in your solution.

About this task

Back up the Database Integration Service configuration to migrate the content to the new Contact Center server. Avaya recommends that you save the configuration file to a network location that you can access from the new server.

Procedure

1. On the server, click **Start > Run**.
2. In the Open box, type `regedit`.
3. Click **OK**.
4. If you are migrating from a Windows 2008 server (Release 6.x Avaya Aura® Contact Center):
 - a. In the Registry Editor, open the key
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Avaya\ICCM\HAI
 - b. From the **File** menu, select **Export**.
 - c. In the Export Registry File dialog box, type a name and location in which to store the configuration file.
 - d. Click **Save**.
5. Close the Registry Editor.

Backing up the Avaya Aura® Contact Center Release 7.1 databases

About this task

Back up the Avaya Aura® Contact Center Release 7.1 databases so you can restore them on the new server after you install the Avaya Aura® Contact Center Release 7.1 software.

Procedure

1. Log on to the existing Avaya Aura® Contact Center Release 7.1 server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
4. In the right pane, click **Create**.
5. From the **Drive Letter** list, select the network drive on which to store the Voice Contact Server database.
6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.

7. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the user password.
9. Click **Save**.
10. Click **OK**.
11. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
12. In the **Media Type** section, select **Network Location**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.
15. Click **Yes**, to continue with the backup.

Preparing custom RCW reports for migration

About this task

You can migrate custom historical reports built using Report Creation Wizard (RCW) in earlier releases to equivalent SSRS reports on Contact Center 7.1. Export the original reports from Crystal format (.rpt) to intermediate files and save them in a network location. After installing the new server you can restore and convert the saved files to SSRS format.

Contact Center 7.x Service Packs include a utility to export the reports. The utility can be found in the "Install Software\CCMA\RCW_Migration_Utility" folder in the Service Pack. This is one version of the utility: AACC 6.x.

Before you begin

Important:

Custom formulas do not migrate to the new server. If the original reports use custom formulas on the existing server, the formulas do not migrate with the custom reports.

Contact Center creates a placeholder formula for each custom formula. The placeholder displays an asterisk character on the migrated report. If possible, the placeholder formula includes the original Crystal Syntax formula text as a comment. You must edit the placeholder formulas, entering valid SSRS expressions for the formula text, to complete the migration. The placeholder formula is limited to 32,000 characters, so it is possible that very long formulas can be truncated.

Document all the custom formulas on the existing server, to assist with re-creating them on the new server after migrating the Contact Center databases.

Procedure

1. From the \Install Software\CCMA directory on the most recent AACC R7.x Service Pack, copy the utility for exporting Crystal reports.

You must copy the version of the utility that corresponds to the Contact Center version from which you are migrating.

2. On the Contact Center server from which you are migrating, extract the tool.
3. Run `MigrationRPTToRCWX.exe`.
4. On the Convert RTP to RCWX screen, click **Browse**, and choose a folder in which to store the output files for the converted reports.
5. Click **Run** to start the conversion.
6. When the export completes, copy the zip file to a network location from which you can copy it to the new Contact Center R7.1 server.

Next steps

Copy the zip files of exported reports to the new Contact Center server, and run the RCW import utility to convert each report to SSRS format.

Backing up the Avaya Aura® Contact Center CCMA data

Before you begin

- Map a network drive on which to back up your database. The network drive must be in NTFS format.
- Log on to the Contact Center Manager Administration server as an administrator.

About this task

Back up the Contact Center Manager Administration data on the source server Release 6.x to enable migration of the data to the new Contact Center server.

If your Contact Center Manager Administration uses High Availability replication, you must backup the data from the active CCMA.

Procedure

1. On the server with CCMA, choose **Start > All Programs > Avaya > Contact Center > Manager Administration > Configuration**.
2. In the left pane of the **Avaya Configuration** window, expand **Avaya > Applications > Backup & Restore**.
3. In the right pane, click **Backup & Restore**.
4. In the **Contact Center Manager Administration - Backup And Restore** dialog box, click **Backup** tab.
5. Select **Drive**.
6. Type the drive where the backed up database is stored.
7. Click **Next**.

8. In the **Perform Backup** section, select **Run Now**.
9. Click **Next**.
10. In the **Username** box, type a user name with administrative privileges for the server to which you store the backup.
11. In the **Password** box, type a password with administrative privileges for the server to which you store the backup.
12. From the **Domain** list, select the domain of the server to which you store the backup.
13. Click **Finish**.

Backing up the Voice and Multimedia Contact Server Release 6.x databases

About this task

Back up the Release 6.x Voice and Multimedia Contact Server databases so you can restore them on the new server after you install the Avaya Aura® Contact Center Release 7.1 software.

Procedure

1. On the existing Release 6.x Voice and Multimedia Contact Server, choose **Start > All Programs > Avaya > Contact Center > Database Utilities > Database Maintenance**.
2. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the right pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which to store the Voice and Multimedia Contact Server database.
5. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.
9. Click **OK**.
10. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. From the **Backup Location** list, select the network drive on which to store the backup.

13. Click **Backup**.
14. Click **Yes**, to continue with the backup.

Backing up the Avaya Aura® Contact Center CCMS database

About this task

Back up the Avaya Aura® Contact Center CCMS 6.x individual database so you can restore it on the new server after you install the Avaya Aura® Contact Center software.

Procedure

1. On the Contact Center Manager Server, choose **Start > All Programs > Avaya > Contact Center > Database Utilities > Database Maintenance**.
2. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the right pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which to store the Contact Center Manager Server database.
5. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.
9. Click **OK**.
10. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Applications** section, select **CCMS**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.
15. Click **Yes**, to continue with the backup.

Backing up the Avaya Aura® Contact Center CCT database

About this task

Back up the Avaya Aura® Contact Center CCT 6.x individual database so you can restore it on the new server after you install the Avaya Aura® Contact Center software.

Procedure

1. On the Communication Control Toolkit server, choose **Start > All Programs > Avaya > Contact Center > Database Maintenance**.
2. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the Backup Locations pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which you stored the Communication Control Toolkit database.
5. In the **UNC Path** box, type the location of the Communication Control Toolkit database in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.
9. Click **OK**.
10. In the Contact Center Database Maintenance window, in the Main Menu pane, select **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Applications** section, select **CCT**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.

Backing up the Avaya Aura® Contact Center CCMM database

Before you begin

Note:

If you back up a Contact Center Multimedia database without backing up the Contact Center Manager Server database, this can result in a mismatch in data when you restore. Avaya

recommends that you back up the Contact Center Manager Server database and the Contact Center Multimedia database at the same time.

About this task

Back up the Avaya Aura® Contact Center Contact Center Multimedia 6.x individual database so you can restore it on the new server after you install the new Contact Center software.

Procedure

1. In the Contact Center Multimedia server, choose **Start > All Programs > Avaya > Contact Center > Database Utilities > Database Maintenance**.
2. In the Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the Backup Locations pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which to store the Contact Center Multimedia database.
5. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.
9. Click **OK**.
10. In the Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Applications** section, select **CCMM**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.

Disabling Windows Server Automatic Maintenance

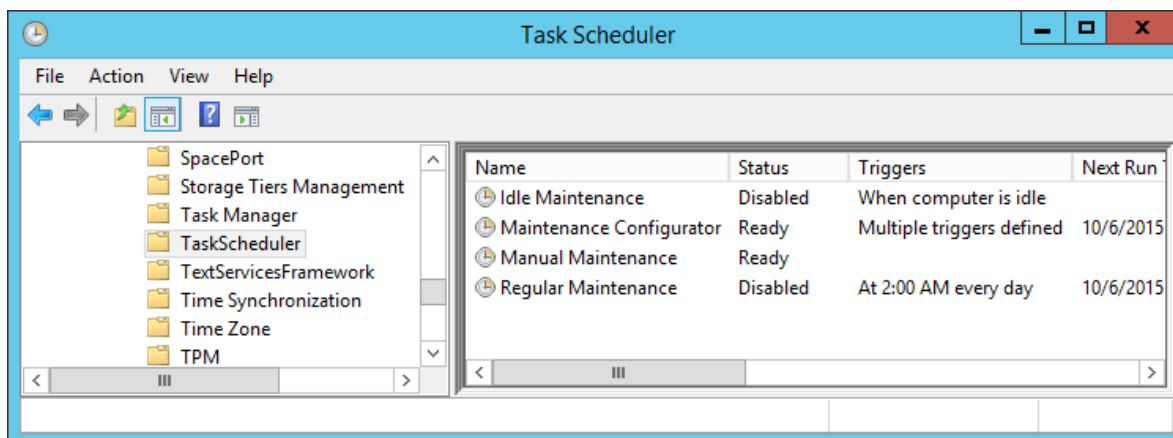
About this task

Disable Windows Server Automatic Maintenance while installing Contact Center software. Windows Server Automatic Maintenance can occasionally interfere with the real-time requirements for Contact Center. You must therefore temporarily disable Automatic Maintenance to install and configure Contact Center software. Re-enable it after deploying Contact Center.

Procedure

1. Log on to the Contact Center server as an administrator.

2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Disable**.
5. In the **Name** column, right-click **Regular Maintenance** and then click **Disable**.



6. From the **File** menu, click **Exit**.

Installing the Voice and Multimedia Contact Server without Avaya Aura® Media Server software for Avaya Aura® Unified Communications platform

Before you begin

- Ensure the Avaya Aura® Unified Communications platform is configured. For more information see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.
- Avoid installation from shared locations, because it might lead to installation failure. To ensure successful installation, either mount a DVD or download a local copy of a build.
- Download the most recent Contact Center patches to the server.
- If you deploy in a virtual environment and want to install Avaya Workspaces, you must manually deploy three virtual machines using the Avaya Workspaces Open Virtual Appliance (OVA). See [Deploying the Avaya Workspaces OVA](#) on page 177.

About this task

Install the Contact Center Voice and Multimedia Contact Server without Avaya Aura® Media Server software and enable your contact center to route contacts to the agents that can answer the call with the correct skills.

Procedure

1. Insert the Contact Center DVD into the DVD drive of your server.
2. If the installation does not automatically start, double-click **Setup.exe**.
3. Click **Install** to install the Microsoft .NET Framework on the server.
If you are prompted to accept the Microsoft .NET Framework license agreement, click **Yes**.
If you are prompted to restart the server, click **Yes** and repeat step 2.

4. The Contact Center software installer runs Operating System and hardware checks on the server. If the installer returns a Fail, the software installation cannot proceed until you correct the problem. Review any failures returned by the System Readiness Check and consult *Avaya Aura® Contact Center Overview and Specification* to determine the actions to resolve the issue.

You can ignore warnings if the potential impact to the operation of the contact center is understood and not applicable.

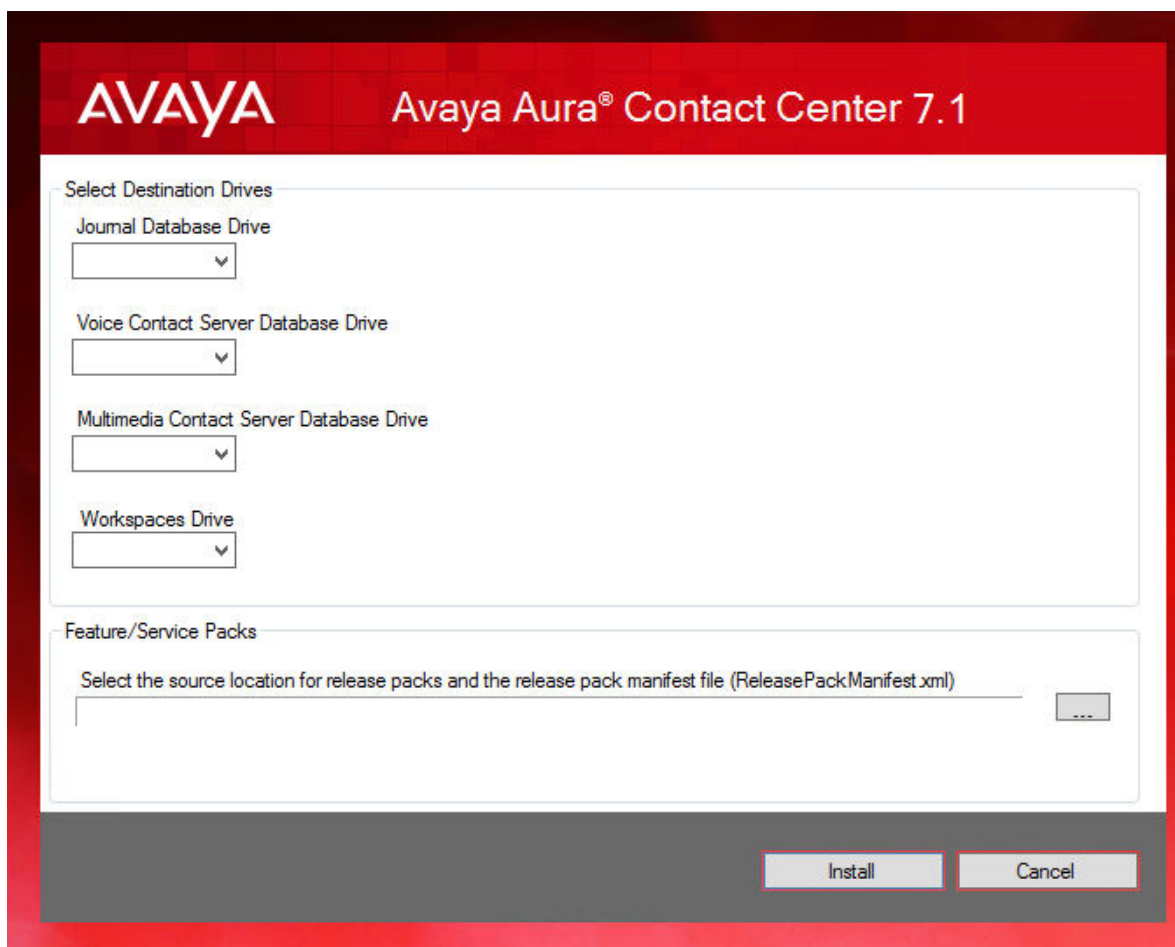
5. The Contact Center software installer platform and server selection screen appears.
6. In the **Select Voice Platform** section, select **Avaya Aura - SIP**.
7. In the **Select Server Installation Option** section, select **Voice and Multimedia Contact Server without Avaya Aura Media Server**.
8. **(Optional)** If you want to install and configure Avaya Workspaces, select the **Configure Workspaces for Avaya Aura Contact Center** check box.
9. Click **Next**.
10. Under **Journal Database Drive**, select the drive for the database journal. The default drive partition is H:.
11. Under **Voice Contact Server Database Drive**, select the drive for the Contact Center Manager Server, Communication Control Toolkit, and Contact Center Manager Administration databases. The default drive partition is F:.
12. Under **Multimedia Contact Server Database Drive**, select the drive for the Contact Center Multimedia database. The default drive partition is G:.
13. **(Optional)** If you deploy on a physical server, under **Workspaces Drive**, select the drive for the Avaya Workspaces database.

Ignore this step if you deploy on a virtual server.

Note:

On virtual installs, the Workspaces Drive option is not available on the Contact Center software installer.

14. In the **Service Packs** section, browse to and select the Service Pack.



15. Click **Install**.
16. The **AVAYA GLOBAL SOFTWARE LICENSE TERMS** window appears.
17. Read the terms of the license.
 - If you accept the terms, click **I ACCEPT THE LICENSE TERMS**. *The installation continues.*
 - If you do not accept the terms, click **I DECLINE THE LICENSE TERMS**. *The installation returns to the Select Destination Drive screen.* Click **Cancel** to stop the install.
 - To print the license terms, click **Print**.
18. The **MICROSOFT SOFTWARE LICENSE TERMS** window appears.
19. Read the terms of the license.
 - If you accept the terms, click **I ACCEPT THE LICENSE TERMS**. *The installation continues.*
 - If you do not accept the terms, click **I DECLINE THE LICENSE TERMS**. *The installation returns to the Select Destination Drive screen.* Click **Cancel** to stop the install.
 - To print the license terms, click **Print**.

20. The **Progress** window appears and displays the installation progress.
21. When the software is installed, you have the following options.
 - To continue configuring the server installation data:
 - a. Select **Launch Avaya Aura Contact Center Ignition Wizard**.
 - b. Click **Configure**. This starts the Avaya Aura® Contact Center Ignition Wizard.
 - To defer configuring the server installation data:
 - a. Clear **Launch Avaya Aura Contact Center Ignition Wizard**.
 - b. On the message box, click **Yes**.
 - c. On the main installer screen, click **Close**.
 - d. Follow the on-screen instructions and shut down the Contact Center server.

You must use the Ignition Wizard to initialize Avaya Aura® Contact Center, otherwise Avaya Aura® Contact Center is not operational. For more information about the Ignition Wizard, see the following procedure.

Configuring the Voice and Multimedia Contact Server without Avaya Aura® Media Server software for Avaya Aura® Unified Communications platform

Before you begin

- Ensure the Avaya Aura® Unified Communications platform is configured. For more information see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.
- You must configure the required language and locale of the Contact Center server operating system, if it is not a Latin-1 language, before configuring the Contact Center server using the Contact Center Ignition Wizard. For more information about configuring language and locale settings on the Contact Center server, see *Avaya Aura® Contact Center Server Administration*.
- Read the Contact Center Release Notes for the most recent instructions.

About this task

Configure the Contact Center Voice and Multimedia Contact Server software and enable your contact center to route contacts to the agents that can answer the call with the correct skills.

Procedure

1. Log on to the Contact Center server using the Administrator account details.
2. On the Contact Center Ignition Wizard screen, click **Next**. If the Contact Center Ignition Wizard is not visible, click the Ignition Wizard shortcut on the desktop.

3. On the **End-User License Agreement** screen, read the license agreement. Optionally, click **Print** to generate a local soft copy (in OpenXPS Document format) of the license agreement.
4. Select **I Accept the Terms of the End-User License Agreement** and click **Next**.
5. On the **Configuration Data** window, type the configuration details for each tab.
6. Select the **Core** tab, and configure the server details.

The screenshot shows the 'Avaya Contact Center' window with the 'Configuration Data' tab selected. The 'Core' tab is active, displaying fields for 'Site Name' (containing 'CC7SIP') and 'Real-Time Statistics Multicast IP Address' (containing '234.5.6.10'). To the right, the 'System Account Configuration' section is visible, showing 'Password' and 'Confirm Password' fields, both containing asterisks, with a green message 'Passwords match' below them. The Avaya logo is in the top right corner. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel', along with a 'Click Next to Continue' prompt.

7. In the **Site Name** box, type the site name for the Contact Center server. The site name must not contain spaces or non-alphabetical characters except hyphen (-) and underscore (_). The first character must be a letter. The site name must be unique and can consist of 6 to 15 characters.
8. In the **Real-Time Statistics Multicast IP Address** box, type the Real-time Statistics Multicast IP Address of the server to associate with sending real-time data. The **IP Address** must be from 224.0.1.0 to 239.255.255.255. The default is 234.5.6.10.
9. In the **System Account Configuration** section, in the **Password** box, type a password for the Contact Center administration account. The password is checked against the server security policy for minimum password requirements. Avaya recommends that you enter a password that conforms to your corporate password policy.
10. In the **Confirm Password** box, type the password.

11. Select the **Licensing** tab, and configure the licensing details.

The screenshot shows the 'Avaya Contact Center' configuration window. The title bar is blue with the text 'Avaya Contact Center'. The main header is 'Configuration Data' in bold black text, with the 'AVAYA' logo in red to the right. Below the header, it says 'Enter the required configuration data.' There are five tabs: 'Core', 'Licensing' (selected), 'SIP', 'Multimedia', and 'Security Configuration'. The 'Licensing' tab contains two main sections. The left section is for 'License Type' and 'License File'. 'License Type' has a dropdown menu set to 'Local WebLM'. 'License File' has a 'License File Location' text box with a 'Browse' button and a 'Skip' button. Below that is a 'System HostID (MAC Address)' text box containing '00:50:56:8D:48:8D'. The right section is for 'License Manager Package' and 'Features'. 'License Manager Package' has a dropdown menu set to 'Nodal Enterprise'. 'Features' is a list of checkboxes: 'Networking', 'Instant Messaging', 'Web Based Statistics', 'Multiplicity', 'Open Queue', 'Open Interfaces Open Queue', 'Open Interfaces Universal Networking', 'Agent Greeting', and 'Offsite Agent'. At the bottom of the window, there is a 'Click Next to Continue' text and three buttons: '< Back', 'Next >', and 'Cancel'.

12. From the **License Type** list, select **Local WebLM** to use the on-server WebLM license manager instance, or select **Remote WebLM** to use a separate Avaya WebLM server.
- If you select **Local WebLM**, you cannot apply your Local WebLM license file until after you configure your contact center using the Ignition Wizard. You must apply your license file during the commissioning process.
 - If you select **Remote WebLM**, in the **IP Address** box, type the IP address for the remote Avaya WebLM server. In the **Port** box, type the port number for the remote Avaya WebLM server. The default port number is 52233.
13. From the **Licensing Package** list, select the license type that you have purchased. Select **Nodal Enterprise** for single-site contact centers.
14. From the list of **Optional Packages**, enable the licensed features that you have purchased.
15. Select the **Open Queue** check box.
16. Select the **SIP** tab, and configure the SIP details.

Avaya Contact Center

Configuration Data

Enter the required configuration data.

Core
Licensing
SIP
Multimedia
Security Configuration

Switch Configuration

Avaya Aura ▼

SIP Voice Proxy Server

IP Address Port Transport

SIP CTI Proxy Server

IP Address Port Transport

Local SIP Subscriber

Domain Name

Backup SIP Voice Proxy Server

IP Address Port Transport

SIP IM Proxy Server

IM Provider

XMPP Domain

IP Address Port Transport

Click Next to Continue

< Back
Next >
Cancel

17. **(Optional)** If you want to configure the No Switch Configured Multimedia Only Server, in the **Switch Configuration** section, from the drop-down list, select **No Switch Configured**.
The other SIP details turn gray. Skip the following steps and continue with the step [33](#) on page 77.
18. In the **SIP Voice Proxy Server** section, in the **IP Address** box, type the IP address for the primary Avaya Aura® Session Manager.
19. In the **SIP Voice Proxy Server** section, in the **Port** box, type the server listening port number. The default port is 5060.
20. In the **SIP Voice Proxy Server** section, from the **Transport** list, select the SIP Network Transport communication protocol. The default is TCP.

*** Note:**

If there are Contact Center agents using SIP deskphones, or if your solution uses Avaya Aura® Presence Services 7.1 or later, you must ensure that the SIP Network Transport communication protocol is set to TLS.

21. In the **SIP CTI Proxy Server** section, in the **IP Address** box, type the IP address for the Avaya Aura® Application Enablement Services server.
22. In the **SIP CTI Proxy Server** section, in the **Port** box, type the SIP CTI Proxy Server port number. The default SIP CTI Proxy Server port is 4723.

23. In the **SIP CTI Proxy Server** section, from the **Transport** list, select the SIP Network Transport CTI communication protocol. The default Avaya Aura® Application Enablement Services communication protocol is TLS.
24. In the **Local SIP Subscriber** section, in the **Domain Name** box, type the SIP domain name for the SIP-enabled contact center. Typically the Avaya Aura® Contact Center SIP Domain Name matches your Active Directory domain name. The Avaya Aura® Contact Center SIP Domain Name matches the Session Manager contact center SIP domain name. The Local SIP Subscriber Domain Name must be different to the XMPP Domain name.
25. If your solution is going to support High Availability, in the **Backup SIP Voice Proxy Server** section, in the **IP Address** box, type the IP address for the second Avaya Aura® Session Manager. You must have a High Availability Standby Server license to support a Backup SIP Voice Proxy Server. If your solution is not going to support High Availability, leave the **Backup SIP Voice Proxy Server** section **IP Address** box empty.
26. In the **Backup SIP Voice Proxy Server** section, in the **Port** box, type the server listening port number. The default port is 5060.
27. In the **Backup SIP Voice Proxy Server** section, from the **Transport** list, select the SIP Network Transport communication protocol. The default is TCP.

 **Note:**

If there are Contact Center agents using SIP deskphones, or if your solution uses Avaya Aura® Presence Services 7.1 or later, you must ensure that the SIP Network Transport communication protocol is set to TLS.

28. In the **SIP IM Proxy Server** section, from the **IM Provider** list, select the Instant Messaging provider. Select Aura Presence Services or, if you are using Microsoft Skype for Business or Microsoft Lync, select Microsoft Lync. The **IM Provider** question is enabled if you select the **Instant Messaging** optional license package on the **Licensing** tab.
29. In the **SIP IM Proxy Server** section, if using an Avaya Aura® Presence Services server, in the **XMPP Domain** box, type the domain name of the Extensible Messaging and Presence Protocol (XMPP) server. The XMPP Domain name must be different to the Local SIP Subscriber Domain Name.
30. In the **SIP IM Proxy Server** section, in the **IP Address** box, type the IP address of the SIP IM Proxy Server.
31. In the **SIP IM Proxy Server** section, in the **Port** box, type the port number for the IM Proxy Server. The default port number for Avaya Aura® Presence Services is 5222. The default port number for Microsoft instant messaging servers is 5060.
32. In the **SIP IM Proxy Server** section, from the **Transport** list, select the SIP IM Proxy Server transport protocol.
33. Select the **Multimedia** tab, and configure the Contact Center Multimedia details.

The screenshot shows the 'Avaya Contact Center' configuration interface. The title bar is blue with the text 'Avaya Contact Center'. The main header area has 'Configuration Data' on the left and the 'AVAYA' logo on the right. Below the header, a message says 'Enter the required configuration data.' There are five tabs: 'Core', 'Licensing', 'SIP', 'Multimedia', and 'Security Configuration'. The 'Security Configuration' tab is selected. It contains two sections: 'Incoming Mail Server' and 'Outgoing Mail Server'. The 'Incoming Mail Server' section has a 'Host Name' text box and a 'Protocol' dropdown menu with 'POP3' selected. The 'Outgoing Mail Server' section has a 'Host Name' text box and a 'Protocol' dropdown menu with 'SMTP' selected. At the bottom, there is a 'Click Next to Continue' instruction and three buttons: '< Back', 'Next >', and 'Cancel'.

34. In the **Incoming Mail Server** box, type the name of the server on which email messages are received in your network.
35. From the **Protocol** list, select the communication protocol for the inbound email server. Select **POP3** or **IMAP**. The default protocol is POP3.
36. In the **Outgoing Mail Server** box, type the name of the server from on which email messages are sent. Your inbound and outbound mail servers can have the same name.
37. **(Optional)** To configure optional Avaya Workspaces, select the **Workspaces** tab. See [Configuring Avaya Workspaces during the initial installation](#) on page 362 for the configuration details.
38. Select the **Security Configuration** tab, and configure the security details in the **Security Store Details** section.

The screenshot shows the 'Avaya Contact Center' configuration interface. The 'Configuration Data' section is active, with the 'Security Configuration' tab selected. The 'Security Store Details' section contains fields for 'Full Computer Name (FQDN)' (CC7SIP.aaccdomain.com), 'Encryption Algorithm Level' (SHA256), 'Key Size' (2048), 'Security Store Password', and 'Confirm Store Password'. The 'Name of Organizational unit' and 'Name of Organization' fields are empty. The 'City or Locality' and 'State or Province' fields are also empty. The 'Two letter country code' field is empty. The 'Subject Alternative Name' section has a 'Type' dropdown set to 'DNS' and a 'Value' field. There are 'Add' and 'Remove' buttons. A 'Skip Security Configuration' checkbox is at the bottom left, and a 'Create Store' button is at the bottom right. Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom.

39. If you do not want to enable security, select the **Skip Security Configuration** checkbox and skip to step [55](#) on page 82.

! Important:

A warning message appears. If you proceed without enabling security, you cannot fully commission your solution. The SIP CTI link is disabled until you configure Contact Center TLS certificates to communicate securely with Application Enablement Services.

40. In the **Full Computer Name (FQDN)** box, type the full FQDN of the server on which you are creating the security store.

! Important:

The FQDN must be the full machine name of the server that the Security Store resides on. The FQDN name is case-sensitive.

41. In the **Name of Organizational unit** box, type the name of the department or division within the company.
42. In the **Name of Organization** box, type the company name.
43. In the **City or Locality** box, type the name of the city or district in which the contact center is located.

44. In the **State or Province** box, type the state or province in which the contact center is located.
45. In the **Two Letter Country Code** box, type the country code in which the contact center is located.
46. In the **Security Store password** box, type a password for accessing the new security store.
47. In the **Confirm Store password** box, confirm the password for accessing the new security store.

 **Important:**

Ensure you remember this password, because you need it when you log on to Security Manager after install. If you forget the password, you cannot access Security Manager.

48. If you are implementing High Availability in the contact center, generate the security store using Subject Alternative Names (SANs). In the **Subject Alternative Name** section, for each SAN you want to add:
 - a. From the **Type** drop-down list, select DNS.
 - b. In the **Value** field, type the FQDN for the server.
 - c. Click **Add**.

For a High Availability system, add the current server FQDN and the Managed name for the HA pair.

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

The default value for **Encryption Algorithm** is SHA256 and the default value for **Key Size** is 2048.

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

50. Click **Create Store**.
51. You can now use the **Security Configuration** tab to create and save a Certificate Signing Request (CSR) file.

The screenshot shows the 'Avaya Contact Center' configuration interface. The 'Configuration Data' section is active, with the 'Security Configuration' tab selected. The page title is 'Configuration Data' with the Avaya logo. Below the title, it says 'Enter the required configuration data.' The tabs are 'Core', 'Licensing', 'SIP', 'Multimedia', and 'Security Configuration'. The main content area is titled 'Store created – Generate Identity Security Certificate by signing the Certificate Signing Request provided.' It contains a 'Certificate Signing Request file' section with a 'Create CSR File' button. Below this is an 'Add' button and a list of 'Imported Trusted Certificate Authority Root Certificate(s)' with a 'Remove' button. There is also a section for 'Imported Identity Security Certificate' with a 'Remove' button. On the right, a 'Status' box contains instructions: 'Ensure that a removable or network drive is available.', 'Create the Certificate Signing Request file and save it to a removable or network drive.', and 'Alternatively, to defer Security Configuration and continue with the Installation Wizard.' There is a 'Reset' button in the status box. At the bottom, there are navigation buttons: '< Back', 'Next >', and 'Cancel'. A 'Click Next to Continue' message is also present.

52. Click **Create CSR File**.

53. From the **Save In** drop-down list, select a shared location in which to save the CSR file and click **Save**.

You must now send the Certificate Signing Request file to a Certificate Authority and receive a signed certificate and root certificate to import to the security store.

54. Click **Add** to import certificates. In the **Open** dialog box, navigate to the location of a certificate and click **Open**. To remove the imported certificate, select the required certificate from the list and click **Remove**.

You can import either a chained certificate, or separate root and signed certificates. Root certificates appear in the **Imported Trusted Certificate Authority Root Certificate(s)** section. A signed certificate appears in the **Imported Identity Security Certificate** section.

If a chained certificate contains both root and signed certificates, you can add root certificates and signed certificate simultaneously by importing just one chained certificate.

If a chained certificate contains root certificates only, you can use the chained certificate to add all root certificates at a time. To add a signed certificate, click **Add** and navigate to the required signed certificate.

If you have separate root and signed certificates, you must add them one by one by clicking the **Add** button. Always add a signed certificate last.

 **Important:**

When adding a chained certificate, the system can prompt you to enter the password you have created for accessing the security store. See step [46](#) on page 80.

55. Click **Next**.
56. Review and verify the summary information and click **Configure**.
57. After the installation is complete, click **Finish**.
58. If prompted, restart the server.

Installing the Voice and Multimedia Contact Server software for CS1000

Before you begin

- Ensure the Avaya Communication Server 1000 is configured. For more information see *Avaya Aura® Contact Center and Avaya Communication Server 1000 Integration*.
- Download the most recent Contact Center and Common Components patches to the server.
- Read the Contact Center Release Notes for the most recent instructions.

About this task

Install the Contact Center Voice and Multimedia Contact Server software on the server.

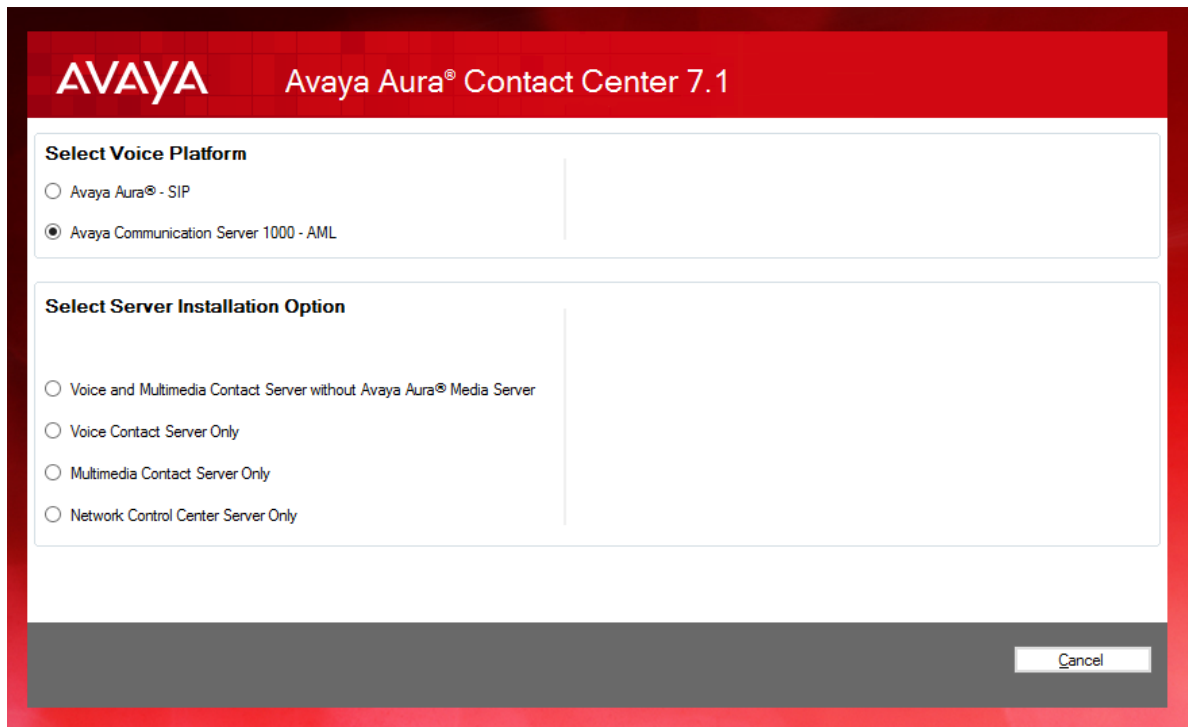
Procedure

1. Insert the Contact Center DVD into the DVD drive of your server.
2. If the installation does not automatically start, double-click **Setup.exe**.
3. Click **Accept** to install the Microsoft .NET Framework on the server.

If you are prompted to accept the Microsoft .NET Framework license agreement, click **Accept**. If you are prompted to restart the server, click **Yes** and repeat step 2.
4. Contact Center software installer runs Operating System and hardware checks on the server. If the installer returns a Fail, the software installation cannot proceed until you correct the problem. Review any failures returned by the System Readiness Check and consult *Avaya Aura® Contact Center Overview and Specification* to determine the actions to resolve the issue.

You can ignore warnings if the potential impact to the operation of the contact center is understood and not applicable.
5. The Contact Center software installer platform and server selection screen appears.

6. In the **Select Voice Platform** section, select **Avaya Communication Server 1000 - AML**.



7. In the **Select Server Installation Option** section, select **Voice and Multimedia Contact Server without Avaya Aura Media Server**.
8. Click **Next**.
9. Under **Journal Database Drive**, select the drive for the database journal. The default drive partition is H:.
10. Under **Voice Contact Server Database Drive**, select the drive for the Contact Center Manager Server, Communication Control Toolkit, and Contact Center Manager Administration databases. The default drive partition is F:.
11. Under **Multimedia Contact Server Database Drive**, select the drive for the Contact Center Multimedia database. The default drive partition is G:.
12. In the **Service Packs** section, browse to and select the Service Pack.
13. Click **Install**.
14. The **AVAYA GLOBAL SOFTWARE LICENSE TERMS** window appears.
15. Read the terms of the license.
 - If you accept the terms, click **I ACCEPT THE LICENSE TERMS**. *The installation continues.*
 - If you do not accept the terms, click **I DECLINE THE LICENSE TERMS**. *The installation returns to the Select Destination Drive screen.* Click **Cancel** to stop the install.
 - To print the license terms, click **Print**.

16. The **MICROSOFT SOFTWARE LICENSE TERMS** window appears.
17. Read the terms of the license.
 - If you accept the terms, click **I ACCEPT THE LICENSE TERMS**. *The installation continues.*
 - If you do not accept the terms, click **I DECLINE THE LICENSE TERMS**. *The installation returns to the Select Destination Drive screen.* Click **Cancel** to stop the install.
 - To print the license terms, click **Print**.
18. The **Progress** window appears and displays the installation progress.
19. When the software is installed, you have the following options.
 - To continue configuring the server installation data:
 - a. Select **Launch Avaya Aura Contact Center Ignition Wizard**.
 - b. Click **Configure**. This starts the Avaya Aura® Contact Center Ignition Wizard.
 - To defer configuring the server installation data:
 - a. Clear **Launch Avaya Aura Contact Center Ignition Wizard**.
 - b. On the message box, click **Yes**.
 - c. On the main installer screen, click **Close**.
 - d. Follow the on-screen instructions and shut down the Contact Center server.

You must use the Ignition Wizard to initialize Avaya Aura® Contact Center, otherwise Avaya Aura® Contact Center is not operational. For more information about the Ignition Wizard, see the following procedures.

Configuring Voice and Multimedia Contact Server software for CS1000

Before you begin

- Ensure the Avaya Communication Server 1000 is configured. For more information see *Avaya Aura® Contact Center and Avaya Communication Server 1000 Integration*.
- You must configure the required language and locale of the Contact Center server operating system, if it is not a Latin-1 language, before configuring the Contact Center server using the Contact Center Ignition Wizard. For more information about configuring language and locale settings on the Contact Center server, see *Avaya Aura® Contact Center Server Administration*.
- Download the most recent Contact Center and Common Components patches to the server.
- Read the Contact Center Release Notes for the most recent instructions.

About this task

Configure the Contact Center Voice and Multimedia Contact Server software and enable your contact center to route contacts to the agents that can answer the call with the correct skills.

Procedure

1. Log on to the Contact Center server using the Administrator account details.
2. On the Contact Center Ignition Wizard screen, click **Next**. If the Contact Center Ignition Wizard is not visible, click the Ignition Wizard shortcut on the desktop.
3. On the **End-User License Agreement** screen, read the license agreement. Optionally, click **Print** to generate a local soft copy (in OpenXPS Document format) of the license agreement.
4. Select **I Accept the Terms of the End-User License Agreement** and click **Next**.
5. On the **Configuration Data** window, type the configuration details for each tab.
6. Select the **Core** tab, and configure the server details.

The screenshot shows the 'Configuration Data' window for the Avaya Contact Center. The 'Core' tab is selected, and the 'System Account Configuration' section is visible. The 'Site Name' field contains 'CC7SIP', the 'Real-Time Statistics Multicast IP Address' field contains '234.5.6.10', and the 'CLAN IP Address' and 'ELAN IP Address' fields are empty. The 'System Account Configuration' section has 'Password' and 'Confirm Password' fields, both empty. The 'AVAYA' logo is in the top right corner. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'.

Avaya Contact Center

Configuration Data

Enter the required configuration data.

Core | Licensing | Multimedia | CS1000 | Security Configuration

Site Name
Site Name
CC7SIP

Real-Time Statistics Multicast IP Address
IP Address
234.5.6.10

Network Configuration
CLAN IP Address
ELAN IP Address

System Account Configuration
Enter a password for the Contact Center administration Windows account.
Password
Confirm Password

Click Next to Continue

< Back | Next > | Cancel

7. In the **Site Name** box, type the site name for the Contact Center server. The site name must not contain spaces or non-alphabetical characters except hyphen (-) and underscore (_). The first character must be a letter. The site name must be unique and can consist of 6 to 15 characters.

8. In the **Real-Time Statistics Multicast IP Address** box, type the Real-time Statistics Multicast IP Address of the server to associate with sending real-time data. The **IP Address** must be from 224.0.1.0 to 239.255.255.255. The default is 234.5.6.10.
9. In the **Network Configuration** section, in the **ELAN IP Address** box, type the IP Address of the embedded local area network. The embedded local area network (ELAN) is a dedicated Ethernet LAN that connects Contact Center to the PABX.
10. In the **CLAN IP Address** box, type the IP Address of the Contact Center server. This is the Contact Center server IP address on the subnet that connects to the other servers and agent client computers in the contact center solution.
11. In the **System Account Configuration** section, in the **Password** box, type a password for the Contact Center administration account. The password is checked against the server security policy for minimum password requirements. Avaya recommends that you enter a password that conforms to your corporate password policy.
12. In the **Confirm Password** box, type the password.
13. Select the **Licensing** tab, and configure the licensing details.
14. From the **License Type** list, select **Standard KRS**.
15. Click **Browse** to locate and load your license file.
16. From the **Licensing Package** list, select the license type that you have purchased. Select **Nodal Enterprise** for single-site contact centers.
17. From the list of **Optional Packages**, enable the licensed features that you have purchased.
18. Select the **Open Queue** check box.
19. Select the **Multimedia** tab, and configure the Contact Center Multimedia details.

Avaya Contact Center

Configuration Data

AVAYA

Enter the required configuration data.

Core Licensing Multimedia CS1000 Security Configuration

Incoming Mail Server

Host Name

Protocol

POP3

v

Outgoing Mail Server

Host Name

Protocol

SMTP

Click Next to Continue

< Back
Next >
Cancel

20. In the **Incoming Mail Server** box, type the name of the server on which email messages are received in your network.
21. From the **Protocol** list, select the communication protocol for the inbound email server. Select **POP3** or **IMAP**. The default protocol is POP3.
22. In the **Outgoing Mail Server** box, type the name of the server from on which email messages are sent. Your inbound and outbound mail servers can have the same name.
23. Select the **CS1000** tab.

Avaya Contact Center

Configuration Data

Enter the required configuration data.

Core Licensing Multimedia **CS1000** Security Configuration

CS1000 Switch Data

Switch Name

Switch IP Address

Switch Customer Number

Switch Serial Number

Alternative Switch IP Address

Alternative Switch Customer Number

Alternative Switch Serial Number

Voice Services Setup

Voice Connection Type

☒ None

☐ Avaya Aura Experience Portal

☐ CallPilot

CallPilot Configuration

ELAN IP Address Port

CPHA Managed CLAN IP Address

CLAN IP Address

Click Next to Continue

< Back Next > Cancel

24. In the **Switch Name** box, type the name of the AML Avaya Communication Server 1000 telephone switch. Valid characters for Avaya Communication Server 1000 names are A–Z, a–z, 0–9, underscore (_), and period (.). Names must begin with an alphabetical character and cannot contain spaces. The last character must not be an underscore or a period. Names must not exceed 80 characters in length.
25. In the **Switch IP Address** box, type the IP address of the Avaya Communication Server 1000.
26. In the **Switch Customer Number** box, type the customer number for the Avaya Communication Server 1000.
27. In the **Alternative Switch IP Address** box, type the IP address of an alternate Avaya Communication Server 1000, if you have one.
28. In the **Alternative Switch Customer Number** box, type the customer number of the alternate Avaya Communication Server 1000, if you have one.
29. In the **Alternative Switch Serial ID** box, type the serial number of the alternate Avaya Communication Server 1000, if you have one.
30. In the **Voice Connection Type** section, select the method used to connect to the PABX. Select **None**, **Avaya Aura Experience Portal**, or **CallPilot**.

31. If you are using an Avaya CallPilot® server, enter the Avaya CallPilot® server **ELAN IP Address** and then configure the **Port** to 10008.
32. If you are using Avaya CallPilot® High Availability, in the **CPHA Managed CLAN IP Address** box, type the Avaya CallPilot® Managed CLAN IP address.
33. If you are using an Avaya CallPilot® server, in the **CLAN IP Address** box, type the CLAN IP address of the Avaya CallPilot® server.
34. Select the **Security Configuration** tab, and configure the security details in the **Security Store Details** section.

The screenshot shows the 'Avaya Contact Center' configuration window. The 'Configuration Data' section is active, with the 'Security Configuration' tab selected. The 'Security Store Details' section contains the following fields:

- Full Computer Name (FQDN): CC7SIP.aaccdomain.com
- Encryption Algorithm Level: SHA256
- Key Size: 2048
- Security Store Password: (empty)
- Confirm Store Password: (empty)
- Name of Organizational unit: (empty)
- Name of Organization: (empty)
- City or Locality: (empty)
- State or Province: (empty)
- Two letter country code: (empty)

The 'Subject Alternative Name' section on the right has a 'Type' dropdown set to 'DNS' and a 'Value' field. Below these are 'Add' and 'Remove' buttons. At the bottom right is a 'Create Store' button. A checkbox labeled 'Skip Security Configuration' is at the bottom left. Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom.

35. If you do not want to enable security, select the **Skip Security Configuration** checkbox and skip to [the next steps](#) on page 92.

Important:

A warning message appears.

36. In the **Full Computer Name (FQDN)** box, type the full FQDN of the server on which you are creating the security store.

Important:

The FQDN must be the full machine name of the server that the Security Store resides on. The FQDN name is case-sensitive.

37. In the **Name of Organizational unit** box, type the name of the department or division within the company.
38. In the **Name of Organization** box, type the company name.
39. In the **City or Locality** box, type the name of the city or district in which the contact center is located.
40. In the **State or Province** box, type the state or province in which the contact center is located.
41. In the **Two Letter Country Code** box, type the country code in which the contact center is located.
42. In the **Security Store password** box, type a password for accessing the new security store.
43. In the **Confirm Store password** box, confirm the password for accessing the new security store.

 **Important:**

Ensure you remember this password, because you need it when you log on to Security Manager after install. If you forget the password, you cannot access Security Manager.

44. If you are implementing High Availability in the contact center, generate the security store using Subject Alternative Names (SANs). In the **Subject Alternative Name** section, for each SAN you want to add:
 - a. From the **Type** drop-down list, select DNS.
 - b. In the **Value** field, type the FQDN for the server.
 - c. Click **Add**.

For a High Availability system, add the current server FQDN and the Managed name for the HA pair.

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

The default value for **Encryption Algorithm** is SHA256 and the default value for **Key Size** is 2048.

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

46. Click **Create Store**.
47. You can now use the **Security Configuration** tab to create and save a Certificate Signing Request (CSR) file.

The screenshot shows the 'Configuration Data' window for 'Avaya Contact Center'. The 'Security Configuration' tab is selected. The window title is 'Configuration Data' with the AVAYA logo. Below the title, it says 'Enter the required configuration data.' The tabs are 'Core', 'Licensing', 'Multimedia', 'CS1000', and 'Security Configuration'. The main content area has a heading 'Store created – Generate Identity Security Certificate by signing the Certificate Signing Request provided.' Below this is a 'Certificate Signing Request file' section with a 'Create CSR File' button. There is an 'Add' button and a list of 'Imported Trusted Certificate Authority Root Certificate(s)' with a 'Remove' button. Below that is an 'Imported Identity Security Certificate' section with a 'Remove' button. On the right, a 'Status' box contains instructions: 'Ensure that a removable or network drive is available.', 'Create the Certificate Signing Request file and save it to a removable or network drive.', and 'Alternatively, to defer Security Configuration and continue with the Installation Wizard.' with a 'Reset' button. At the bottom, it says 'Click Next to Continue' and has '< Back', 'Next >', and 'Cancel' buttons.

48. Click **Create CSR File**.

49. From the **Save In** drop-down list, select a shared location in which to save the CSR file and click **Save**.

You must now send the Certificate Signing Request file to a Certificate Authority and receive a signed certificate and root certificate to import to the security store.

50. Click **Add** to import certificates. In the **Open** dialog box, navigate to the location of a certificate and click **Open**. To remove the imported certificate, select the required certificate from the list and click **Remove**.

You can import either a chained certificate, or separate root and signed certificates. Root certificates appear in the **Imported Trusted Certificate Authority Root Certificate(s)** section. A signed certificate appears in the **Imported Identity Security Certificate** section.

If a chained certificate contains both root and signed certificates, you can add root certificates and signed certificate simultaneously by importing just one chained certificate.

If a chained certificate contains root certificates only, you can use the chained certificate to add all root certificates at a time. To add a signed certificate, click **Add** and navigate to the required signed certificate.

If you have separate root and signed certificates, you must add them one by one by clicking the **Add** button. Always add a signed certificate last.

! Important:

When adding a chained certificate, the system can ask you to enter the password you created for accessing the security store. See [the previous steps](#) on page 90.

51. Click **Next**.
52. Review and verify the summary information, and click **Configure**.
53. After the installation is complete, click **Finish**.
54. If prompted, restart the server.

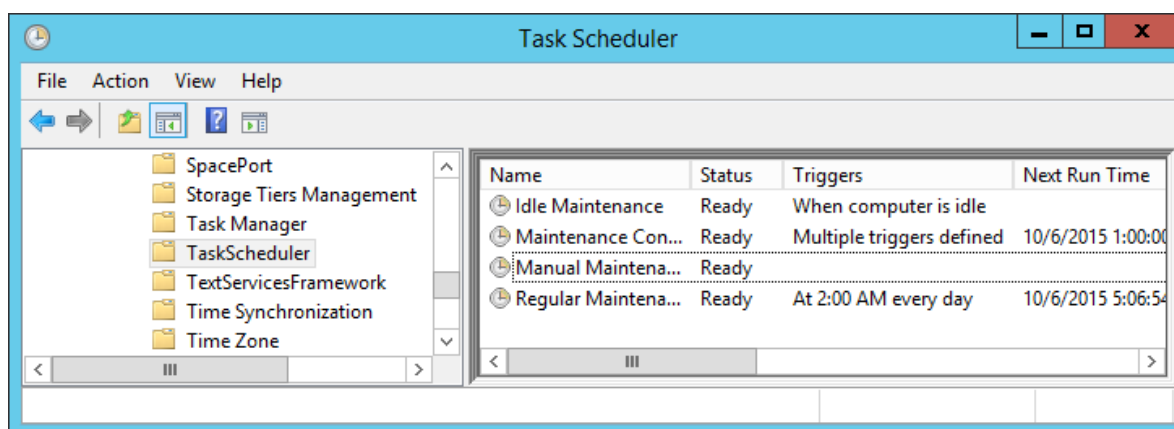
Enabling Windows Server Automatic Maintenance

About this task

Enable Windows Server Automatic Maintenance after deploying Contact Center software.

Procedure

1. Log on to the Contact Center server as an administrator.
2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Enable**.
5. In the **Name** column, right-click **Regular Maintenance** and then click **Enable**.



6. From the **File** menu, click **Exit**.

Backing up the new Avaya Aura® Contact Center Release 7.1 databases

About this task

After running the Ignition Wizard, backup the Avaya Aura® Contact Center Release 7.1 databases.

The backup databases capture the system in a known clean state and these might be required later if issues arise during data migration.

Procedure

1. Log on to the new Avaya Aura® Contact Center Release 7.1 server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
4. In the right pane, click **Create**.
5. From the **Drive Letter** list, select the network drive on which to store the databases.
6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.
7. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the user password.
9. Click **Save**.
10. Click **OK**.
11. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
12. In the **Media Type** section, select **Network Location**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.
15. Click **Yes**, to continue with the backup.

Turning off Web Services security

About this task

Turn off Web Services security before you restore a CCMM database from a system that did not have security enabled. If you are migrating from an Avaya Aura® Contact Center Release 7.x system that has Web Services security turned on, you can skip this procedure.

Before you begin

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

Procedure

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

Important:

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

2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. On the Store Access dialog, type the password for the security store, and click **OK**.
4. On the Security Manager screen, select the **Security Configuration** tab.
5. Click **Security Off**.
6. Click **Apply**.
7. On the Security Change Confirmation dialog, click **Confirm**.
8. Click **Log Out**.
9. Restart the Contact Center server.

Next steps

Complete the migration procedures in this book. After the migration, to complete your security configuration, follow the procedures in *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* or *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000*.

Restoring the Database Integration Service configuration

About this task

If you backed up the Database Integration Service configuration on your old server, restore the configuration to the registry on the new server. Contact Center automatically copies the configuration from the registry into the database on the next restart.

Procedure

1. On the Contact Center server, on the **Desktop** screen, right-click **Start** and select **Run**.
2. Type `regedit`.
3. Click **OK**.
4. On the **Registry Editor** dialog box, click **File** > **Import**.
5. On the **Import Registry File** dialog box, select the HAI configuration file that you saved from the old server.

6. Click **Open**.
7. On the **Registry Editor** message box, click **OK**.

Next steps

If you used custom DSNs in the Database Integration Service configuration on your old server, you must manually re-configure these DSNs on the new server.

Restoring the Voice and Multimedia Contact Server Release 7.1 databases

Before you begin

- Back up the old Voice and Multimedia Contact Server databases.
- On the new server, map a drive to the Voice and Multimedia Contact Server database backups.

Important:

When you migrate configuration information from the old server to the new server, do not run the two application servers simultaneously. Both applications are configured the same, so they attempt to access and control the same resources. Continuing to run the old applications in the Contact Center can result in unpredictable behavior.

About this task

Restore the Voice and Multimedia Contact Server Release 7.1 databases to the new server. The Database Maintenance utility can restore all application databases at one time. Restore the data for the CCMS, CCT, CCMA, and CCMM databases. You must restore the CCMS, CCT, CCMA, and CCMM databases as a matched set, and all databases must be stored in the same backup location.

Procedure

1. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
2. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the Backup Locations pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which you stored the Voice and Multimedia Contact Server database backup.
5. In the **UNC Path** box, type the location of the Voice and Multimedia Contact Server databases in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.

8. Click **Save**.
9. Click **OK**.
10. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Restore**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Application** section, select **CCT**, **CCMS**, **CCMA**, and **CCMM**.
13. In the **Restore contents** section, select **Data** and **Offline**.
14. From the **Backup Location** list, select the network drive containing the backed up Voice and Multimedia Contact Server databases.
15. Click **Restore**.
16. Click **Yes**.
17. Use the **Progress information** field to monitor the progress of the restoration.
18. On the **Database Maintenance** message box, click **OK**.
19. From the **Start** menu, in the Avaya area, click **Server Configuration**.
20. In the **Server Configuration** dialog box, click **Apply All**.
21. Click **Yes** to restart Contact Center.

Restoring the Voice and Multimedia Contact Server databases

Before you begin

- Back up the old Voice and Multimedia Contact Server databases.
- On the new server, map a drive to the Voice and Multimedia Contact Server database backups.

Important:

When you migrate configuration information from the old server to the new server, do not run the two application servers simultaneously. Both applications are configured the same, so they attempt to access and control the same resources. Continuing to run the old applications in the Contact Center can result in unpredictable behavior.

About this task

Restore the Voice and Multimedia Contact Server databases to the new server. The Database Maintenance utility can restore all application databases at one time. Restore the data for the CCMS, CCT, and CCMM databases. You must restore the CCMS, CCT, and CCMM databases as a matched set, and all databases must be stored in the same backup location.

Procedure

1. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
2. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the Backup Locations pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which you stored the Voice and Multimedia Contact Server database backup.
5. In the **UNC Path** box, type the location of the Voice and Multimedia Contact Server databases in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.
9. Click **OK**.
10. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Restore**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Application** section, select **CCT**, **CCMS**, and **CCMM**.
13. In the **Restore contents** section, select **Data**. If you are restoring an AACC Release 6.4 database, select **Offline** also.
14. From the **Backup Location** list, select the network drive containing the backed up Voice and Multimedia Contact Server databases.
15. Click **Restore**.
16. Click **Yes**.
17. Use the **Progress information** field to monitor the progress of the restoration.
18. On the **Database Maintenance** message box, click **OK**.
19. From the **Start** menu, in the Avaya area, click **Server Configuration**.
20. In the **Server Configuration** dialog box, click **Apply All**.
21. Click **Yes** to restart Contact Center.

Restoring Contact Center Manager Administration data

Before you begin

- Know the network location (in Universal Naming Convention (UNC) format) of the drive for the backed up data.

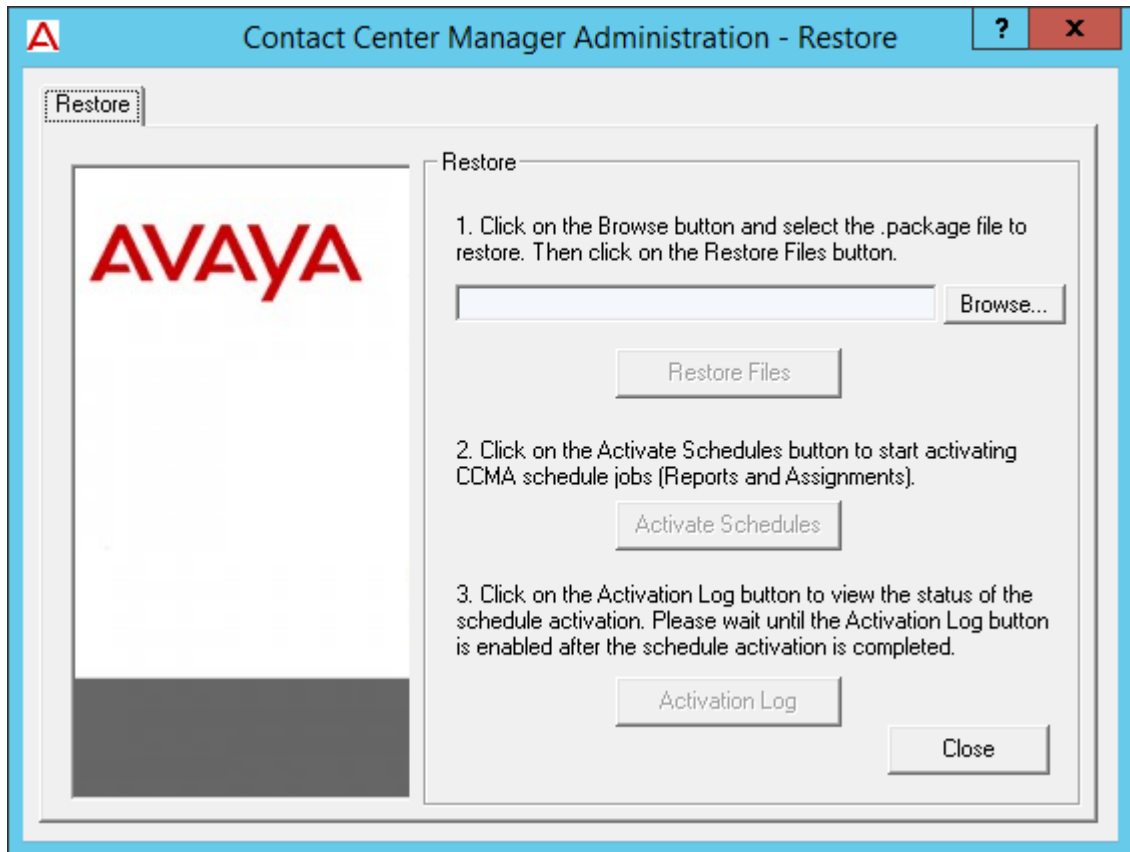
About this task

Restore the Contact Center Manager Administration data to migrate the data to the new server. Use this procedure if you are restoring Avaya Aura® Contact Center Contact Center Manager Administration data. You must restore the CCMA database as part of a matched set; the CCMA data must be restored to the same server as its corresponding databases (for example, CCMS, CCT, or CCMM).

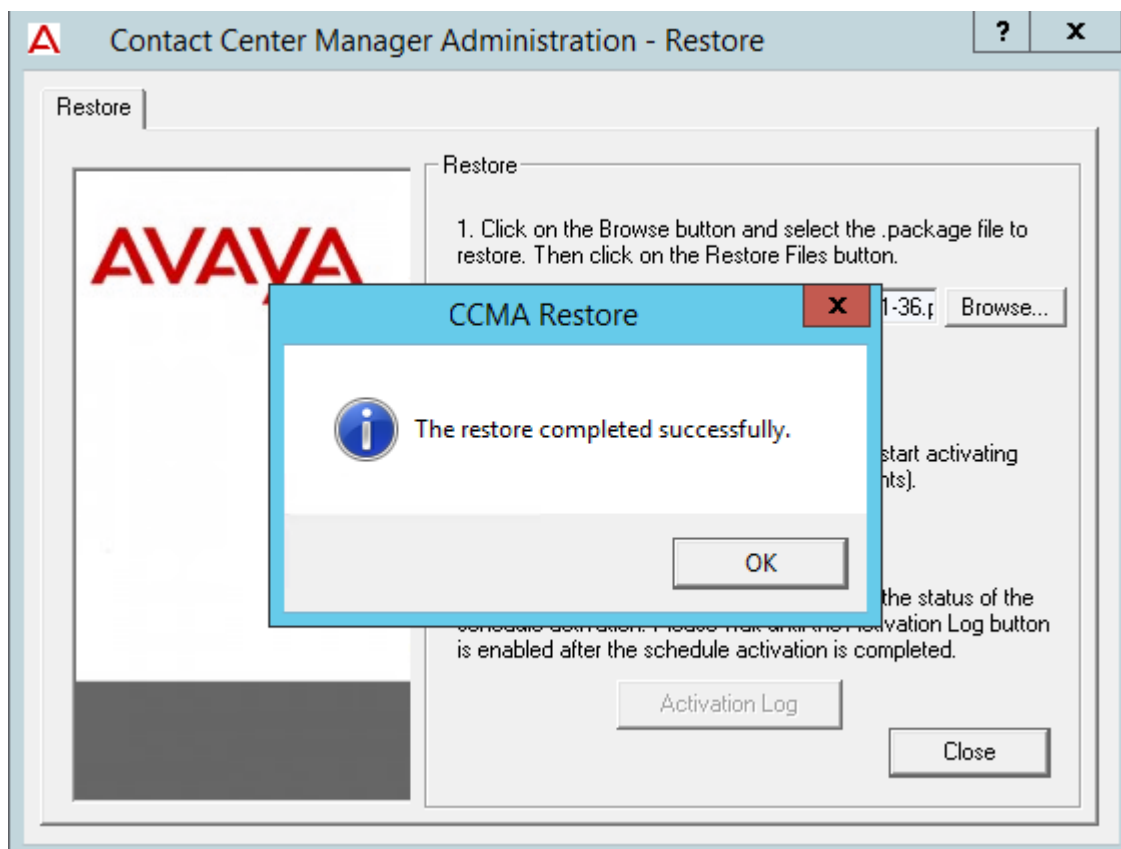
Procedure

1. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.
2. In the left pane of the Avaya Configuration window, expand **Avaya > Applications > Restore**.
3. In the right pane, click **Restore**.
4. On the **Restore** message box, click **OK**.

5. In the **Contact Center Manager Administration - Restore** dialog box, click the **Restore** tab.



6. To select a backup file to restore from, click **Browse**.
 7. In the **Select a backup file** dialog box, select the required .package file.
 8. Click **Open**.
 9. To restore the backup file data onto the administration data server, click **Restore Files**.
- The restore completed successfully message box appears.



10. Click **OK**.

Upgrading the Contact Center Manager Administration data

Before you begin

- Restore the backed up Contact Center Manager Administration (CCMA) data.

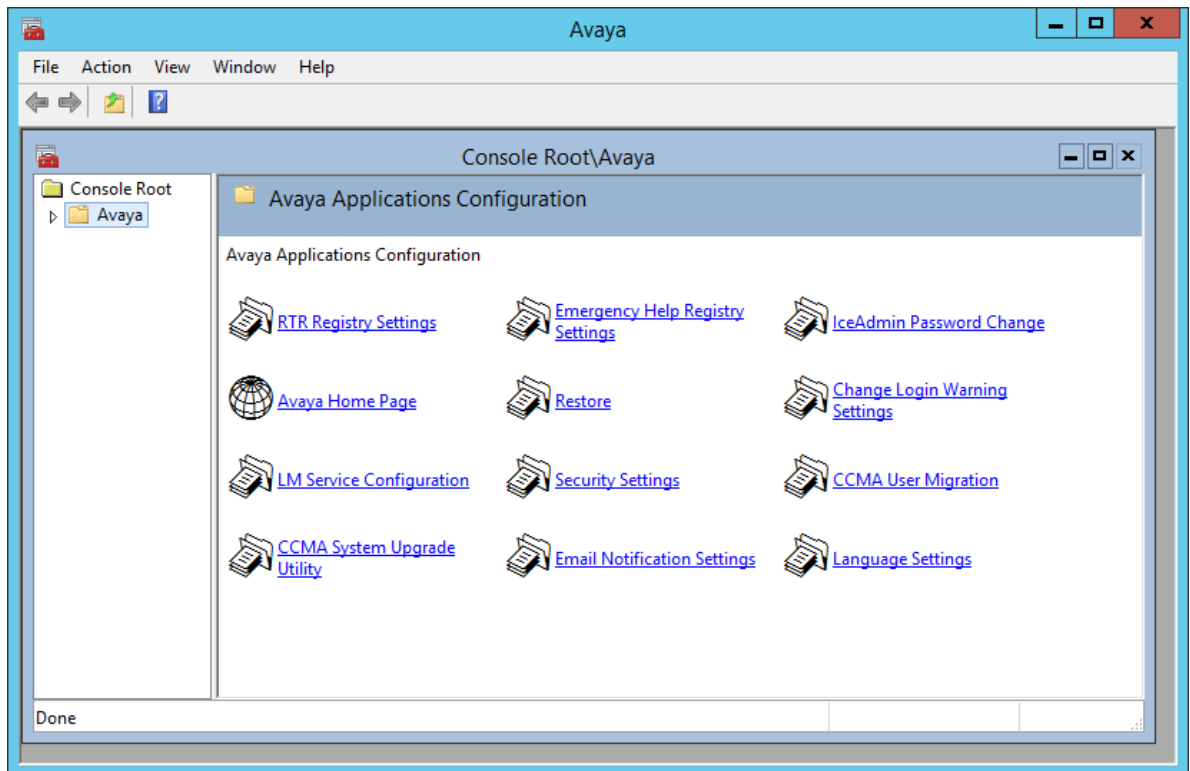
About this task

Upgrade Contact Center Manager Administration (CCMA) data to the Intersystems Caché database format used by Avaya Aura® Contact Center Release 7.1.

Procedure

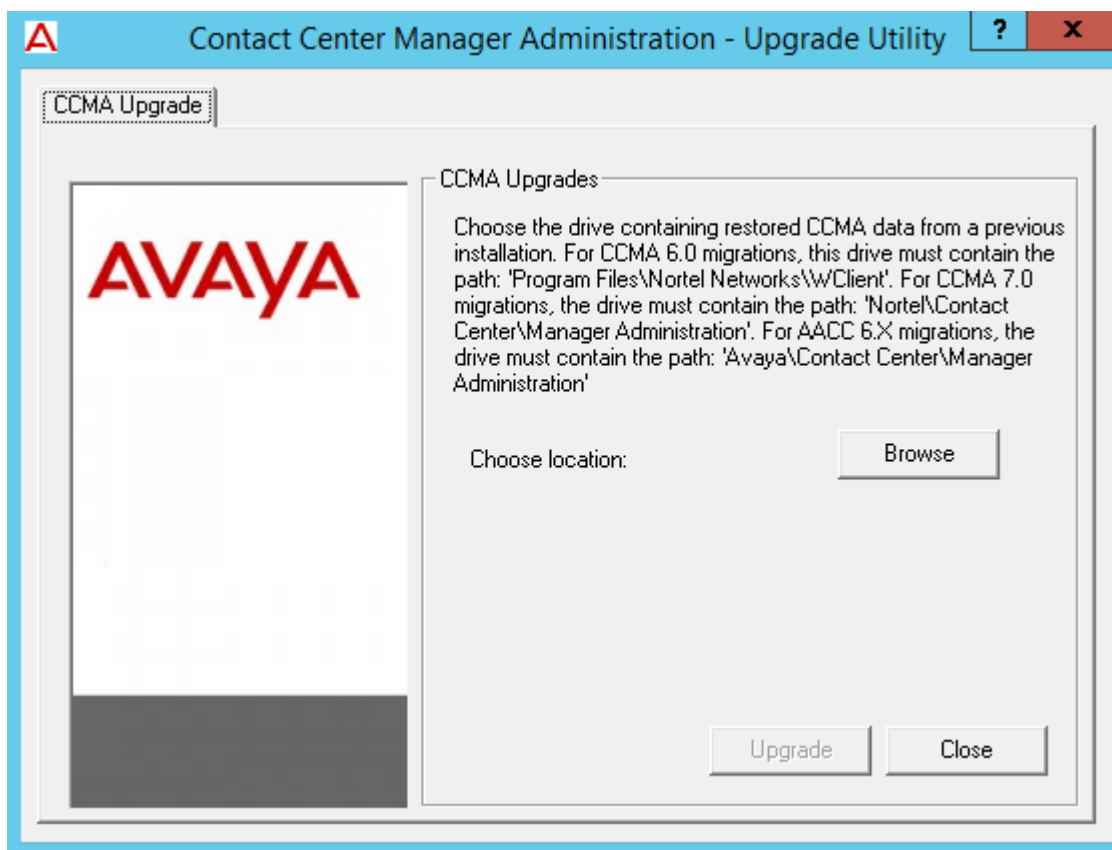
1. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.

2. In the left pane, click **Avaya** > **Applications** > **CCMA System Upgrade Utility**.



3. In the right pane, click **CCMA System Upgrade Utility**.

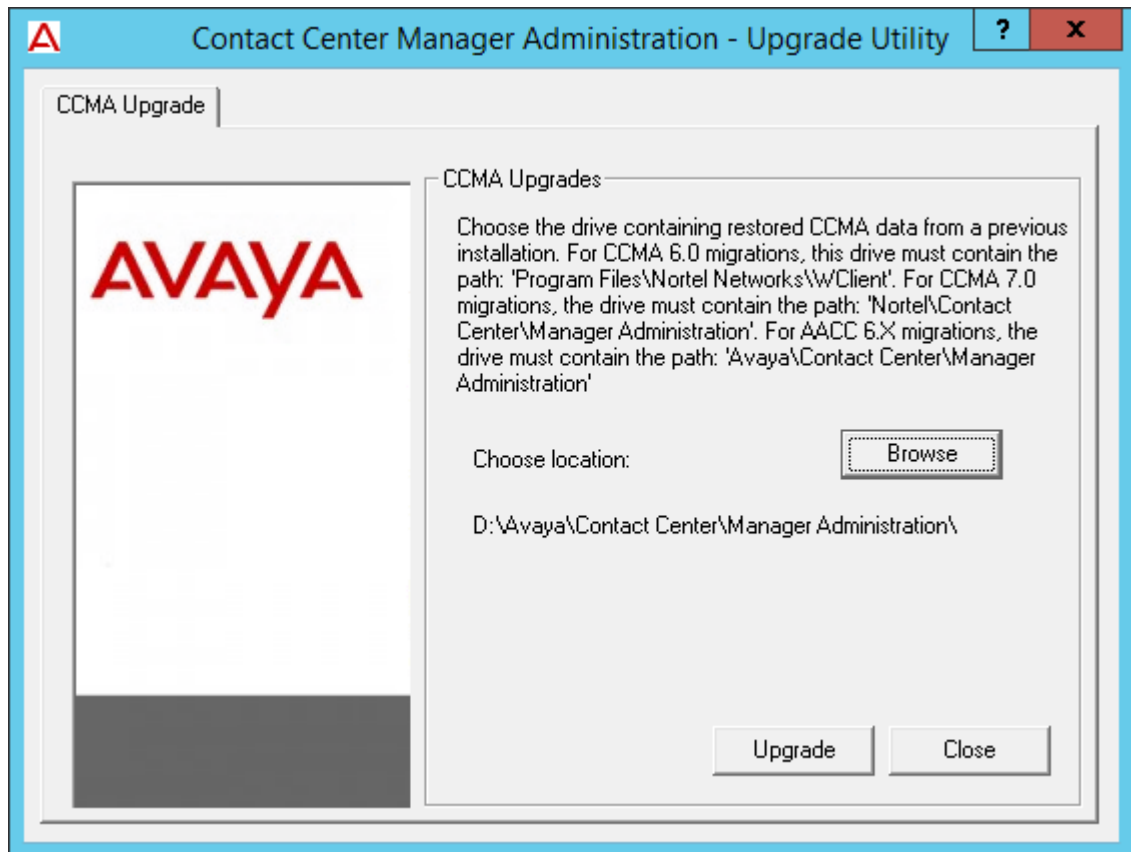
4. Click **Yes** on the confirmation dialog box.



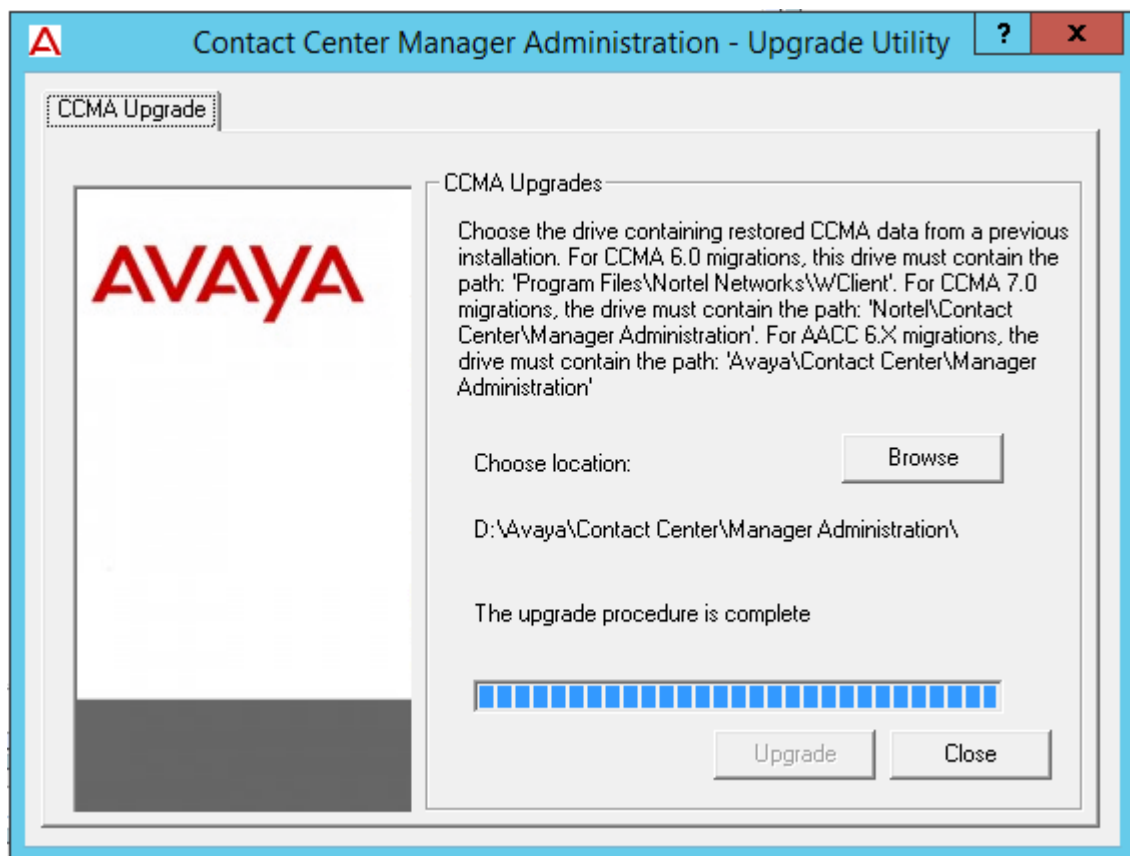
5. On the Upgrade Utility, click **Browse** and follow the instructions on the **CCMA Upgrades** screen to choose a location.

Select only the drive letter as the location of the restored CCMA data. The upgrade utility automatically detects and appends the correct directory structure for the old system data.

Example of upgrading from an Avaya Aura® Contact Center Release 6.4 system:



6. Click **Upgrade**.



7. Close the Upgrade Utility application. Click **Close**.

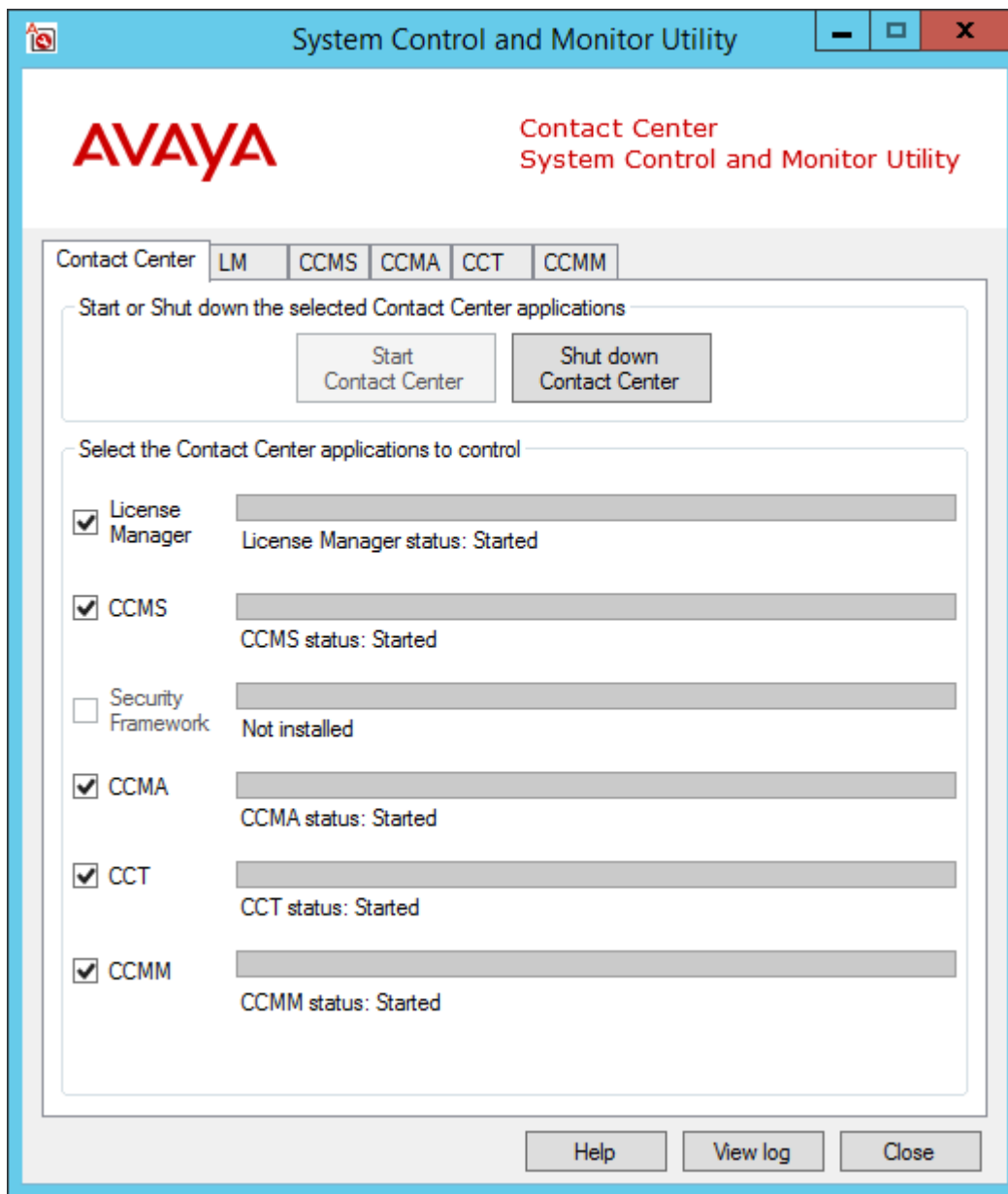
Starting Contact Center services

About this task

Start the Contact Center services to begin re-configuration after migrating or upgrading a system. The database restore and upgrade utilities automatically stop Contact Center services. Start Contact Center services to continue commissioning the solution.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **System Control and Monitor Utility**.
3. Click the **Contact Center** tab.
4. Click **Start Contact Center**.



Wait for Contact Center services to start.

Configuring the Contact Center Manager Administration system components

About this task

Configure the Contact Center Manager Administration (CCMA) system components for the new solution. Ensure the Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), and Contact Center Multimedia (CCMM) settings are correct for the new solution.

To access CCMA and other Contact Center components, you must use the Microsoft Edge browser in Internet Explorer mode.

Procedure

1. In your browser, type the URL of the server and then press **Enter**.
The default URL is `https://<server name>`, where `<server name>` is the host name of the Avaya Aura® Contact Center Release 7.1.x server. If you turned off Web Services security, use `http://<server name>`.
2. On the main login page, in the **User ID** field, type the username.
The default user ID is `webadmin`.
3. In the **Password** box, type the password.
The default password is `webadmin`.
4. Click **Log In**.
5. On the launchpad, click **Configuration**.
6. In the left pane, right-click the CCMS server name and then click **Edit Properties**.
7. Update the Contact Center Manager Server details to match your new solution and then click **Submit**.
8. In the left pane, right-click the CCMS server name and then click **Refresh Server**.
9. On both Contact Center Manager Administration dialogs, click **Yes**.
10. In the left pane, right-click **CCT** and then click **Edit Properties**.
11. Update the Communication Control Toolkit details to match your new solution and then click **Submit**.
12. In the left pane, right-click **CCMM** and then click **Edit Properties**.
13. Update the Contact Center Multimedia details to match your new solution and then click **Submit**.
14. Log off from CCMA.
15. Using the System Control and Monitor Utility (SCMU), restart Avaya Aura® Contact Center services.

Configuring the Contact Center Multimedia new details

About this task

Configure the Contact Center Multimedia (CCMM) Dashboard and Administration details.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Multimedia Dashboard**.
3. On the CCMM Dashboard, under **Server Availability**, right-click **Contact Center Manager Administration** and select **Edit**.
4. On the **Administrator Login** dialog, in the **User Name** box, type `GeneralAdmin`.
5. In the **Password** box, type the password. The default password is “__ccmm!”.
6. Click **Login**.
7. On the **Administrator Login** dialog, in the text box, type the name for the current Voice and Multimedia Contact Server.
8. Click **Save**.
9. Log on to the new Contact Center Manager Administration Web interface with administrative privileges.
10. On the **Launchpad**, click **Multimedia**.
11. In the left pane, select the Contact Center Multimedia to which you want to log on.
12. Under **CCMM Administration**, select **General Administration**.
13. Select **Server Settings**.
14. Update the server names to match the new Contact Center solution.
15. Under **CCMM Administration**, on the main menu, select **E-mail > General Settings**.
16. Under **Attachment Files**, ensure the **Inbound URL**, **Inbound Share**, **Outbound URL**, and **Outbound Share** locations match the new Contact Center solution.
17. Restart the Contact Center server.

Configuring Multimedia data management

About this task

When you migrate from a multimedia-enabled AACC Release 6.3 or earlier, Contact Center creates a new offline database and applies new data management tasks and utilities. To ensure efficient use of the Multimedia database drive on the new Contact Center server, configure Multimedia data management.

Procedure

Use the CCMM Data Management tool to create and schedule cleanup tasks to clear closed contacts from the MULTIMEDIA database. For more information on using the CCMM Data Management tool, see *Maintaining Avaya Aura® Contact Center*.

Configuring settings for Multimedia Complement for Elite server migration

About this task

If you are migrating from an existing Avaya Aura® Contact Center Multimedia Complement for Elite server, perform the following steps on the new Voice and Multimedia Contact Server to complete the migration.

Procedure

1. Update the Local Settings, SIP Network Settings, and SIP Local Subscriber data on the new server using the Server Configuration utility.
2. Ensure that the licensing details are configured correctly on the new server.
3. Log on to CCMA Configuration, right-click on each server and select **Edit Properties**. Update the server details for the new solution.
4. Open the CCMM Administration utility and perform the following steps:
 - a. Click **General Administration > Server Settings**. Ensure that the server details are correct for the new solution.
 - b. Click **E-mail > General Settings**. Ensure that the details are correct for the new solution.
5. Open the Multimedia Dashboard. Ensure that the Computer Name for the CCMA and CCMM servers are correct for the new solution.
6. Restart the server.
7. On each client computer, uninstall Agent Desktop. Install Agent Desktop using the new server name.

Note:

At this point in the migration, existing agents can process Multimedia contacts as before.

8. Using the Configuration Tool or CCMA Management, add a Voice URI for each agent and assign each agent to a voice skillset. After you reconfigure the agent details, agents must log out and log back on to complete these configuration changes.

+ Tip:

Use the Configuration Tool to perform a bulk change.

Converting custom RCW reports to Contact Center R7.1 format

About this task

Copy the zip file of converted RCW reports to the Contact Center R7.1 server, and convert each report to SSRS format.

Before you begin

Prepare the RCW reports for migration on the old server, and copy them to a network location.

Custom formulas do not migrate to the new server. If the original reports use custom formulas on the existing server, the formulas do not migrate with the custom reports.

Contact Center creates a placeholder formula for each custom formula. The placeholder displays an asterisk character on the migrated report. If possible, the placeholder formula includes the original Crystal Syntax formula text as a comment. You must edit the placeholder formulas, entering valid SSRS expressions for the formula text, to complete the migration. The placeholder formula is limited to 32,000 characters, so it is possible that very long formulas can be truncated.

Document all the custom formulas on the existing server, to assist with re-creating them on the new server after migrating the Contact Center databases.

Procedure

1. Log on to the Contact Center R7.1 server.
2. Run the RCW report utility `d:\avaya\contact center\manager administration\server\bin\MigrationRCWImporter.exe`
3. On the RCW Importer screen, click **Browse**, and browse to and select the zip file of converted RCW reports.
4. Click **Run** to start the conversion.
The RCW Importer utility unpacks the reports to the RCW\Private folder.
5. Log on to Contact Center Manager Administration.
6. On the **Launchpad**, click **Historical Reporting**.
7. In the left pane, click the Contact Center Manager Server.
8. From the **Report** menu, select **Report Creation Wizard**.
9. Select **Open Existing Report**.
10. For each `.rcwx` report in the list:
 - a. Select the report and click **Next**.

Contact Center opens the report in RCW.

- b. Click the **Preview Report** button.
- c. On the Preview Data Filter screen, click **Preview**.

Check that the report opens correctly in the preview.

- d. If you saw errors in the preview, correct the data fields and formulas as applicable.
- e. Click the **Save Report** button.
- f. On the Save RCW Report window, click **Save**.

Do not change the default file location: the .rdl file must save in the same location as the .rcwx file.

Contact Center saves the report in .rdl format.

Commissioning the Contact Center solution

About this task

Commission the Contact Center solution.

Procedure

1. After migrating your server and restoring the server databases, some of the old configuration settings might not match your new solution. Commission your new server in the new solution. For more information, refer to *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000* or *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications*.
2. Use the procedures in *Avaya Aura® Contact Center Server Administration* to configure your licensed features.

Chapter 6: Voice and Multimedia Contact Server without Avaya Aura[®] Media Server patch installation

This chapter describes how to install patches on the Voice and Multimedia Contact Server without Avaya Aura[®] Media Server Release 7.1 server.

If your Avaya Aura[®] Contact Center is licensed for Standby Servers, you can hot patch your software to minimize down time. You must ensure that you patch both the active and standby servers to the same patch level. For information about hot patching, see [Common procedures](#) on page 353.

A Voice and Multimedia Contact Server without Avaya Aura[®] Media Server includes the following server software:

- Contact Center Manager Server (CCMS)
- Contact Center Manager Server Utility
- Contact Center License Manager (LM)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center Multimedia (CCMM)
- Avaya Workspaces (optional)

Voice and Multimedia Contact Server without Avaya Aura[®] Media Server patch installation prerequisites

- Download the most recent documentation. See [Downloading the most recent documentation](#) on page 45.
- Download and review the latest Avaya Aura[®] Contact Center Release Notes. The Release Notes contain information about known issues, patches, and workarounds specific to a release and patch line-up of Contact Center. For more information about the Contact Center Release Notes, see the Avaya website (<http://support.avaya.com>).

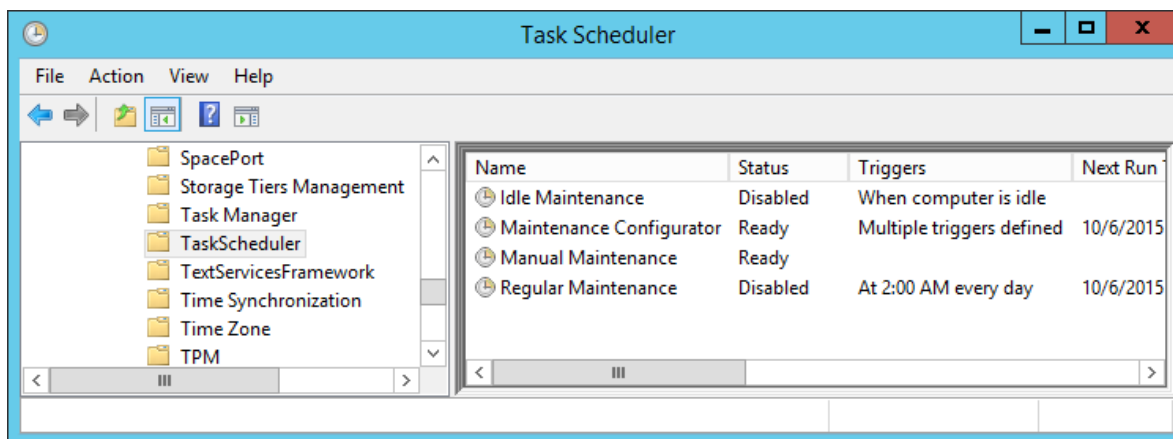
Disabling Windows Server Automatic Maintenance

About this task

Disable Windows Server Automatic Maintenance while updating Contact Center software. Windows Server Automatic Maintenance can occasionally interfere with the real-time requirements for Contact Center. You must therefore temporarily disable Automatic Maintenance to update Contact Center software. Re-enable it after the update.

Procedure

1. Log on to the Contact Center server as an administrator.
2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Disable**.
5. In the **Name** column, right-click **Regular Maintenance** and then click **Disable**.



6. From the **File** menu, click **Exit**.

Installing Voice and Multimedia Contact Server without Avaya Aura® Media Server Release Packs, Feature Packs and Service Packs

Before you begin

- Download the most recent Contact CenterRelease Pack, Feature Pack and Service Packs.
- Download the most recent Contact Center software patches.
- Back up the Contact Center databases.

- Temporarily stop Microsoft Windows Server Automatic Maintenance while you update Voice and Multimedia Contact Server software.
- Avoid installation from shared locations, because it might lead to installation failure. To ensure successful installation, mount the Release Bundle or install it locally.
- If you deploy in a virtual environment and want to install Avaya Workspaces, you must manually deploy three virtual machines using the Avaya Workspaces Open Virtual Appliance (OVA). See [Deploying the Avaya Workspaces OVA](#) on page 177.

About this task

Install the most recent Voice and Multimedia Contact Server Release Packs, Feature Packs and Service Packs to take advantage of new features, and to ensure that you have the most current application updates.

Procedure

1. Open the Release Pack, Feature Pack or Service Pack ZIP file.
2. Browse to the Avaya Release Pack Installer directory.
3. Double-click `setup.exe` to launch the Contact Center Release Pack Installer.
4. If you downloaded GA patches along with the Release Pack:
 - a. Select **Yes**.
 - b. Click **Browse**.
 - c. On the Browse for Folder screen, browse to the folder where you downloaded the patches, and click **OK**.
5. **(Optional)** If you want to configure Avaya Workspaces:
 - For non-HA solutions, select **Yes**.
 - For HA solutions, if installing on the Active server, select **Yes**.
 - For HA solutions, if installing on the Standby server, select **No**. You must only configure Avaya Workspaces on your Active server.
6. On the Contact Center Release Pack Installer screen, click **Next**.
7. On the Avaya Global License Terms screen, click **I ACCEPT THE LICENSE TERMS**.
8. On the MICROSOFT SOFTWARE LICENSE TERMS screen, click **I ACCEPT THE LICENSE TERMS**.

The Avaya Release Pack Installer shuts down Contact Center and installs the Release Pack, Feature Pack or Service Pack.
9. When the software update completes successfully, click **Restart**.

Contact Center reboots the server.

Next steps

If you select to configure Avaya Workspaces, when Contact Center restarts, the Contact Center Update Configurator opens so that you can configure Avaya Workspaces. For more information, see [Configuring Avaya Workspaces using the Update Configurator](#) on page 365.

Installing Voice and Multimedia Contact Server without Avaya Aura® Media Server software patches

Before you begin

- Download the most recent Contact Center patches.
- Ensure that you have a recent backup of the Contact Center databases. Avaya recommends that you schedule a daily backup of the Contact Center databases at an off peak time. For more information on scheduling backups, see *Maintaining Avaya Aura® Contact Center*.
- Temporarily stop Microsoft Windows Server Automatic Maintenance while you update Voice and Multimedia Contact Server software.

About this task

Install the most recent Voice and Multimedia Contact Server software patches to ensure that you have the most current application updates.

Procedure

1. From the **Start** menu, in the Avaya area, click **Update Manager**.
2. Click **Install**.
3. Click **Browse** and navigate to the folder where you downloaded the patches.
4. Click **Scan for Patches**.

The Contact Center Updates section displays the available patches.

5. Select the appropriate patches.
6. Click **Install Patch(es)**.

The Update Manager installs the patch and displays a confirmation message.

7. Click **Close**.
8. Verify that the newly installed patch appears under **Installed Updates**.
9. If the System Management and Monitoring Component (SMMC) is installed on the server, verify that it starts. For more information about starting SMMC, see [Starting SMMC](#) on page 358.

Next steps

Re-enable Microsoft Windows Server Automatic Maintenance.

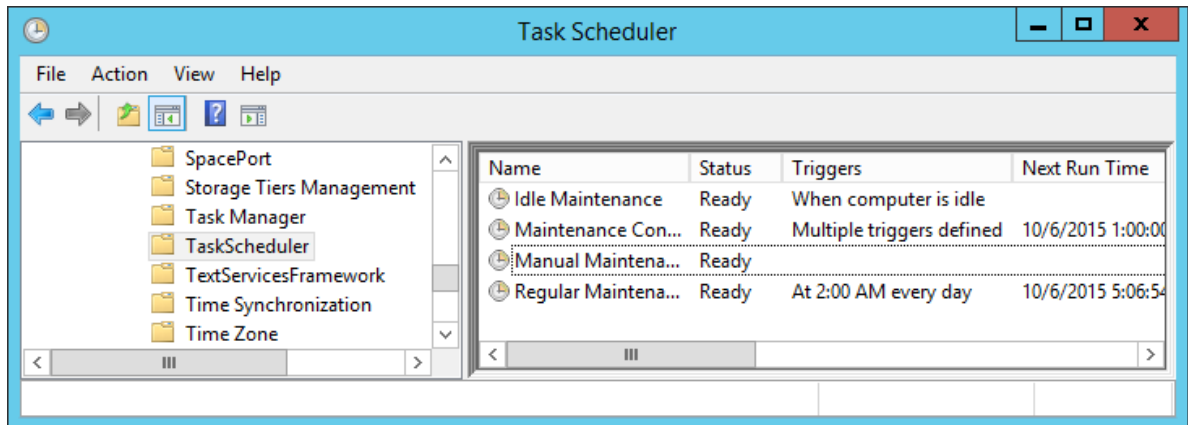
Enabling Windows Server Automatic Maintenance

About this task

Enable Windows Server Automatic Maintenance after updating Contact Center software.

Procedure

1. Log on to the Contact Center server as an administrator.
2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Enable**.
5. In the **Name** column, right-click **Regular Maintenance** and then click **Enable**.



6. From the **File** menu, click **Exit**.

Part 2: Voice Contact Server migrations and patches

- [Voice Contact Server migration](#) on page 117
- [Voice Contact Server patch installation](#) on page 165

Chapter 7: Voice Contact Server migration

This chapter describes how to migrate Avaya Aura® Contact Center Release 6.x to a new server running Avaya Aura® Contact Center Voice Contact Server Release 7.1.x. This chapter also describes how to migrate Avaya Aura® Contact Center Voice Contact Server from one Release 7.x server to another.

Existing system	New server
Avaya Aura® Contact Center Release 6.x on Windows Server 2008 R2	Avaya Aura® Contact Center Voice Contact Server Release 7.1.x on Windows Server 2016 or 2019
Avaya Aura® Contact Center Voice Contact Server Release 7.0 on Windows Server 2012 R2	
Avaya Aura® Contact Center Voice Contact Server Release 7.1.x on Windows Server 2016 or 2019	

This section describes how to migrate from an existing Avaya Aura® Unified Communications SIP enabled solution to a new Avaya Aura® Contact Center Release 7.1.x SIP enabled solution.

This section also describes how to migrate from an existing Avaya Communication Server 1000 AML-based solution to a new Avaya Aura® Contact Center Release 7.1.x AML-based solution.

You can use the procedures in this chapter to:

- Migrate data from your existing co-resident Contact Center Manager Server, Contact Center Manager Administration, and Communication Control Toolkit server to a new Avaya Aura® Contact Center Voice Contact Server.
- Migrate Contact Center Manager Server, Contact Center Manager Administration, and Communication Control Toolkit to a single Voice Contact Server.
- Migrate an Avaya Aura® Contact Center Voice Contact Server to a new server. For example, to move Voice Contact Server Release 7.1.x software from one server to a new larger and faster server.

An Avaya Aura® Contact Center Voice Contact Server server includes the following server software:

- Contact Center Manager Server (CCMS)
- Contact Center Manager Server Utility
- Contact Center License Manager (LM)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)

Voice Contact Server migration prerequisites

- Ensure that your hardware meets all requirements as described in *Avaya Aura® Contact Center Overview and Specification*.
- Prepare your new server for software installation. For more information see, [Common server preparation procedures](#) on page 45.

Voice Contact Server migration procedures

About this task

This task flow shows you the sequence of procedures you perform to migrate to an Avaya Aura® Contact Center 7.1 Voice Contact Server.

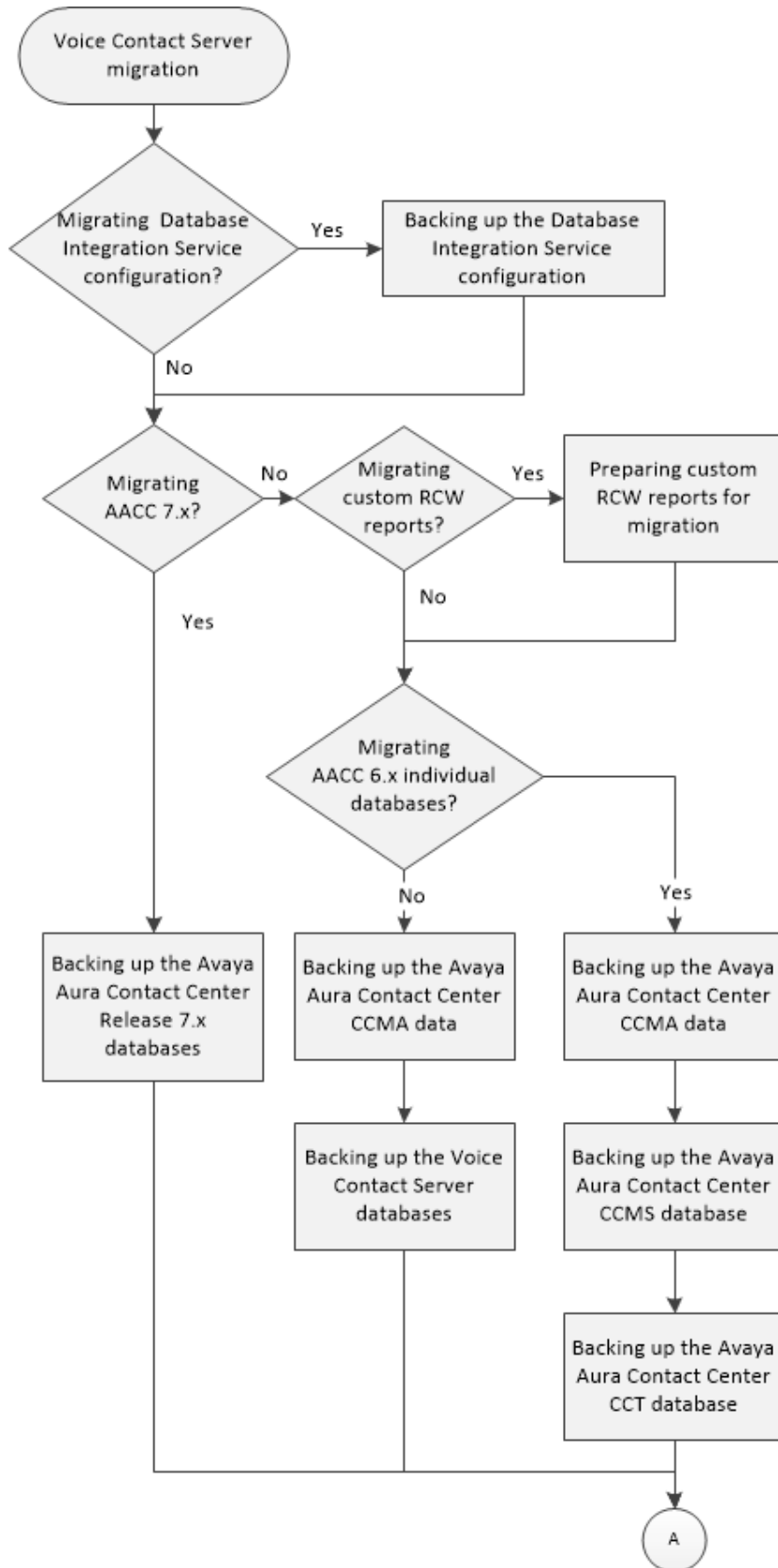
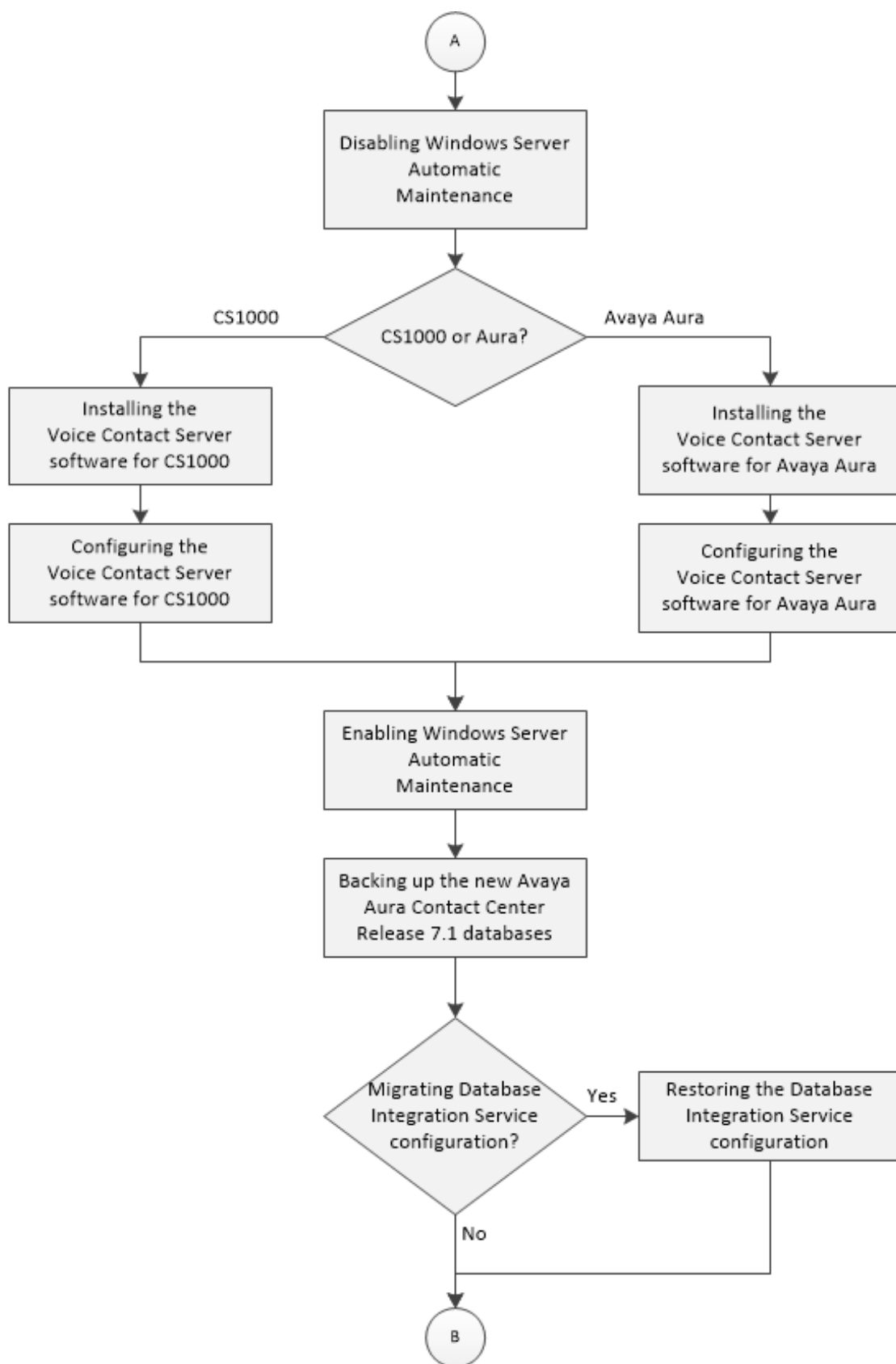
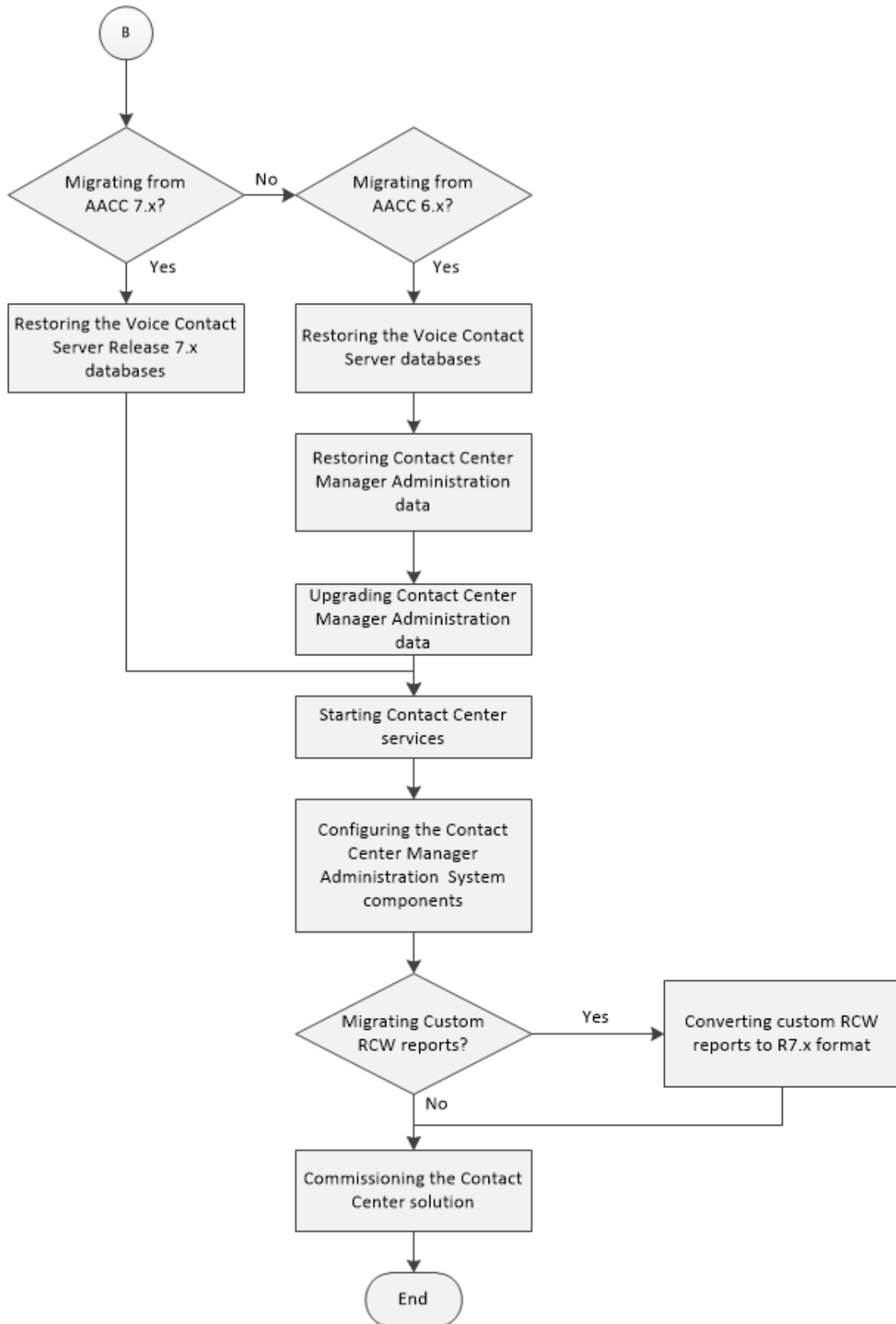


Figure 5: Voice Contact Server migration procedures

**Figure 6: Voice Contact Server migration procedures continued**

**Figure 7: Voice Contact Server migration procedures continued**

Backing up the Database Integration Service configuration

Before you begin

- When you migrate the Database Integration Service to a new Contact Center server, you must manually re-configure any custom DSNs that you use in your solution.

About this task

Back up the Database Integration Service configuration to migrate the content to the new Contact Center server. Avaya recommends that you save the configuration file to a network location that you can access from the new server.

Procedure

1. On the server, click **Start** > **Run**.
2. In the Open box, type `regedit`.
3. Click **OK**.
4. If you are migrating from a Windows 2008 server (Release 6.x Avaya Aura® Contact Center):
 - a. In the Registry Editor, open the key
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Avaya\ICCM\HAI
 - b. From the **File** menu, select **Export**.
 - c. In the Export Registry File dialog box, type a name and location in which to store the configuration file.
 - d. Click **Save**.
5. Close the Registry Editor.

Backing up the Avaya Aura® Contact Center Release 7.1 databases

About this task

Back up the Avaya Aura® Contact Center Release 7.1 databases so you can restore them on the new server after you install the Avaya Aura® Contact Center Release 7.1 software.

Procedure

1. Log on to the existing Avaya Aura® Contact Center Release 7.1 server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
4. In the right pane, click **Create**.

5. From the **Drive Letter** list, select the network drive on which to store the Voice Contact Server database.
6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.
7. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the user password.
9. Click **Save**.
10. Click **OK**.
11. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
12. In the **Media Type** section, select **Network Location**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.
15. Click **Yes**, to continue with the backup.

Preparing custom RCW reports for migration

About this task

You can migrate custom historical reports built using Report Creation Wizard (RCW) in earlier releases to equivalent SSRS reports on Contact Center 7.1. Export the original reports from Crystal format (.rpt) to intermediate files and save them in a network location. After installing the new server you can restore and convert the saved files to SSRS format.

Contact Center 7.x Service Packs include a utility to export the reports. The utility can be found in the "Install Software\CCMA\RCW_Migration_Utility" folder in the Service Pack. This is one version of the utility: AACC 6.x.

Before you begin

Important:

Custom formulas do not migrate to the new server. If the original reports use custom formulas on the existing server, the formulas do not migrate with the custom reports.

Contact Center creates a placeholder formula for each custom formula. The placeholder displays an asterisk character on the migrated report. If possible, the placeholder formula includes the original Crystal Syntax formula text as a comment. You must edit the placeholder formulas, entering valid SSRS expressions for the formula text, to complete the migration. The placeholder formula is limited to 32,000 characters, so it is possible that very long formulas can be truncated.

Document all the custom formulas on the existing server, to assist with re-creating them on the new server after migrating the Contact Center databases.

Procedure

1. From the `\Install Software\CCMA` directory on the most recent AACC R7.x Service Pack, copy the utility for exporting Crystal reports.

You must copy the version of the utility that corresponds to the Contact Center version from which you are migrating.

2. On the Contact Center server from which you are migrating, extract the tool.
3. Run `MigrationRPTToRCWX.exe`.
4. On the Convert RTP to RCWX screen, click **Browse**, and choose a folder in which to store the output files for the converted reports.
5. Click **Run** to start the conversion.
6. When the export completes, copy the zip file to a network location from which you can copy it to the new Contact Center R7.1 server.

Next steps

Copy the zip files of exported reports to the new Contact Center server, and run the RCW import utility to convert each report to SSRS format.

Backing up the Avaya Aura[®] Contact Center CCMA data

Before you begin

- Map a network drive on which to back up your database. The network drive must be in NTFS format.
- Log on to the Contact Center Manager Administration server as an administrator.

About this task

Back up the Contact Center Manager Administration data on the source server Release 6.x to enable migration of the data to the new Contact Center server.

If your Contact Center Manager Administration uses High Availability replication, you must backup the data from the active CCMA.

Procedure

1. On the server with CCMA, choose **Start > All Programs > Avaya > Contact Center > Manager Administration > Configuration**.
2. In the left pane of the **Avaya Configuration** window, expand **Avaya > Applications > Backup & Restore**.
3. In the right pane, click **Backup & Restore**.
4. In the **Contact Center Manager Administration - Backup And Restore** dialog box, click **Backup** tab.

5. Select **Drive**.
6. Type the drive where the backed up database is stored.
7. Click **Next**.
8. In the **Perform Backup** section, select **Run Now**.
9. Click **Next**.
10. In the **Username** box, type a user name with administrative privileges for the server to which you store the backup.
11. In the **Password** box, type a password with administrative privileges for the server to which you store the backup.
12. From the **Domain** list, select the domain of the server to which you store the backup.
13. Click **Finish**.

Backing up the Voice Contact Server Release 6.x databases

About this task

Back up the Release 6.x Voice Contact Server databases so you can restore them on the new server after you install the Avaya Aura® Contact Center Release 7.1 software.

Procedure

1. On the existing Release 6.x Voice Contact Server, choose **Start > All Programs > Avaya > Contact Center > Database Utilities > Database Maintenance**.
2. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the right pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which to store the Voice Contact Server database.
5. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.
9. Click **OK**.

10. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. From the **Backup Location** list, select the network drive on which to store the backup.
13. Click **Backup**.
14. Click **Yes**, to continue with the backup.

Backing up the Avaya Aura[®] Contact Center CCMS database

About this task

Back up the Avaya Aura[®] Contact Center CCMS 6.x individual database so you can restore it on the new server after you install the Avaya Aura[®] Contact Center software.

Procedure

1. On the Contact Center Manager Server, choose **Start > All Programs > Avaya > Contact Center > Database Utilities > Database Maintenance**.
2. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the right pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which to store the Contact Center Manager Server database.
5. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.
9. Click **OK**.
10. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Applications** section, select **CCMS**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.

15. Click **Yes**, to continue with the backup.

Backing up the Avaya Aura® Contact Center CCT database

About this task

Back up the Avaya Aura® Contact Center CCT 6.x individual database so you can restore it on the new server after you install the Avaya Aura® Contact Center software.

Procedure

1. On the Communication Control Toolkit server, choose **Start > All Programs > Avaya > Contact Center > Database Maintenance**.
2. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the Backup Locations pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which you stored the Communication Control Toolkit database.
5. In the **UNC Path** box, type the location of the Communication Control Toolkit database in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.
9. Click **OK**.
10. In the Contact Center Database Maintenance window, in the Main Menu pane, select **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Applications** section, select **CCT**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.

Disabling Windows Server Automatic Maintenance

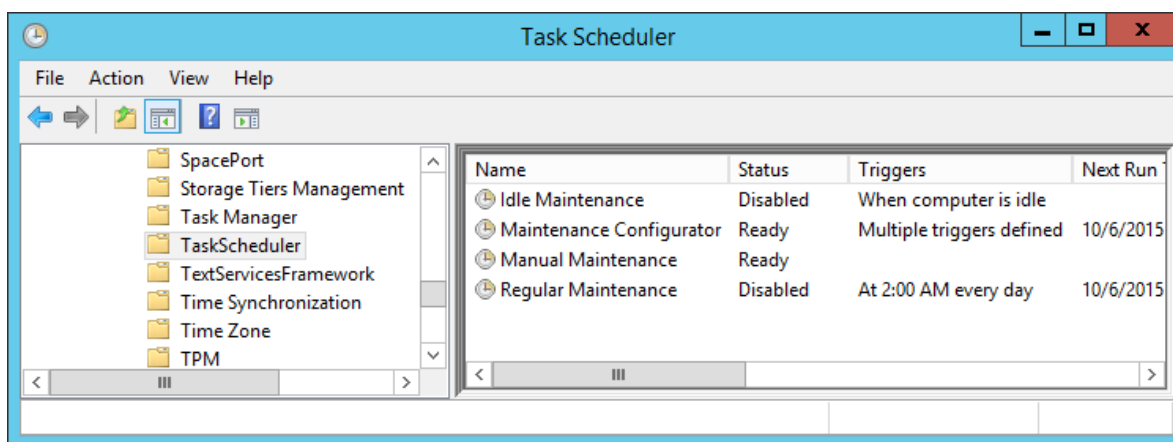
About this task

Disable Windows Server Automatic Maintenance while installing Contact Center software. Windows Server Automatic Maintenance can occasionally interfere with the real-time

requirements for Contact Center. You must therefore temporarily disable Automatic Maintenance to install and configure Contact Center software. Re-enable it after deploying Contact Center.

Procedure

1. Log on to the Contact Center server as an administrator.
2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Disable**.
5. In the **Name** column, right-click **Regular Maintenance** and then click **Disable**.



6. From the **File** menu, click **Exit**.

Installing the Voice Contact Server software for Avaya Aura® Unified Communications platform

Before you begin

- Ensure the Avaya Aura® Unified Communications platform is configured. For more information see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.
- Download the most recent Contact Center patches to the server.

About this task

Install the Contact Center Voice Contact Server software and enable your contact center to route contacts to the agents that can answer the call with the correct skills.

Procedure

1. Insert the Contact Center DVD into the DVD drive of your server.

2. If the installation does not automatically start, double-click **Setup.exe**.

3. Click **Accept** to install the Microsoft .NET Framework on the server.

If you are prompted to accept the Microsoft .NET Framework license agreement, click **Accept**. If you are prompted to restart the server, click **Yes** and repeat step 2.

4. Contact Center software installer runs Operating System and hardware checks on the server. If the installer returns a Fail, the software installation cannot proceed until you correct the problem. Review any failures returned by the System Readiness Check and consult *Avaya Aura® Contact Center Overview and Specification* to determine the actions to resolve the issue.

You can ignore warnings if the potential impact to the operation of the contact center is understood and not applicable.

5. The Contact Center software installer platform and server selection screen appears.
6. In the **Select Voice Platform** section, select **Avaya Aura - SIP**.
7. In the **Select Server Installation Option** section, select **Voice Contact Server Only**.
8. Click **Next**.
9. Under **Journal Database Drive**, select the drive for the database journal.
10. Under **Voice Contact Server Database Drive**, select the drive for the Contact Center Manager Server, Communication Control Toolkit, and Contact Center Manager Administration databases. The default drive partition is F:.
11. In the **Service Packs** section, browse to and select the Service Pack.



12. Click **Install**.
13. The **AVAYA GLOBAL SOFTWARE LICENSE TERMS** window appears.
14. Read the terms of the license.
 - If you accept the terms, click **I ACCEPT THE LICENSE TERMS**. *The installation continues.*
 - If you do not accept the terms, click **I DECLINE THE LICENSE TERMS**. *The installation returns to the Select Destination Drive screen.* Click **Cancel** to stop the install.
 - To print the license terms, click **Print**.
15. The **MICROSOFT SOFTWARE LICENSE TERMS** window appears.
16. Read the terms of the license.
 - If you accept the terms, click **I ACCEPT THE LICENSE TERMS**. *The installation continues.*
 - If you do not accept the terms, click **I DECLINE THE LICENSE TERMS**. *The installation returns to the Select Destination Drive screen.* Click **Cancel** to stop the install.
 - To print the license terms, click **Print**.

17. The **Progress** window appears and displays the installation progress.
18. When the software is installed, you have the following options.
 - To continue configuring the server installation data:
 - a. Select **Launch Avaya Aura Contact Center Ignition Wizard**.
 - b. Click **Configure**. This starts the Avaya Aura® Contact Center Ignition Wizard.
 - To defer configuring the server installation data:
 - a. Clear **Launch Avaya Aura Contact Center Ignition Wizard**.
 - b. On the message box, click **Yes**.
 - c. On the main installer screen, click **Close**.
 - d. Follow the on-screen instructions and shut down the Contact Center server.

You must use the Ignition Wizard to initialize Avaya Aura® Contact Center, otherwise Avaya Aura® Contact Center is not operational. For more information about the Ignition Wizard, see the following procedure.

Configuring the Voice Contact Server software for Avaya Aura® Unified Communications platform

Before you begin

- Ensure the Avaya Aura® Unified Communications platform is configured. For more information see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.
- You must configure the required language and locale of the Contact Center server operating system, if it is not a Latin-1 language, before configuring the Contact Center server using the Contact Center Ignition Wizard. For more information about configuring language and locale settings on the Contact Center server, see *Avaya Aura® Contact Center Server Administration*.
- Read the Contact Center Release Notes for the most recent instructions.

About this task

Configure the Contact Center Voice Contact Server software and enable your contact center to route contacts to the agents that can answer the call with the correct skills.

Procedure

1. Log on to the Contact Center server using the Administrator account details.
2. On the Contact Center Ignition Wizard screen, click **Next**. If the Contact Center Ignition Wizard is not visible, click the Ignition Wizard shortcut on the desktop.
3. On the **End-User License Agreement** screen, read the license agreement. Optionally, click **Print** to generate a local soft copy (in OpenXPS Document format) of the license agreement.

4. Select **I Accept the Terms of the End-User License Agreement** and click **Next**.
5. On the **Configuration Data** window, type the configuration details for each tab.
6. Select the **Core** tab, and configure the server details.

The screenshot shows the 'Configuration Data' window for the Avaya Contact Center. The window has a blue header with the text 'Avaya Contact Center' and the Avaya logo. Below the header, the title 'Configuration Data' is displayed. A subtitle reads 'Enter the required configuration data.' There are four tabs: 'Core', 'Licensing', 'SIP', and 'Security Configuration'. The 'Core' tab is selected. It contains two main sections: 'Site Name' and 'Real-Time Statistics Multicast IP Address'. The 'Site Name' section has a text box with 'CC7SIP' entered. The 'Real-Time Statistics Multicast IP Address' section has a text box with '234.5.6.10' entered. To the right, the 'System Account Configuration' section is visible, with a subtitle 'Enter a password for the Contact Center administration Windows account.' It contains two password fields, both with '*****' entered. Below these fields, the text 'Passwords match' is displayed in green. At the bottom of the window, there is a button labeled 'Click Next to Continue' and three buttons: '< Back', 'Next >', and 'Cancel'.

7. In the **Site Name** box, type the site name for the Contact Center server. The site name must not contain spaces or non-alphabetical characters except hyphen (-) and underscore (_). The first character must be a letter. The site name must be unique and can consist of 6 to 15 characters.
8. In the **Real-Time Statistics Multicast IP Address** box, type the Real-time Statistics Multicast IP Address of the server to associate with sending real-time data. The **IP Address** must be from 224.0.1.0 to 239.255.255.255. The default is 234.5.6.10.
9. In the **System Account Configuration** section, in the **Password** box, type a password for the Contact Center administration account. The password is checked against the server security policy for minimum password requirements. Avaya recommends that you enter a password that conforms to your corporate password policy.
10. In the **Confirm Password** box, type the password.
11. Select the **Licensing** tab, and configure the licensing details.

The screenshot shows the 'Configuration Data' window for the Avaya Contact Center. The 'Licensing' tab is selected. The 'License Type' dropdown is set to 'Local WebLM'. The 'License File' section has a 'License File Location' field with a 'Browse' button and a 'Skip' button. The 'System HostID (MAC Address)' field contains '00:50:56:8D:48:8D'. The 'License Manager Package' dropdown is set to 'Nodal Enterprise'. The 'Features' section has several checkboxes: 'Networking', 'Instant Messaging', 'Web Based Statistics', 'Multiplicity', 'Open Queue', 'Open Interfaces Open Queue', 'Open Interfaces Universal Networking', 'Agent Greeting', and 'Offsite Agent'. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

12. From the **License Type** list, select **Local WebLM** to use the on-server WebLM license manager instance, or select **Remote WebLM** to use a separate Avaya WebLM server.
 - If you select **Local WebLM**, you cannot apply your Local WebLM license file until after you configure your contact center using the Ignition Wizard. You must apply your license file during the commissioning process.
 - If you select **Remote WebLM**, in the **IP Address** box, type the IP address for the remote Avaya WebLM server. In the **Port** box, type the port number for the remote Avaya WebLM server. The default port number is 52233.
13. From the **Licensing Package** list, select the license type that you have purchased. Select **Nodal Enterprise** for single-site contact centers.
14. From the list of **Optional Packages**, enable the licensed features that you have purchased.
15. Select the **Open Queue** check box.
16. Select the **SIP** tab, and configure the SIP details.

Avaya Contact Center

Configuration Data

Enter the required configuration data.

Core
Licensing
SIP
Security Configuration

Switch Configuration

Avaya Aura

SIP Voice Proxy Server

IP Address: Port: 5060 Transport: TCP

SIP CTI Proxy Server

IP Address: Port: 4723 Transport: TLS

Local SIP Subscriber

Domain Name:

Backup SIP Voice Proxy Server

IP Address: Port: 5060 Transport: TCP

SIP IM Proxy Server

IM Provider: Aura Presence Services

XMPP Domain:

IP Address: Port: Transport:

Click Next to Continue

< Back
Next >
Cancel

17. In the **SIP Voice Proxy Server** section, in the **IP Address** box, type the IP address for the primary Avaya Aura® Session Manager.
18. In the **SIP Voice Proxy Server** section, in the **Port** box, type the server listening port number. The default port is 5060.
19. In the **SIP Voice Proxy Server** section, from the **Transport** list, select the SIP Network Transport communication protocol. The default is TCP.

*** Note:**

If there are Contact Center agents using SIP deskphones, or if your solution uses Avaya Aura® Presence Services 7.1 or later, you must ensure that the SIP Network Transport communication protocol is set to TLS.

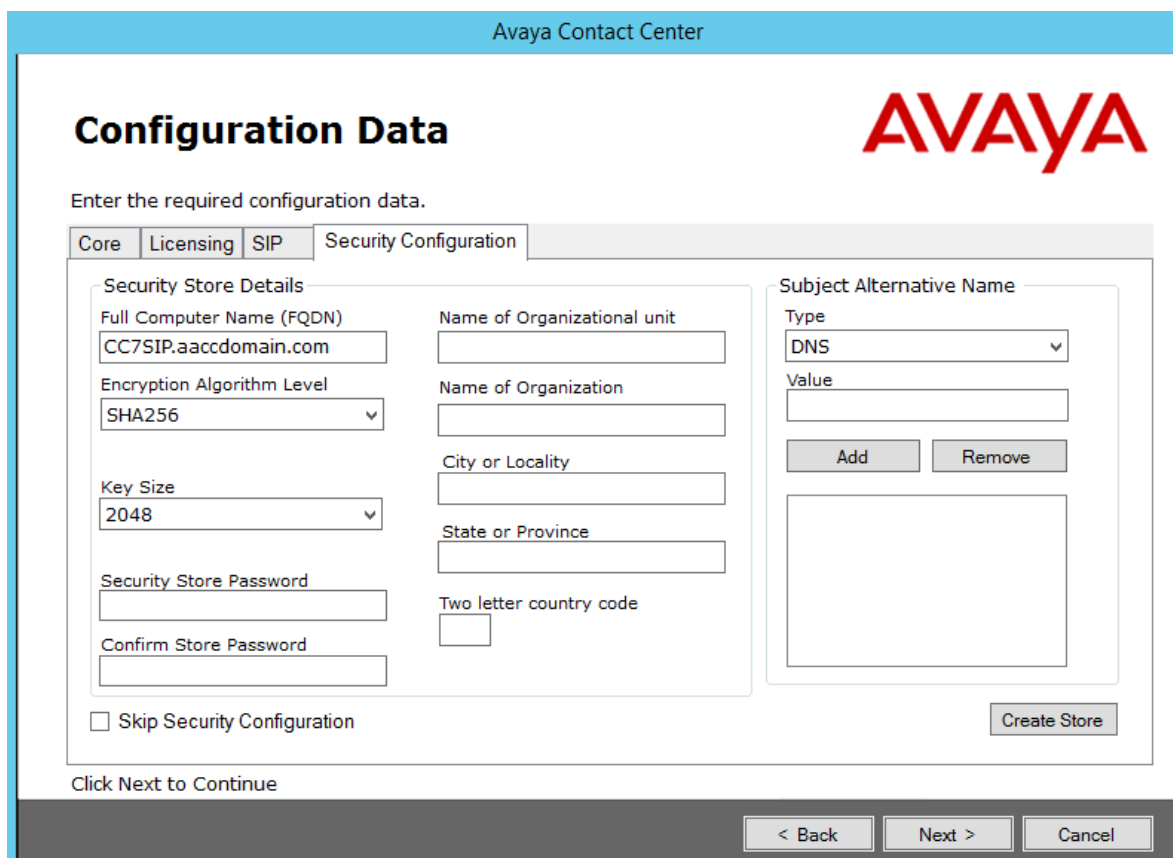
20. In the **SIP CTI Proxy Server** section, in the **IP Address** box, type the IP address for the Avaya Aura® Application Enablement Services server.
21. In the **SIP CTI Proxy Server** section, in the **Port** box, type the SIP CTI Proxy Server port number. The default SIP CTI Proxy Server port is 4723.
22. In the **SIP CTI Proxy Server** section, from the **Transport** list, select the SIP Network Transport CTI communication protocol. The default Avaya Aura® Application Enablement Services communication protocol is TLS.

23. In the **Local SIP Subscriber** section, in the **Domain Name** box, type the SIP domain name for the SIP-enabled contact center. Typically the Avaya Aura® Contact Center SIP Domain Name matches your Active Directory domain name. The Avaya Aura® Contact Center SIP Domain Name matches the Session Manager contact center SIP domain name. The Local SIP Subscriber Domain Name must be different to the XMPP Domain name.
24. If your solution is going to support High Availability, in the **Backup SIP Voice Proxy Server** section, in the **IP Address** box, type the IP address for the second Avaya Aura® Session Manager. You must have a High Availability Standby Server license to support a Backup SIP Voice Proxy Server. If your solution is not going to support High Availability, leave the **Backup SIP Voice Proxy Server** section **IP Address** box empty.
25. In the **Backup SIP Voice Proxy Server** section, in the **Port** box, type the server listening port number. The default port is 5060.
26. In the **Backup SIP Voice Proxy Server** section, from the **Transport** list, select the SIP Network Transport communication protocol. The default is TCP.

 **Note:**

If there are Contact Center agents using SIP deskphones, or if your solution uses Avaya Aura® Presence Services 7.1 or later, you must ensure that the SIP Network Transport communication protocol is set to TLS.

27. In the **SIP IM Proxy Server** section, from the **IM Provider** list, select the Instant Messaging provider. Select Aura Presence Services or, if you are using Microsoft Skype for Business or Microsoft Lync, select Microsoft Lync. The **IM Provider** question is enabled if you select the **Instant Messaging** optional license package on the **Licensing** tab.
28. In the **SIP IM Proxy Server** section, if using an Avaya Aura® Presence Services server, in the **XMPP Domain** box, type the domain name of the Extensible Messaging and Presence Protocol (XMPP) server. The XMPP Domain name must be different to the Local SIP Subscriber Domain Name.
29. In the **SIP IM Proxy Server** section, in the **IP Address** box, type the IP address of the SIP IM Proxy Server.
30. In the **SIP IM Proxy Server** section, in the **Port** box, type the port number for the IM Proxy Server. The default port number for Avaya Aura® Presence Services is 5222. The default port number for Microsoft instant messaging servers is 5060.
31. In the **SIP IM Proxy Server** section, from the **Transport** list, select the SIP IM Proxy Server transport protocol.
32. Select the **Security Configuration** tab, and configure the security details in the **Security Store Details** section.



Avaya Contact Center

Configuration Data

Enter the required configuration data.

Core | Licensing | SIP | **Security Configuration**

Security Store Details

Full Computer Name (FQDN)
CC7SIP.aaccdomain.com

Encryption Algorithm Level
SHA256

Key Size
2048

Security Store Password

Confirm Store Password

☐ Skip Security Configuration

Name of Organizational unit

Name of Organization

City or Locality

State or Province

Two letter country code

Subject Alternative Name

Type
DNS

Value

Add Remove

Create Store

Click Next to Continue

< Back Next > Cancel

33. If you do not want to enable security, select the **Skip Security Configuration** checkbox and skip to [the next steps](#) on page 139.

! Important:

A warning message appears. If you proceed without enabling security, you cannot fully commission your solution. The SIP CTI link is disabled until you configure Contact Center TLS certificates to communicate securely with Application Enablement Services.

34. In the **Full Computer Name (FQDN)** box, type the full FQDN of the server on which you are creating the security store.

! Important:

The FQDN must be the full machine name of the server that the Security Store resides on. The FQDN name is case-sensitive.

35. In the **Name of Organizational unit** box, type the name of the department or division within the company.
36. In the **Name of Organization** box, type the company name.
37. In the **City or Locality** box, type the name of the city or district in which the contact center is located.

38. In the **State or Province** box, type the state or province in which the contact center is located.
39. In the **Two Letter Country Code** box, type the country code in which the contact center is located.
40. In the **Security Store password** box, type a password for accessing the new security store.
41. In the **Confirm Store password** box, confirm the password for accessing the new security store.

 **Important:**

Ensure you remember this password, because you need it when you log on to Security Manager after install. If you forget the password, you cannot access Security Manager.

42. If you are implementing High Availability in the contact center, generate the security store using Subject Alternative Names (SANs). In the **Subject Alternative Name** section, for each SAN you want to add:
 - a. From the **Type** drop-down list, select DNS.
 - b. In the **Value** field, type the FQDN for the server.
 - c. Click **Add**.

For a High Availability system, add the current server FQDN and the Managed name for the HA pair.

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

The default value for **Encryption Algorithm** is SHA256 and the default value for **Key Size** is 2048.

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

44. Click **Create Store**.
45. You can now use the **Security Configuration** tab to create and save a Certificate Signing Request (CSR) file.

The screenshot shows the 'Configuration Data' page for the Avaya Contact Center. The 'Security Configuration' tab is selected. The page title is 'Configuration Data' with the Avaya logo. Below the title, it says 'Enter the required configuration data.' The tabs are 'Core', 'Licensing', 'SIP', and 'Security Configuration'. The main content area has a heading 'Store created – Generate Identity Security Certificate by signing the Certificate Signing Request provided.' Below this, there is a section for 'Certificate Signing Request file' with a 'Create CSR File' button. There is also an 'Add' button and a list for 'Imported Trusted Certificate Authority Root Certificate(s)' with a 'Remove' button. Below that is a section for 'Imported Identity Security Certificate' with a 'Remove' button. On the right, there is a 'Status' panel with instructions: 'Ensure that a removable or network drive is available.', 'Create the Certificate Signing Request file and save it to a removable or network drive.', and 'Alternatively, to defer Security Configuration and continue with the Installation Wizard.' There is a 'Reset' button in the status panel. At the bottom, there is a 'Click Next to Continue' button and navigation buttons: '< Back', 'Next >', and 'Cancel'.

46. Click **Create CSR File**.

47. From the **Save In** drop-down list, select a shared location in which to save the CSR file and click **Save**.

You must now send the Certificate Signing Request file to a Certificate Authority and receive a signed certificate and root certificate to import to the security store.

48. Click **Add** to import certificates. In the **Open** dialog box, navigate to the location of a certificate and click **Open**. To remove the imported certificate, select the required certificate from the list and click **Remove**.

You can import either a chained certificate, or separate root and signed certificates. Root certificates appear in the **Imported Trusted Certificate Authority Root Certificate(s)** section. A signed certificate appears in the **Imported Identity Security Certificate** section.

If a chained certificate contains both root and signed certificates, you can add root certificates and signed certificate simultaneously by importing just one chained certificate.

If a chained certificate contains root certificates only, you can use the chained certificate to add all root certificates at a time. To add a signed certificate, click **Add** and navigate to the required signed certificate.

If you have separate root and signed certificates, you must add them one by one by clicking the **Add** button. Always add a signed certificate last.

 **Important:**

When adding a chained certificate, the system can ask you to enter the password you created for accessing the security store. See [the previous steps](#) on page 137.

49. Click **Next**.
50. Review and verify the summary information, and click **Configure**.
51. After the installation is complete, click **Finish**.
52. If prompted, restart the server.

Installing the Voice Contact Server software for CS1000

Before you begin

- Ensure the Avaya Communication Server 1000 is configured. For more information see *Avaya Aura® Contact Center and Avaya Communication Server 1000 Integration*.
- Download the most recent Contact Center and Common Components patches to the server.
- Read the Contact Center Release Notes for the most recent instructions.

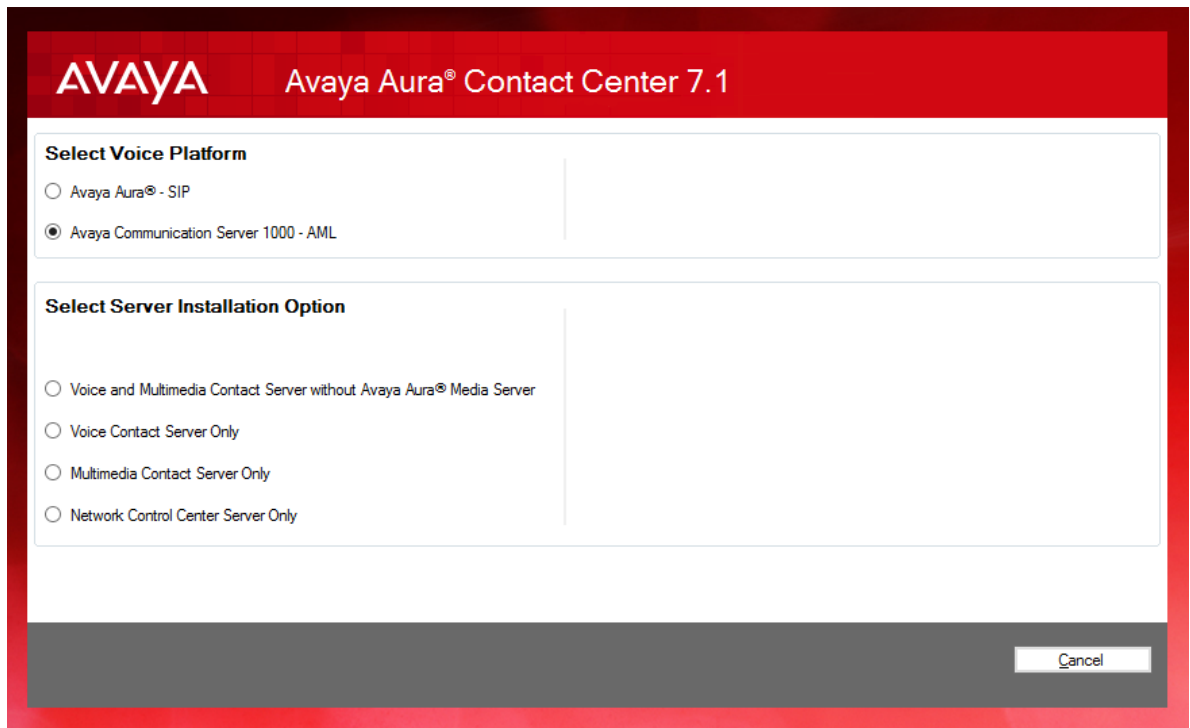
About this task

Install the Contact Center Voice Contact Server software on the server.

Procedure

1. Insert the Contact Center DVD into the DVD drive of your server.
2. If the installation does not automatically start, double-click **Setup.exe**.
3. Click **Accept** to install the Microsoft .NET Framework on the server.
If you are prompted to accept the Microsoft .NET Framework license agreement, click **Accept**. If you are prompted to restart the server, click **Yes** and repeat step 2.
4. Contact Center software installer runs Operating System and hardware checks on the server. If the installer returns a Fail, the software installation cannot proceed until you correct the problem. Review any failures returned by the System Readiness Check and consult *Avaya Aura® Contact Center Overview and Specification* to determine the actions to resolve the issue.

You can ignore warnings if the potential impact to the operation of the contact center is understood and not applicable.
5. The Contact Center software installer platform and server selection screen appears.
6. In the **Select Voice Platform** section, select **Avaya Communication Server 1000 - AML**.



The screenshot shows the Avaya Aura Contact Center 7.1 installation wizard. The title bar is red with the Avaya logo and the text 'Avaya Aura® Contact Center 7.1'. The main content area is white and contains two sections: 'Select Voice Platform' and 'Select Server Installation Option'. In the 'Select Voice Platform' section, the 'Avaya Communication Server 1000 - AML' option is selected with a radio button. In the 'Select Server Installation Option' section, the 'Voice Contact Server Only' option is selected with a radio button. A 'Cancel' button is located in the bottom right corner of the window.

AVAYA Avaya Aura® Contact Center 7.1

Select Voice Platform

☐ Avaya Aura® - SIP

☒ Avaya Communication Server 1000 - AML

Select Server Installation Option

☐ Voice and Multimedia Contact Server without Avaya Aura® Media Server

☐ Voice Contact Server Only

☐ Multimedia Contact Server Only

☐ Network Control Center Server Only

Cancel

7. In the **Select Server Installation Option** section, select **Voice Contact Server Only**.
8. Click **Next**.
9. Under **Journal Database Drive**, select the drive for the database journal. The default drive partition is H:.
10. Under **Voice Contact Server Database Drive**, select the drive for the Contact Center Manager Server, Communication Control Toolkit, and Contact Center Manager Administration databases. The default drive partition is F:.
11. In the **Service Packs** section, browse to and select the Service Pack.



12. Click **Install**.
13. The **AVAYA GLOBAL SOFTWARE LICENSE TERMS** window appears.
14. Read the terms of the license.
 - If you accept the terms, click **I ACCEPT THE LICENSE TERMS**. *The installation continues.*
 - If you do not accept the terms, click **I DECLINE THE LICENSE TERMS**. *The installation returns to the Select Destination Drive screen.* Click **Cancel** to stop the install.
 - To print the license terms, click **Print**.
15. The **MICROSOFT SOFTWARE LICENSE TERMS** window appears.
16. Read the terms of the license.
 - If you accept the terms, click **I ACCEPT THE LICENSE TERMS**. *The installation continues.*
 - If you do not accept the terms, click **I DECLINE THE LICENSE TERMS**. *The installation returns to the Select Destination Drive screen.* Click **Cancel** to stop the install.
 - To print the license terms, click **Print**.

17. The **Progress** window appears and displays the installation progress.
18. When the software is installed, you have the following options.
 - To continue configuring the server installation data:
 - a. Select **Launch Avaya Aura Contact Center Ignition Wizard**.
 - b. Click **Configure**. This starts the Avaya Aura® Contact Center Ignition Wizard.
 - To defer configuring the server installation data:
 - a. Clear **Launch Avaya Aura Contact Center Ignition Wizard**.
 - b. On the message box, click **Yes**.
 - c. On the main installer screen, click **Close**.
 - d. Follow the on-screen instructions and shut down the Contact Center server.

You must use the Ignition Wizard to initialize Avaya Aura® Contact Center, otherwise Avaya Aura® Contact Center is not operational. For more information about the Ignition Wizard, see the following procedures.

Configuring Voice Contact Server software for CS1000

Before you begin

- Ensure the Avaya Communication Server 1000 is configured. For more information see *Avaya Aura® Contact Center and Avaya Communication Server 1000 Integration*.
- You must configure the required language and locale of the Contact Center server operating system, if it is not a Latin-1 language, before configuring the Contact Center server using the Contact Center Ignition Wizard. For more information about configuring language and locale settings on the Contact Center server, see *Avaya Aura® Contact Center Server Administration*.
- Download the most recent Contact Center and Common Components patches to the server.
- Read the Contact Center Release Notes for the most recent instructions.

About this task

Configure the Contact Center Voice Contact Server software and enable your contact center to route contacts to the agents that can answer the call with the correct skills.

Procedure

1. Log on to the Contact Center server using the Administrator account details.
2. On the Contact Center Ignition Wizard screen, click **Next**. If the Contact Center Ignition Wizard is not visible, click the Ignition Wizard shortcut on the desktop.
3. On the **End-User License Agreement** screen, read the license agreement. Optionally, click **Print** to generate a local soft copy (in OpenXPS Document format) of the license agreement.

4. Select **I Accept the Terms of the End-User License Agreement** and click **Next**.
5. On the **Configuration Data** window, type the configuration details for each tab.
6. Select the **Core** tab, and configure the server details.

The screenshot shows the 'Configuration Data' window for the Avaya Contact Center. The 'Core' tab is selected, and the 'CS1000' sub-tab is active. The window contains several input fields for configuration data. The 'Site Name' field is pre-filled with 'CC7SIP'. The 'Real-Time Statistics Multicast IP Address' field is pre-filled with '234.5.6.10'. The 'Network Configuration' section has two empty fields for 'CLAN IP Address' and 'ELAN IP Address'. The 'System Account Configuration' section has two empty fields for 'Password' and 'Confirm Password'. The Avaya logo is in the top right corner. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'. A message at the bottom left says 'Click Next to Continue'.

7. In the **Site Name** box, type the site name for the Contact Center server. The site name must not contain spaces or non-alphabetical characters except hyphen (-) and underscore (_). The first character must be a letter. The site name must be unique and can consist of 6 to 15 characters.
8. In the **Real-Time Statistics Multicast IP Address** box, type the Real-time Statistics Multicast IP Address of the server to associate with sending real-time data. The **IP Address** must be from 224.0.1.0 to 239.255.255.255. The default is 234.5.6.10.
9. In the **Network Configuration** section, in the **ELAN P Address** box, type the IP Address of the embedded local area network. The embedded local area network (ELAN) is a dedicated Ethernet LAN that connects Contact Center to the PABX.
10. In the **CLAN IP Address** box, type the IP Address of the Contact Center server. This is the Contact Center server IP address on the subnet that connects to the other servers and agent client computers in the contact center solution.
11. In the **System Account Configuration** section, in the **Password** box, type a password for the Contact Center administration account. The password is checked against the server

security policy for minimum password requirements. Avaya recommends that you enter a password that conforms to your corporate password policy.

12. In the **Confirm Password** box, type the password.
13. Select the **Licensing** tab, and configure the licensing details.
14. From the **License Type** list, select **Standard KRS**.
15. Click **Browse** to locate and load your license file.
16. From the **Licensing Package** list, select the license type that you have purchased. Select **Nodal Enterprise** for single-site contact centers.
17. From the list of **Optional Packages**, enable the licensed features that you have purchased.
18. Select the **Open Queue** check box.
19. Select the **CS1000** tab.

The screenshot shows the 'Configuration Data' window for the Avaya Contact Center. The 'CS1000' tab is selected. The window is divided into two main sections: 'CS1000 Switch Data' and 'Voice Services Setup'.

CS1000 Switch Data:

- Switch Name: [Text Box]
- Switch IP Address: [Text Box]
- Switch Customer Number: [Text Box]
- Switch Serial Number: [Text Box]
- Alternative Switch IP Address: [Text Box]
- Alternative Switch Customer Number: [Text Box]
- Alternative Switch Serial Number: [Text Box]

Voice Services Setup:

- Voice Connection Type:**
 - ☒ None
 - ☐ Avaya Aura Experience Portal
 - ☐ CallPilot
- CallPilot Configuration:**
 - ELAN IP Address: [Text Box] Port: [Text Box]
 - CPHA Managed CLAN IP Address: [Text Box]
 - CLAN IP Address: [Text Box]

At the bottom, there is a 'Click Next to Continue' instruction and three buttons: '< Back', 'Next >', and 'Cancel'.

20. In the **Switch Name** box, type the name of the AML Avaya Communication Server 1000 telephone switch. Valid characters for Avaya Communication Server 1000 names are A–Z, a–z, 0–9, underscore (_), and period (.). Names must begin with an alphabetical character and cannot contain spaces. The last character must not be an underscore or a period. Names must not exceed 80 characters in length.

21. In the **Switch IP Address** box, type the IP address of the Avaya Communication Server 1000.
22. In the **Switch Customer Number** box, type the customer number for the Avaya Communication Server 1000.
23. In the **Alternative Switch IP Address** box, type the IP address of an alternate Avaya Communication Server 1000, if you have one.
24. In the **Alternative Switch Customer Number** box, type the customer number of the alternate Avaya Communication Server 1000, if you have one.
25. In the **Alternative Switch Serial ID** box, type the serial number of the alternate Avaya Communication Server 1000, if you have one.
26. In the **Voice Connection Type** section, select the method used to connect to the PABX. Select **None**, **Avaya Aura Experience Portal**, or **CallPilot**.
27. If you are using an Avaya CallPilot® server, enter the Avaya CallPilot® server **ELAN IP Address** and then configure the **Port** to 10008.
28. If you are using Avaya CallPilot® High Availability, in the **CPHA Managed CLAN IP Address** box, type the Avaya CallPilot® Managed CLAN IP address.
29. If you are using an Avaya CallPilot® server, in the **CLAN IP Address** box, type the CLAN IP address of the Avaya CallPilot® server.
30. Select the **Security Configuration** tab, and configure the security details in the **Security Store Details** section.

Avaya Contact Center

Configuration Data

Enter the required configuration data.

Core
Licensing
CS1000
Security Configuration

Security Store Details

Full Computer Name (FQDN)

Encryption Algorithm Level

Key Size

Security Store Password

Confirm Store Password

Name of Organizational unit

Name of Organization

City or Locality

State or Province

Two letter country code

☐ Skip Security Configuration

Subject Alternative Name

Type

Value

Click Next to Continue

31. If you do not want to enable security, select the **Skip Security Configuration** checkbox and skip to [the next steps](#) on page 149.

! Important:

A warning message appears.

32. In the **Full Computer Name (FQDN)** box, type the full FQDN of the server on which you are creating the security store.

! Important:

The FQDN must be the full machine name of the server that the Security Store resides on. The FQDN name is case-sensitive.

33. In the **Name of Organizational unit** box, type the name of the department or division within the company.
34. In the **Name of Organization** box, type the company name.
35. In the **City or Locality** box, type the name of the city or district in which the contact center is located.
36. In the **State or Province** box, type the state or province in which the contact center is located.

37. In the **Two Letter Country Code** box, type the country code in which the contact center is located.
38. In the **Security Store password** box, type a password for accessing the new security store.
39. In the **Confirm Store password** box, confirm the password for accessing the new security store.

 **Important:**

Ensure you remember this password, because you need it when you log on to Security Manager after install. If you forget the password, you cannot access Security Manager.

40. If you are implementing High Availability in the contact center, generate the security store using Subject Alternative Names (SANs). In the **Subject Alternative Name** section, for each SAN you want to add:
 - a. From the **Type** drop-down list, select DNS.
 - b. In the **Value** field, type the FQDN for the server.
 - c. Click **Add**.

For a High Availability system, add the current server FQDN and the Managed name for the HA pair.

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

The default value for **Encryption Algorithm** is SHA256 and the default value for **Key Size** is 2048.

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

42. Click **Create Store**.
43. You can now use the **Security Configuration** tab to create and save a Certificate Signing Request (CSR) file.

The screenshot shows the 'Configuration Data' window for 'Avaya Contact Center'. The 'Security Configuration' tab is selected. The window title is 'Avaya Contact Center'. The main heading is 'Configuration Data'. Below it, it says 'Enter the required configuration data.' The tabs are 'Core', 'Licensing', 'CS1000', and 'Security Configuration'. The main content area has a section titled 'Store created – Generate Identity Security Certificate by signing the Certificate Signing Request provided.' It contains a 'Certificate Signing Request file' section with a 'Create CSR File' button. Below that is an 'Add' button and a section titled 'Imported Trusted Certificate Authority Root Certificate(s)' with a 'Remove' button. There is also a section for 'Imported Identity Security Certificate' with a 'Remove' button. On the right, there is a 'Status' section with instructions: 'Ensure that a removable or network drive is available.', 'Create the Certificate Signing Request file and save it to a removable or network drive.', and 'Alternatively, to defer Security Configuration and continue with the Installation Wizard.' There is a 'Reset' button. At the bottom, there is a 'Click Next to Continue' button and navigation buttons: '< Back', 'Next >', and 'Cancel'.

44. Click **Create CSR File**.

45. From the **Save In** drop-down list, select a shared location in which to save the CSR file and click **Save**.

You must now send the Certificate Signing Request file to a Certificate Authority and receive a signed certificate and root certificate to import to the security store.

46. Click **Add** to import certificates. In the **Open** dialog box, navigate to the location of a certificate and click **Open**. To remove the imported certificate, select the required certificate from the list and click **Remove**.

You can import either a chained certificate, or separate root and signed certificates. Root certificates appear in the **Imported Trusted Certificate Authority Root Certificate(s)** section. A signed certificate appears in the **Imported Identity Security Certificate** section.

If a chained certificate contains both root and signed certificates, you can add root certificates and signed certificate simultaneously by importing just one chained certificate.

If a chained certificate contains root certificates only, you can use the chained certificate to add all root certificates at a time. To add a signed certificate, click **Add** and navigate to the required signed certificate.

If you have separate root and signed certificates, you must add them one by one by clicking the **Add** button. Always add a signed certificate last.

! Important:

When adding a chained certificate, the system can ask you to enter the password you created for accessing the security store. See [the previous steps](#) on page 147.

47. Click **Next**.
48. Review and verify the summary information, and click **Configure**.
49. After the installation is complete, click **Finish**.
50. If prompted, restart the server.

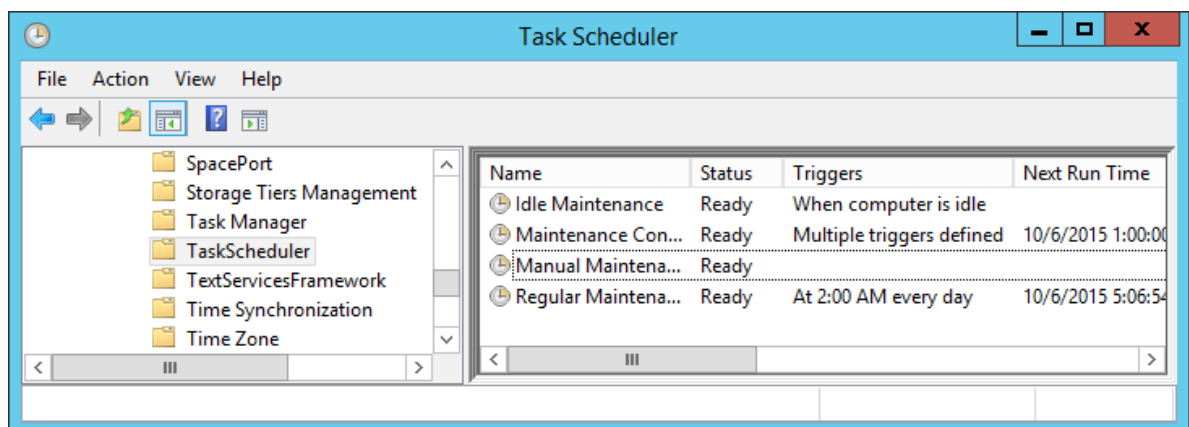
Enabling Windows Server Automatic Maintenance

About this task

Enable Windows Server Automatic Maintenance after deploying Contact Center software.

Procedure

1. Log on to the Contact Center server as an administrator.
2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Enable**.
5. In the **Name** column, right-click **Regular Maintenance** and then click **Enable**.



6. From the **File** menu, click **Exit**.

Backing up the new Avaya Aura® Contact Center Release 7.1 databases

About this task

After running the Ignition Wizard, backup the Avaya Aura® Contact Center Release 7.1 databases.

The backup databases capture the system in a known clean state and these might be required later if issues arise during data migration.

Procedure

1. Log on to the new Avaya Aura® Contact Center Release 7.1 server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
4. In the right pane, click **Create**.
5. From the **Drive Letter** list, select the network drive on which to store the databases.
6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.
7. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the user password.
9. Click **Save**.
10. Click **OK**.
11. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
12. In the **Media Type** section, select **Network Location**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.
15. Click **Yes**, to continue with the backup.

Restoring the Database Integration Service configuration

About this task

If you backed up the Database Integration Service configuration on your old server, restore the configuration to the registry on the new server. Contact Center automatically copies the configuration from the registry into the database on the next restart.

Procedure

1. On the Contact Center server, on the **Desktop** screen, right-click **Start** and select **Run**.
2. Type `regedit`.
3. Click **OK**.
4. On the **Registry Editor** dialog box, click **File** > **Import**.
5. On the **Import Registry File** dialog box, select the HAI configuration file that you saved from the old server.
6. Click **Open**.
7. On the **Registry Editor** message box, click **OK**.

Next steps

If you used custom DSNs in the Database Integration Service configuration on your old server, you must manually re-configure these DSNs on the new server.

Restoring the Voice Contact Server Release 7.1 databases

Before you begin

- Back up the old Voice Contact Server databases.
- On the new server, map a drive to the Voice Contact Server database backups.

Important:

When you migrate configuration information from the old server to the new server, do not run the two application servers simultaneously. Both applications are configured the same, so they attempt to access and control the same resources. Continuing to run the old applications in the Contact Center can result in unpredictable behavior.

About this task

Restore the Voice Contact Server Release 7.1 databases. After you complete this procedure, you must restart your server.

Important:

You must complete this procedure to ensure all databases are restored at the same time.

Procedure

1. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
2. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the Backup Locations pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which you stored the Voice Contact Server database backup.

5. In the **UNC Path** box, type the location of the Voice Contact Server databases in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.
9. Click **OK**.
10. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Restore**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Application** section, select **CCT**, **CCMS**, **ADMIN**, and **CCMA**.
13. In the **Restore contents** section, select **Data**.
14. From the **Backup Location** list, select the network drive containing the backed up Contact Center server databases.
15. Click **Restore**.
16. Click **Yes**.
17. Use the **Progress information** field to monitor the progress of the restoration.
18. On the **Database Maintenance** message box, click **OK**.
Wait for the restore to complete.
19. From the **Start** menu, in the Avaya area, click **Server Configuration**.
20. In the Server Configuration dialog box, click **Apply All**.
21. Click **Yes** to restart Contact Center.

 **Important:**

If you have a Hot-standby (AML) High Availability solution, ensure CCMS service monitoring in the High Availability utility on the active server is disabled before you restart the server. Re-enable service monitoring on the active server only after all CCMS services have fully started.

Restoring the Voice Contact Server databases

Before you begin

- Back up the old Voice Contact Server databases.
- On the new server, map a drive to the CCMS and CCT database backups.

 **Important:**

When you migrate configuration information from the old server to the new server, do not run the two application servers simultaneously. Both applications are configured the same, so they attempt to access and control the same resources. Continuing to run the old applications in the Contact Center can result in unpredictable behavior.

About this task

Restore the CCMS and CCT databases to the new server. The Database Maintenance utility can restore all application databases at one time. You must restore the data for the databases as a matched set, and all databases must be stored in the same backup location.

Procedure

1. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
2. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the Backup Locations pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which you stored the Voice Contact Server database backup.
5. In the **UNC Path** box, type the location of the Voice Contact Server database in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.
9. Click **OK**.
10. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Restore**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Application** section, select **CCT** and **CCMS**.
13. In the **Restore contents** section, select **Data**.
14. From the **Backup Location** list, select the network drive containing the backed up Voice Contact Server databases.
15. Click **Restore**.
16. Click **Yes**.
17. Use the **Progress information** field to monitor the progress of the restoration.
18. On the **Database Maintenance** message box, click **OK**.
19. From the **Start** menu, in the Avaya area, click **Server Configuration**.
20. In the **Server Configuration** dialog box, click **Apply All**.

21. Click **Yes** to restart Contact Center.

Restoring Contact Center Manager Administration data

Before you begin

- Know the network location (in Universal Naming Convention (UNC) format) of the drive for the backed up data.

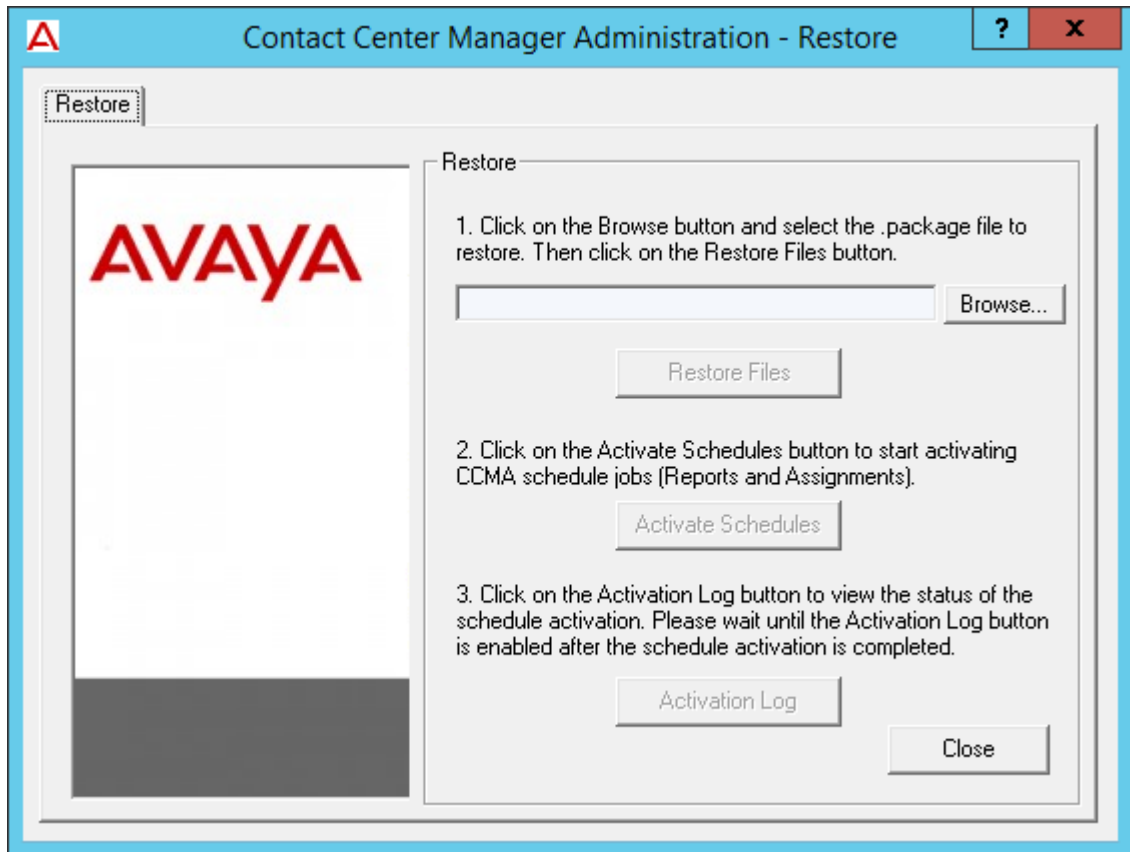
About this task

Restore the Contact Center Manager Administration data to migrate the data to the new server. Use this procedure if you are restoring Avaya Aura® Contact Center Contact Center Manager Administration data. You must restore the CCMA database as part of a matched set; the CCMA data must be restored to the same server as its corresponding databases (for example, CCMS, CCT, or CCMM).

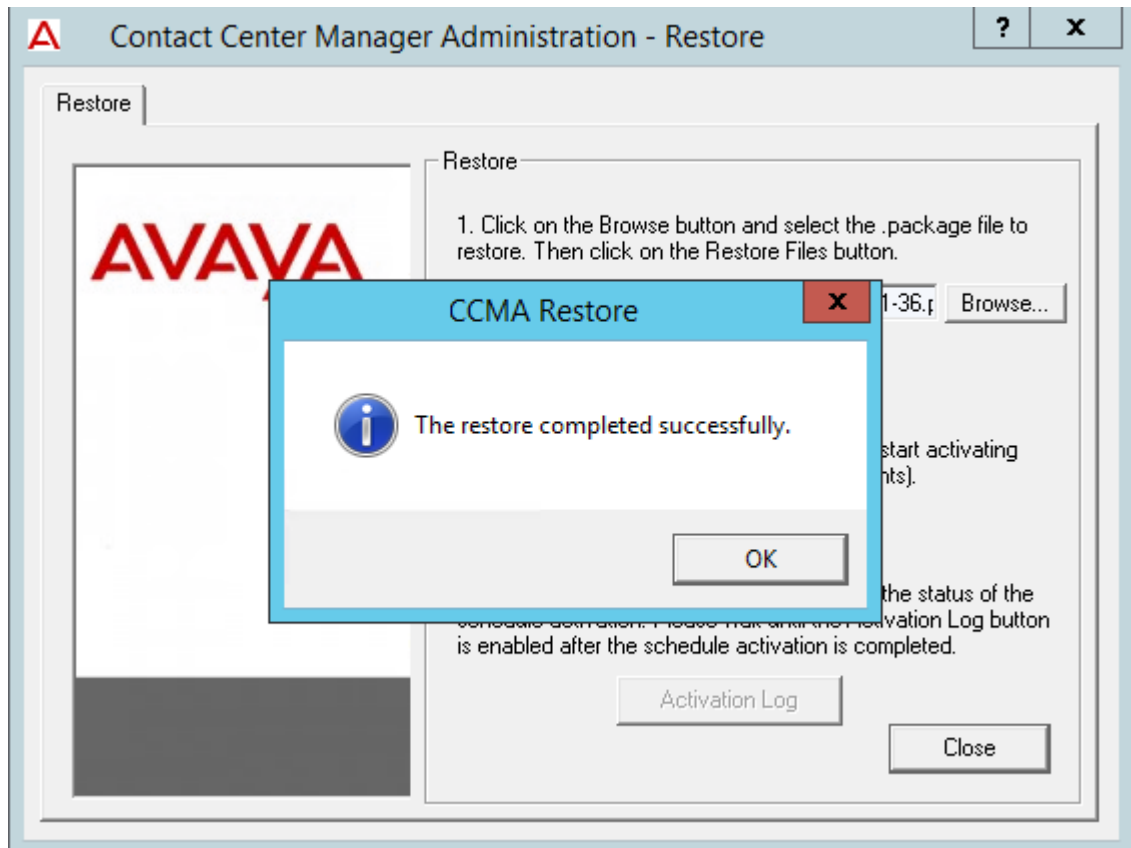
Procedure

1. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.
2. In the left pane of the Avaya Configuration window, expand **Avaya > Applications > Restore**.
3. In the right pane, click **Restore**.
4. On the **Restore** message box, click **OK**.

5. In the **Contact Center Manager Administration - Restore** dialog box, click the **Restore** tab.



6. To select a backup file to restore from, click **Browse**.
 7. In the **Select a backup file** dialog box, select the required .package file.
 8. Click **Open**.
 9. To restore the backup file data onto the administration data server, click **Restore Files**.
- The restore completed successfully message box appears.



10. Click **OK**.

Upgrading the Contact Center Manager Administration data

Before you begin

- Restore the backed up Contact Center Manager Administration (CCMA) data.

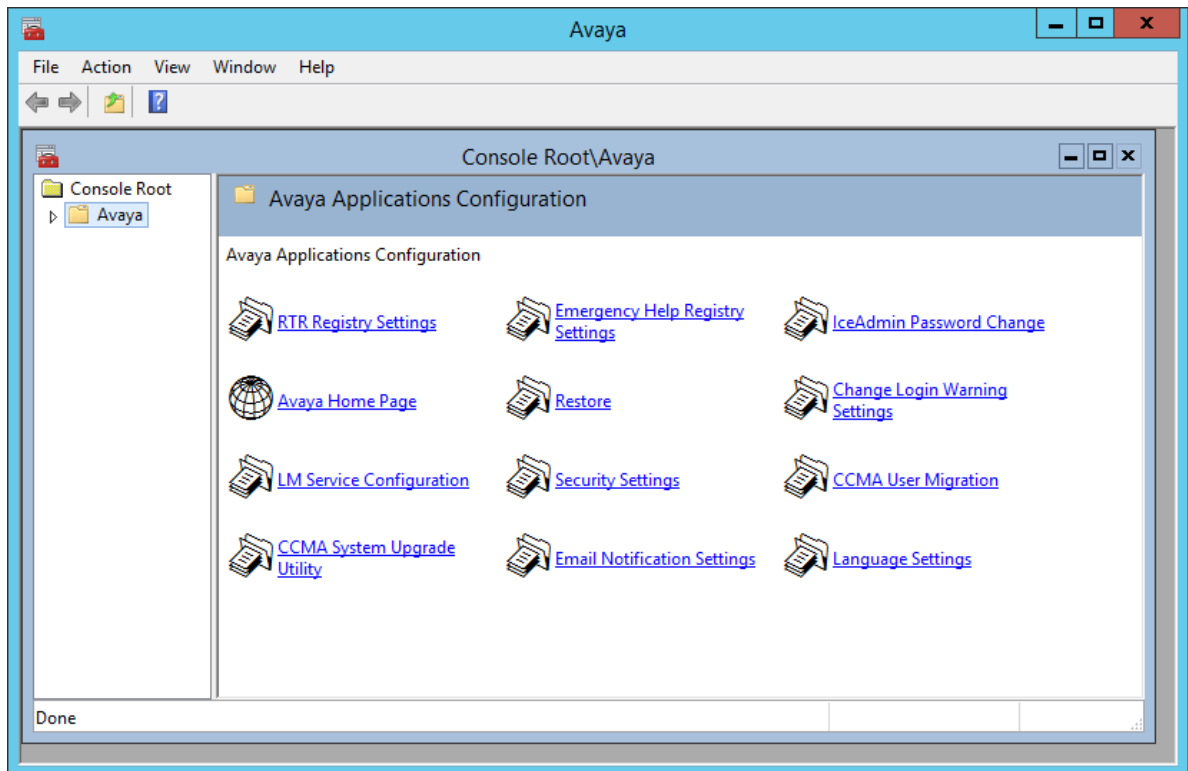
About this task

Upgrade Contact Center Manager Administration (CCMA) data to the Intersystems Caché database format used by Avaya Aura® Contact Center Release 7.1.

Procedure

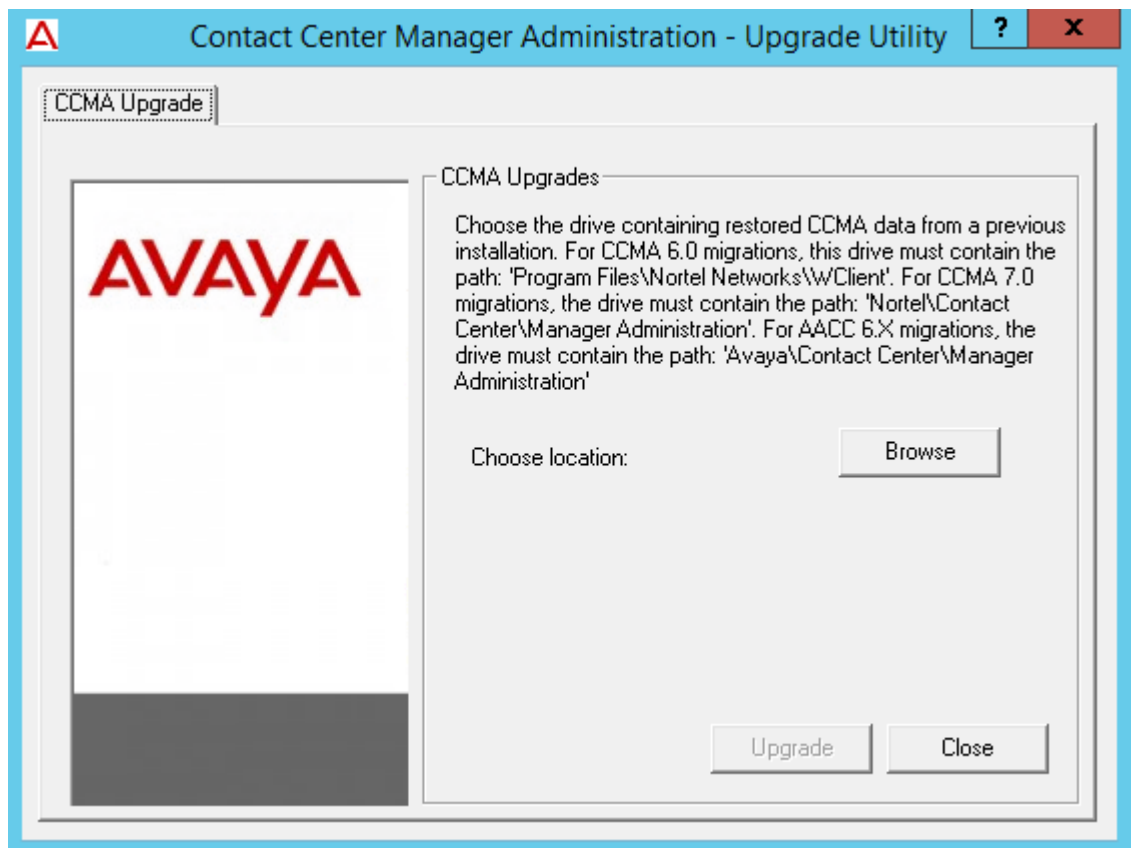
1. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.

2. In the left pane, click **Avaya** > **Applications** > **CCMA System Upgrade Utility**.



3. In the right pane, click **CCMA System Upgrade Utility**.

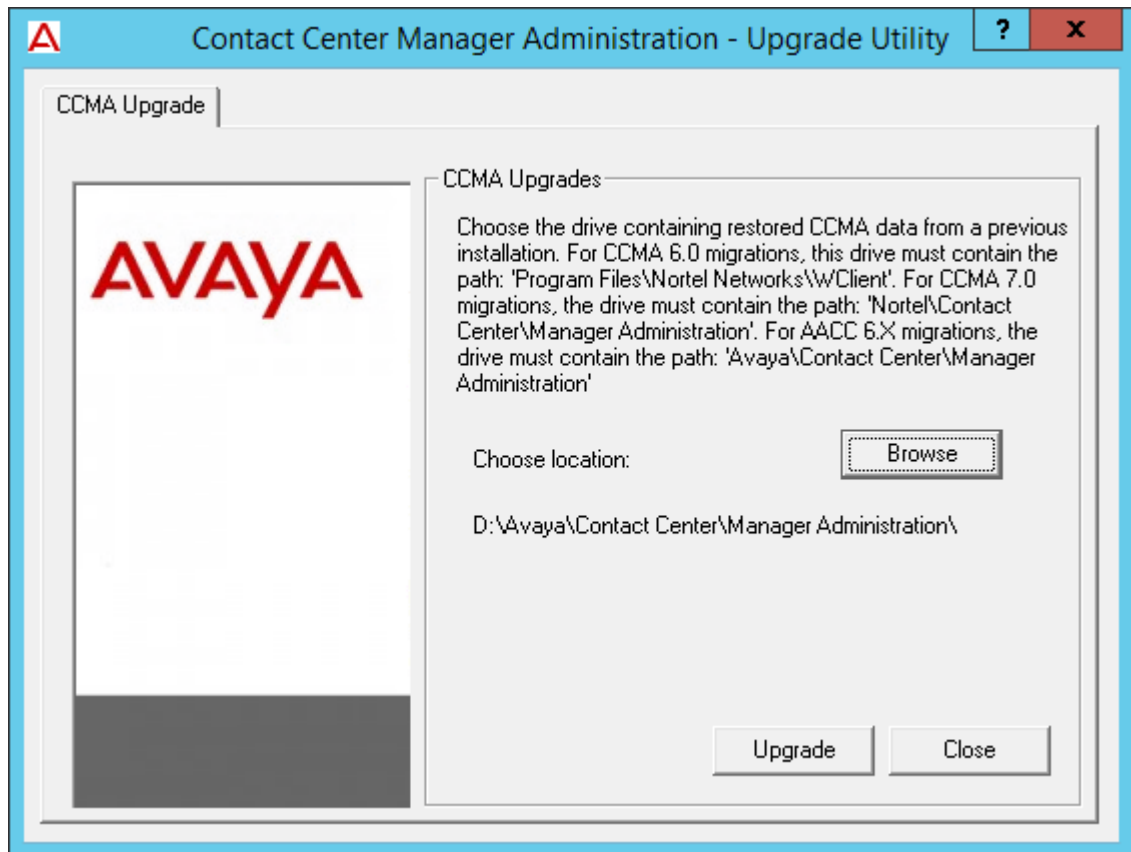
4. Click **Yes** on the confirmation dialog box.



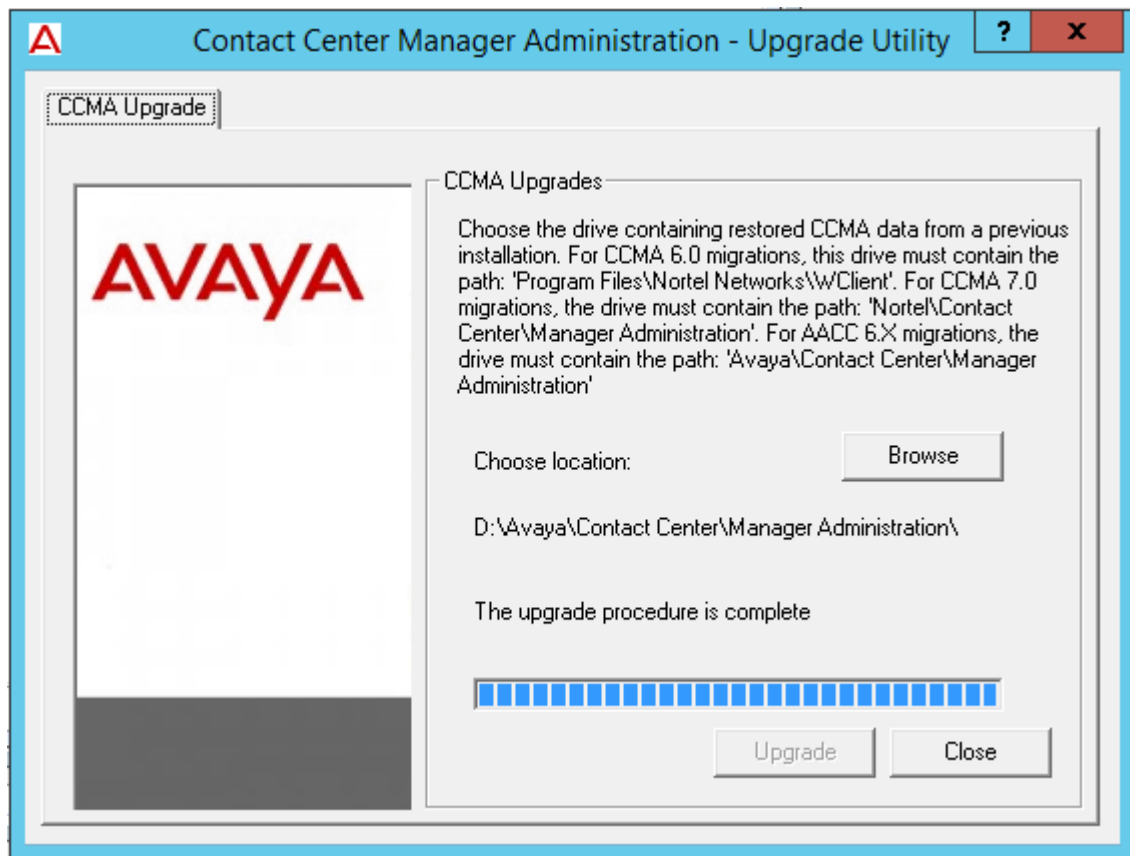
5. On the Upgrade Utility, click **Browse** and follow the instructions on the **CCMA Upgrades** screen to choose a location.

Select only the drive letter as the location of the restored CCMA data. The upgrade utility automatically detects and appends the correct directory structure for the old system data.

Example of upgrading from an Avaya Aura® Contact Center Release 6.4 system:



6. Click **Upgrade**.



7. Close the Upgrade Utility application. Click **Close**.

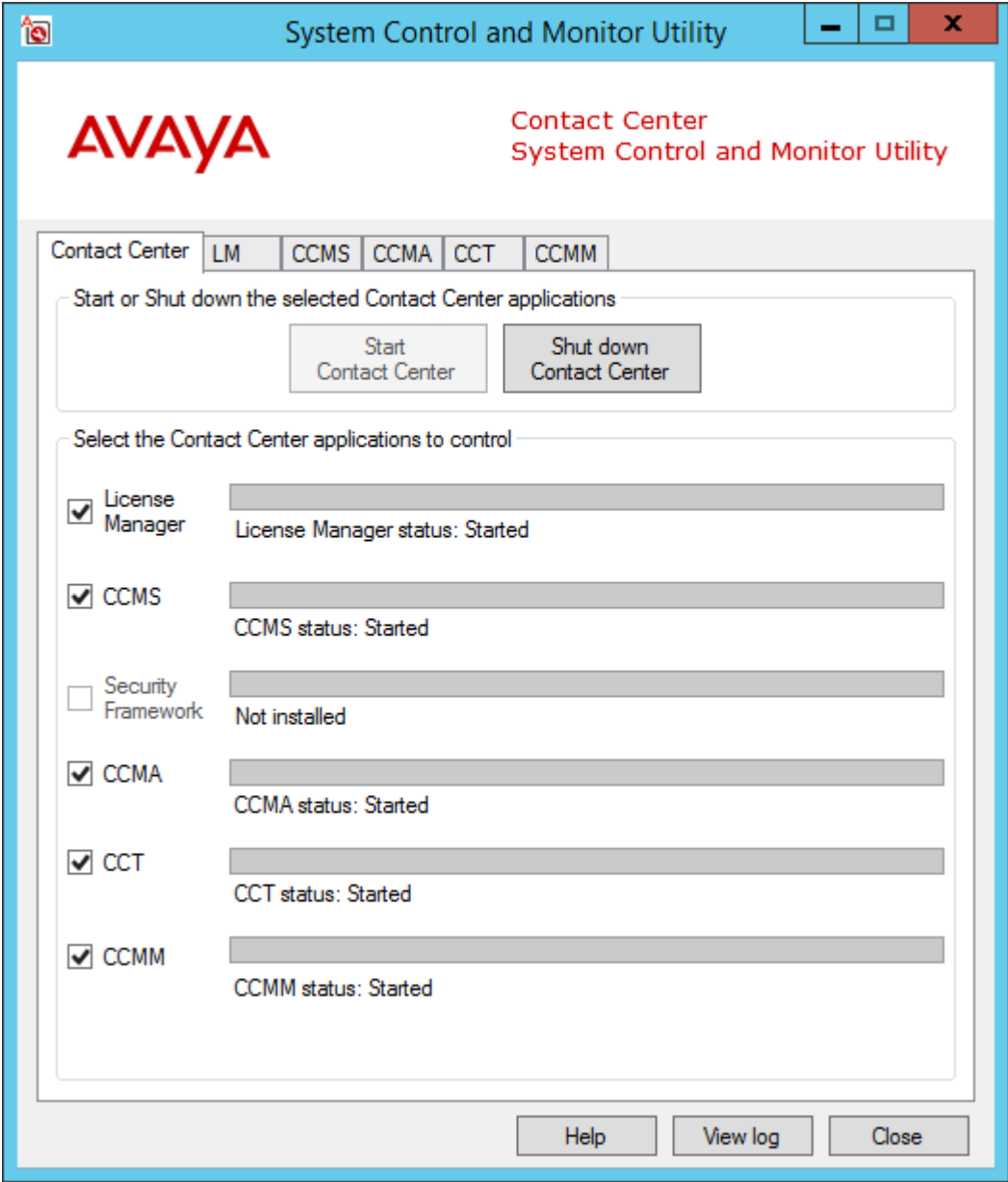
Starting Contact Center services

About this task

Start the Contact Center services to begin re-configuration after migrating or upgrading a system. The database restore and upgrade utilities automatically stop Contact Center services. Start Contact Center services to continue commissioning the solution.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **System Control and Monitor Utility**.
3. Click the **Contact Center** tab.
4. Click **Start Contact Center**.



Wait for Contact Center services to start.

Configuring the Contact Center Manager Administration system components

About this task

Configure the Contact Center Manager Administration (CCMA) system components for the new solution. Ensure the Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), and Contact Center Multimedia (CCMM) settings are correct for the new solution.

To access CCMA and other Contact Center components, you must use the Microsoft Edge browser in Internet Explorer mode.

Procedure

1. In your browser, type the URL of the server and then press **Enter**.

The default URL is `https://<server name>`, where `<server name>` is the host name of the Avaya Aura® Contact Center Release 7.1.x server. If you turned off Web Services security, use `http://<server name>`.

2. On the main login page, in the **User ID** field, type the username.

The default user ID is `webadmin`.

3. In the **Password** box, type the password.

The default password is `webadmin`.

4. Click **Log In**.

5. On the launchpad, click **Configuration**.

6. In the left pane, right-click the CCMS server name and then click **Edit Properties**.

7. Update the Contact Center Manager Server details to match your new solution and then click **Submit**.

8. In the left pane, right-click the CCMS server name and then click **Refresh Server**.

9. On both Contact Center Manager Administration dialogs, click **Yes**.

10. In the left pane, right-click **CCT** and then click **Edit Properties**.

11. Update the Communication Control Toolkit details to match your new solution and then click **Submit**.

12. In the left pane, right-click **CCMM** and then click **Edit Properties**.

13. Update the Contact Center Multimedia details to match your new solution and then click **Submit**.

14. Log off from CCMA.

15. Using the System Control and Monitor Utility (SCMU), restart Avaya Aura® Contact Center services.

Converting custom RCW reports to Contact Center R7.1 format

About this task

Copy the zip file of converted RCW reports to the Contact Center R7.1 server, and convert each report to SSRS format.

Before you begin

Prepare the RCW reports for migration on the old server, and copy them to a network location.

Custom formulas do not migrate to the new server. If the original reports use custom formulas on the existing server, the formulas do not migrate with the custom reports.

Contact Center creates a placeholder formula for each custom formula. The placeholder displays an asterisk character on the migrated report. If possible, the placeholder formula includes the original Crystal Syntax formula text as a comment. You must edit the placeholder formulas, entering valid SSRS expressions for the formula text, to complete the migration. The placeholder formula is limited to 32,000 characters, so it is possible that very long formulas can be truncated.

Document all the custom formulas on the existing server, to assist with re-creating them on the new server after migrating the Contact Center databases.

Procedure

1. Log on to the Contact Center R7.1 server.
2. Run the RCW report utility `d:\avaya\contact center\manager administration\server\bin\MigrationRCWImporter.exe`
3. On the RCW Importer screen, click **Browse**, and browse to and select the zip file of converted RCW reports.
4. Click **Run** to start the conversion.
The RCW Importer utility unpacks the reports to the RCW\Private folder.
5. Log on to Contact Center Manager Administration.
6. On the **Launchpad**, click **Historical Reporting**.
7. In the left pane, click the Contact Center Manager Server.
8. From the **Report** menu, select **Report Creation Wizard**.
9. Select **Open Existing Report**.
10. For each `.rcwx` report in the list:
 - a. Select the report and click **Next**.
Contact Center opens the report in RCW.
 - b. Click the **Preview Report** button.
 - c. On the Preview Data Filter screen, click **Preview**.
Check that the report opens correctly in the preview.

- d. If you saw errors in the preview, correct the data fields and formulas as applicable.
- e. Click the **Save Report** button.
- f. On the Save RCW Report window, click **Save**.

Do not change the default file location: the .rdl file must save in the same location as the .rcwx file.

Contact Center saves the report in .rdl format.

Commissioning the Contact Center solution

About this task

Commission the Contact Center solution.

Procedure

1. After migrating your server and restoring the server databases, some of the old configuration settings might not match your new solution. Commission your new server in the new solution. For more information, refer to *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000* or *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications*.
2. Use the procedures in *Avaya Aura® Contact Center Server Administration* to configure your licensed features.

Chapter 8: Voice Contact Server patch installation

This chapter describes how to install Avaya Aura® Contact Center patches on the Voice Contact Server. Apply patches to a Voice Contact Server to resolve product issues. When installing software patches, follow the instructions in the Avaya Aura® Contact Center patch Release Notes.

A Voice Contact Server includes the following server software:

- Contact Center Manager Server (CCMS)
- Contact Center Manager Server Utility
- Contact Center License Manager (LM)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)

If your Avaya Aura® Contact Center is licensed for Standby Servers, you can hot patch your software to minimize down time. You must ensure that you patch both the active and standby servers to the same patch level. For information about hot patching, see [Common procedures](#) on page 353.

Voice Contact Server patch installation prerequisites

- Download the most recent documentation. See [Downloading the most recent documentation](#) on page 45.
- Download and review the latest Avaya Aura® Contact Center Release Notes. The Release Notes contain information about known issues, patches, and workarounds specific to a release and patch line-up of Contact Center. For more information about the Contact Center Release Notes, see the Avaya website (<http://support.avaya.com>).

Disabling Windows Server Automatic Maintenance

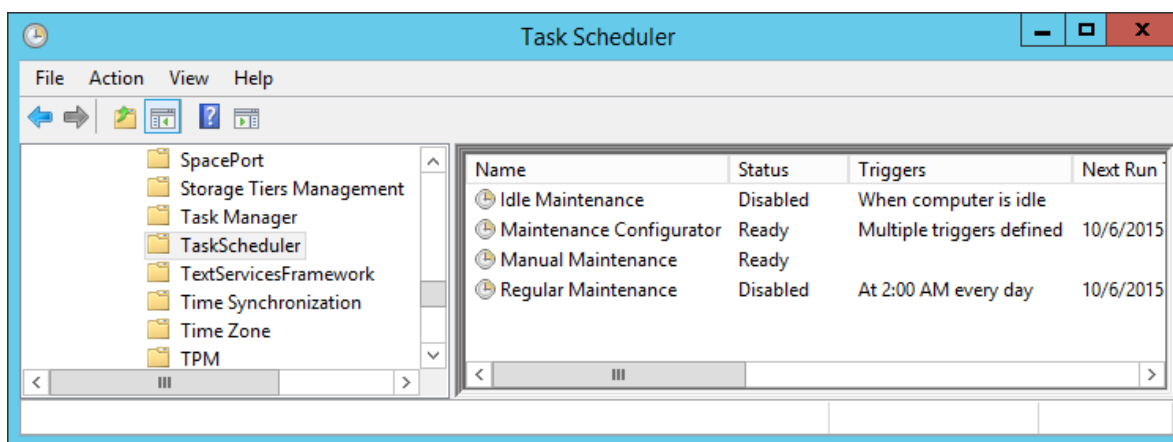
About this task

Disable Windows Server Automatic Maintenance while updating Contact Center software. Windows Server Automatic Maintenance can occasionally interfere with the real-time

requirements for Contact Center. You must therefore temporarily disable Automatic Maintenance to update Contact Center software. Re-enable it after the update.

Procedure

1. Log on to the Contact Center server as an administrator.
2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Disable**.
5. In the **Name** column, right-click **Regular Maintenance** and then click **Disable**.



6. From the **File** menu, click **Exit**.

Installing Voice Contact Server Release Packs, Feature Packs and Service Packs

Before you begin

- Download the most recent Contact Center Release Pack, Feature Pack and Service Packs.
- Download the most recent Contact Center software patches.
- Back up the Contact Center databases.
- Temporarily stop Microsoft Windows Server Automatic Maintenance while you update Voice and Multimedia Contact Server software.
- Avoid installation from shared locations, because it might lead to installation failure. To ensure successful installation, mount the Release Bundle or install it locally.
- If you deploy in a virtual environment and want to install Avaya Workspaces, you must manually deploy three virtual machines using the Avaya Workspaces Open Virtual Appliance (OVA). See [Deploying the Avaya Workspaces OVA](#) on page 177.

About this task

Install the most recent Voice Contact Server Release Packs, Feature Packs and Service Packs to take advantage of new features, and to ensure that you have the most current application updates.

Procedure

1. Open the Release Pack, Feature Pack or Service Pack ZIP file.
2. Browse to the Avaya Release Pack Installer directory.
3. Double-click `setup.exe`.

Contact Center displays the Contact Center Release Pack Installer screen.

4. If you downloaded GA patches along with the Release Pack:
 - a. Select **Yes**.
 - b. Click **Browse**.
 - c. On the Browse for Folder screen, browse to the folder where you downloaded the patches, and click **OK**.
5. On the Contact Center Release Pack Installer screen, click **Next**.
6. On the Avaya Global License Terms screen, click **I ACCEPT THE LICENSE TERMS**.
7. On the MICROSOFT SOFTWARE LICENSE TERMS screen, click **I ACCEPT THE LICENSE TERMS**.

The Avaya Release Pack Installer shuts down Contact Center and installs the Release Pack, Feature Pack or Service Pack.

8. When the software update completes successfully, click **Restart**.

Contact Center reboots the server.

Installing Voice Contact Server software patches

Before you begin

- Download the most recent Contact Center Voice Contact Server patches.
- Ensure that you have a recent backup of the Contact Center databases. Avaya recommends that you schedule a daily backup of the Contact Center databases at an off peak time. For more information on scheduling backups, see *Maintaining Avaya Aura® Contact Center*.
- Temporarily stop Microsoft Windows Server Automatic Maintenance while you update Voice Contact Server software.

About this task

Install the most recent Voice Contact Server software patches to ensure that you have the most current application updates.

Procedure

1. From the **Start** menu, in the Avaya area, click **Update Manager**.
2. Click **Install**.
3. Click **Browse** and navigate to the folder where you downloaded the patches.
4. Click **Scan for Patches**.

The Contact Center Updates section displays the available patches.

5. Select the appropriate patches.
6. Click **Install Patch(es)**.

The Update Manager installs the patch and displays a confirmation message.

7. Click **Close**.
8. Verify that the newly installed patch appears under **Installed Updates**.
9. If the System Management and Monitoring Component (SMMC) is installed on the server, verify that it starts. For more information about starting SMMC, see [Starting SMMC](#) on page 358.

Next steps

Re-enable Microsoft Windows Server Automatic Maintenance.

Enabling Windows Server Automatic Maintenance

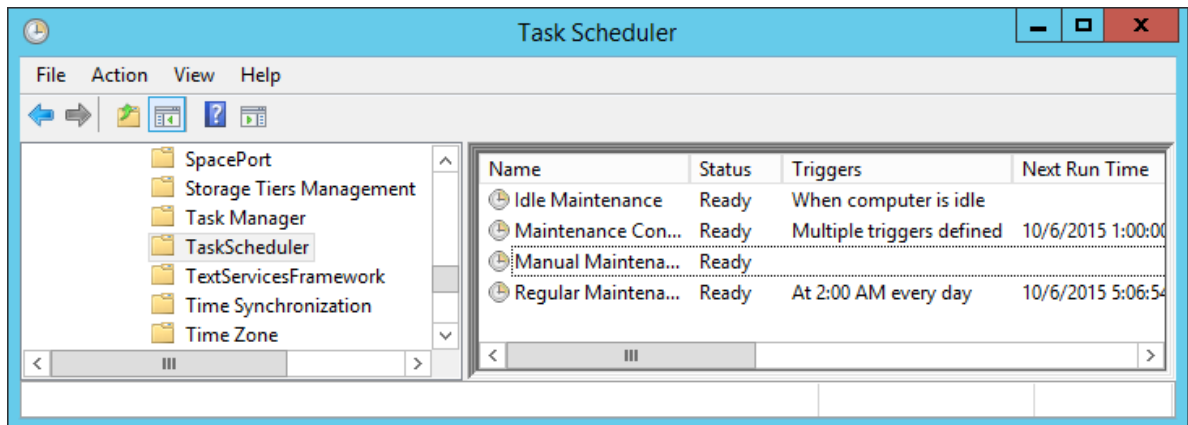
About this task

Enable Windows Server Automatic Maintenance after updating Contact Center software.

Procedure

1. Log on to the Contact Center server as an administrator.
2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Enable**.

5. In the **Name** column, right-click **Regular Maintenance** and then click **Enable**.



6. From the **File** menu, click **Exit**.

Part 3: Multimedia Contact Server migrations and patches

- [Multimedia Contact Server migration](#) on page 171
- [Multimedia Contact Server patch installation](#) on page 193

Chapter 9: Multimedia Contact Server migration

This chapter describes how to migrate Avaya Aura® Contact Center Release 6.x to a new server running Avaya Aura® Contact Center Multimedia Contact Server Release 7.1.x. This chapter also describes how to migrate Multimedia Contact Server from one Release 7.x server to another.

Existing system	New server
Avaya Aura® Contact Center Release 6.x on Windows Server 2008 R2	Avaya Aura® Contact Center Multimedia Contact Server Release 7.1.x on Windows Server 2016 or 2019
Avaya Aura® Contact Center Multimedia Contact Server Release 7.0 on Windows Server 2012 R2	
Avaya Aura® Contact Center Multimedia Contact Server Release 7.1.x on Windows Server 2016 or 2019	

This section describes how to migrate from an existing Avaya Aura® Unified Communications SIP enabled solution to a new Avaya Aura® Contact Center Release 7.1.x SIP enabled solution.

This section also describes how to migrate from an existing Avaya Communication Server 1000 AML-based solution to a new Avaya Aura® Contact Center Release 7.1.x AML-based solution.

You can use the procedures in this chapter to:

- Migrate data from your existing Contact Center Multimedia server to a new Avaya Aura® Contact Center Multimedia Contact Server.
- Migrate a Multimedia Contact Server to a new server. For example, to move Multimedia Contact Server Release 7.1.x software from one server to a new larger and faster server.

A Multimedia Contact Server includes the following server software:

- Contact Center Multimedia (CCMM)
- Avaya Workspaces (optional)

Multimedia Contact Server migration prerequisites

- Ensure that your hardware meets all requirements as described in *Avaya Aura® Contact Center Overview and Specification*.

- If you are migrating from AACC Release 6.3 or earlier, archive contacts from the CCMM database.
- Prepare your new server for software installation. For more information see, [Common server preparation procedures](#) on page 45.
- If the new server has the same name as the existing server, ensure the attachments folder and backup folder are configured the same for both servers.

Multimedia Contact Server migration procedures

About this task

This task flow shows you the sequence of procedures you perform to migrate to an Avaya Aura® Contact Center Release 7.1 Multimedia Contact Server.

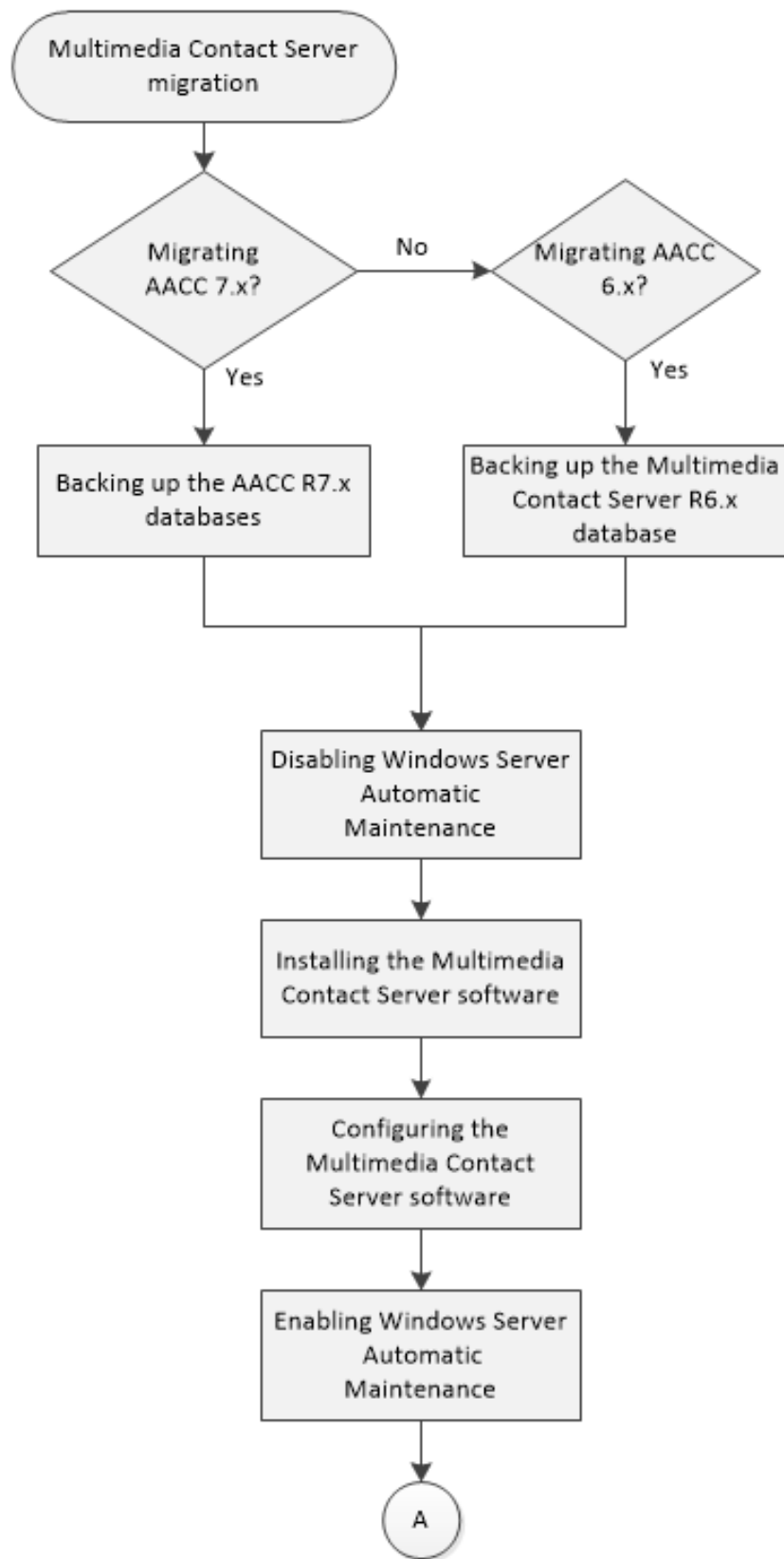


Figure 8: Multimedia Contact Server migration procedures

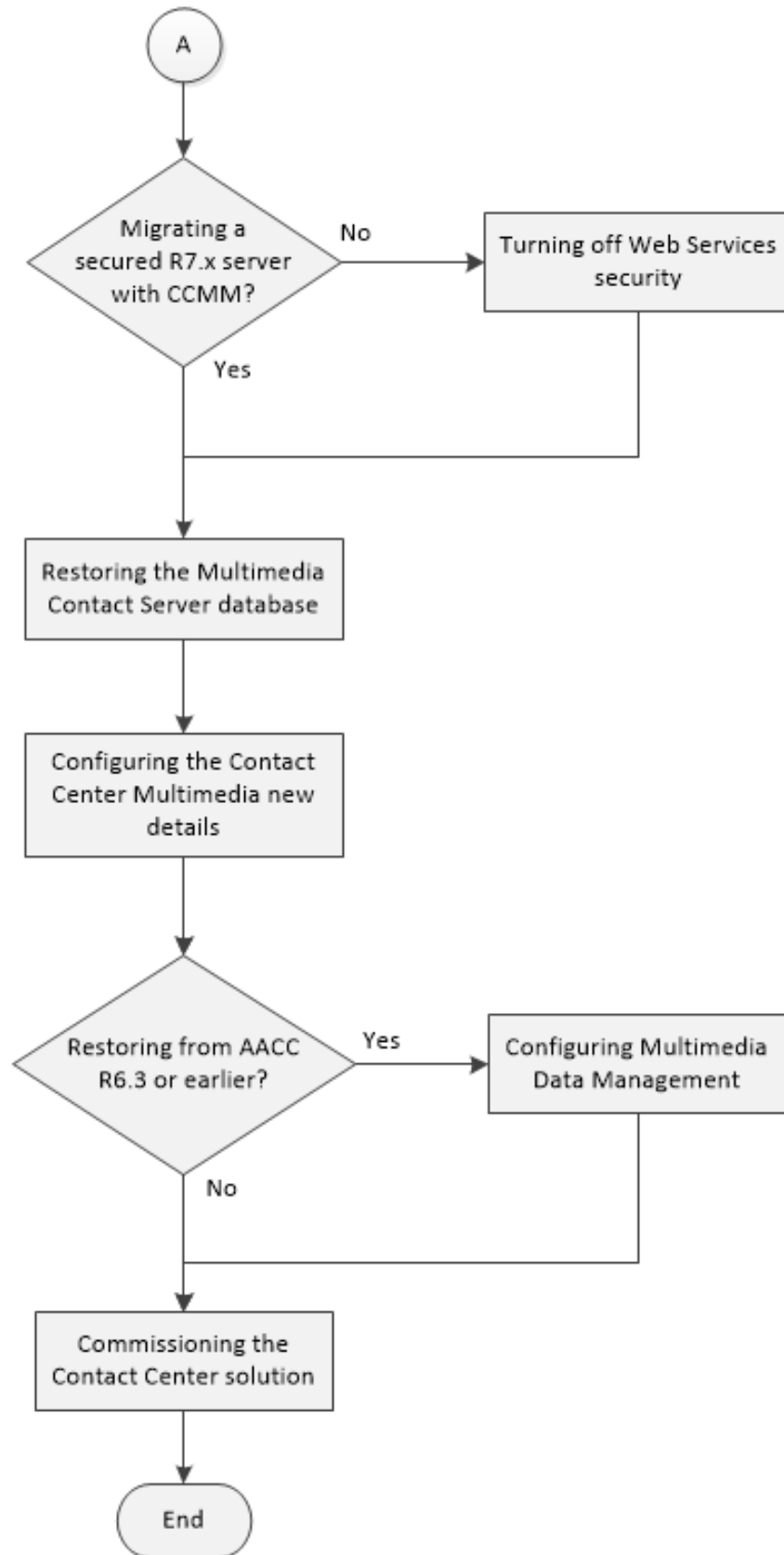


Figure 9: Multimedia Contact Server migration procedures

Backing up the Avaya Aura® Contact Center Release 7.1 databases

About this task

Back up the Avaya Aura® Contact Center Release 7.1 databases so you can restore them on the new server after you install the Avaya Aura® Contact Center Release 7.1 software.

Procedure

1. Log on to the existing Avaya Aura® Contact Center Release 7.1 server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
4. In the right pane, click **Create**.
5. From the **Drive Letter** list, select the network drive on which to store the Voice Contact Server database.
6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.
7. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the user password.
9. Click **Save**.
10. Click **OK**.
11. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
12. In the **Media Type** section, select **Network Location**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.
15. Click **Yes**, to continue with the backup.

Backing up the Multimedia Contact Server Release 6.x database

About this task

Back up the Release 6.x Multimedia Contact Server database so you can restore it on the new server after you install the new Contact Center software.

Procedure

1. On the existing Release 6.x Multimedia Contact Server, choose **Start > All Programs > Avaya > Contact Center > Database Utilities > Database Maintenance**.
2. In the Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the Backup Locations pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which to store the Multimedia Contact Server database.
5. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.
9. Click **OK**.
10. In the Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. From the **Backup Location** list, select the network drive on which to store the backup.
13. Click **Backup**.

Disabling Windows Server Automatic Maintenance

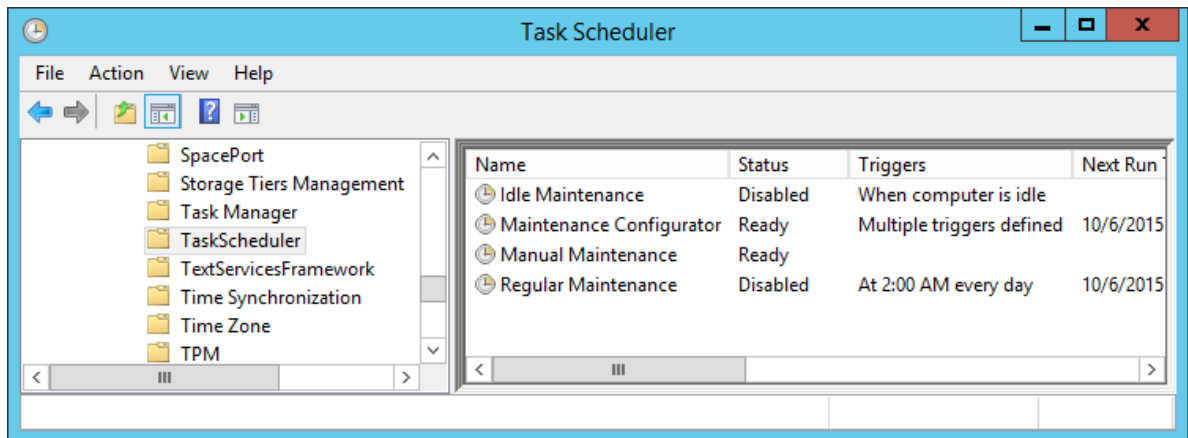
About this task

Disable Windows Server Automatic Maintenance while installing Contact Center software. Windows Server Automatic Maintenance can occasionally interfere with the real-time requirements for Contact Center. You must therefore temporarily disable Automatic Maintenance to install and configure Contact Center software. Re-enable it after deploying Contact Center.

Procedure

1. Log on to the Contact Center server as an administrator.
2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Disable**.

5. In the **Name** column, right-click **Regular Maintenance** and then click **Disable**.



6. From the **File** menu, click **Exit**.

Deploying the Avaya Workspaces OVA

Before you begin

Download the Avaya Workspaces OVA from the Avaya Support website at <https://support.avaya.com>.

* Note:

If upgrading from a previously configured Avaya Workspaces installation, you must re-deploy the Avaya Workspaces cluster using the OVA, which is shipped with the latest release. Before you start deploying new virtual machines, shut down the virtual machines created from OVAs of the previous release.

About this task

Use this procedure to deploy optional Avaya Workspaces in a virtual environment. Deploy the Avaya Workspaces OVA file onto a VMware ESXi host server using vCenter to create a virtual machine with the Avaya Workspaces software for use in the Contact Center solutions.

For Avaya Aura® Contact Center, you need to deploy three virtual machines from the Avaya Workspaces OVA. There is no restriction for the virtual machine names. For example, you can use the following names: wsk8master, wsk8node1, and wsk8node2. Use this procedure to deploy and configure each of the three virtual machines.

You must also ensure that you correctly configure CPU and memory reservation parameters for the Avaya Workspaces virtual machines. For more information, see *Avaya Aura® Contact Center Overview and Specification*.

Procedure

1. In your vCenter client, select the host server on which to deploy the Avaya Workspaces OVA.

2. Select **File > Deploy OVF Template**.
3. On the **Source** window, click **Browse**.
4. On the **Open** message box, select the Avaya Workspaces OVA file.
5. Click **Open**.
6. On the **Source** window, click **Next**.
7. On the **OVF Template Details** window, verify the details of the Avaya Workspaces OVA template and click **Next**.
8. On the **End User License Agreement** window, read the license agreement, and if acceptable, click **Accept**.
9. Click **Next**.
10. On the **Name and Location** window, type the name of the new Avaya Workspaces virtual machine. This is not the server hostname. This is the name of the VMware virtual machine as it appears in the VMware inventory.
11. Click **Next**.
12. On the **Host and Cluster** window, select the host server or cluster to deploy the Avaya Workspaces OVA. If you selected a cluster, select a **Specific Host** on that cluster.
13. Click **Next** to display the **Storage** window.
14. From the **Select a destination storage for the virtual machine files** list, select a location to store the Avaya Workspaces virtual machine image. Ensure that the storage location you select has sufficient available storage space to store a thick provisioned virtual machine image.
15. Click **Next**.
16. On the **Disk Format** window, select **Thin Provision**.
17. Click **Next**.
18. On the **Ready to Complete** window, verify the deployment settings. If you need to modify any settings, click **Back**.
19. Click **Power on after deployment**.
20. Log on to the Avaya Workspaces virtual machine using the default credentials.

The user name is `root`, and the password is `root01`. You must not change the default credentials at this step. You can create a new password later when configuring Avaya Workspaces in the Ignition Wizard.
21. Enter the `# ifconfig` command to establish the name of your network adapter.
22. To open the network configuration script, enter the `# vi /etc/sysconfig/network-scripts/ifcfg-ens192` command.

Ensure the network adapter name matches your environment.
23. Press the **Insert** key to enter the edit mode.

24. Modify the **IPADDR**, **GATEWAY**, **NETMASK**, and **DNS** fields as required. Ensure the **BOOTPROTO** field is set to *none*.
25. To save the changes, press **Esc** and type `'wq!'`. To exit without changes, press **Esc** and type `'q!'`.
26. Enter the `# systemctl restart network` command to restart the network service and enable the changes.
27. In **VM Options**, under the **VMWare tools** section, clear the **Synchronize guest time with host** check box.

You must use NTP servers for time synchronization of Contact Center machines and Avaya Workspaces nodes. You can configure time synchronization settings while configuring Avaya Workspaces in the Ignition Wizard for fresh installs or in the Update Configurator when installing at a later stage or upgrading.

Installing the Multimedia Contact Server software

Before you begin

- Download the most recent Contact Center Multimedia and common component patches to the server.
- Avoid installation from shared locations, because it might lead to installation failure. To ensure successful installation, either mount a DVD or download a local copy of a build.
- Empty all temporary folders on the server. To determine the specific temporary folders for a server, access the DOS prompt and type `set`. Note the values listed for `TEMP` and `TMP`, and delete all files in those locations.
- If you deploy in a virtual environment and want to install Avaya Workspaces, you must manually deploy three virtual machines using the Avaya Workspaces Open Virtual Appliance (OVA). See [Deploying the Avaya Workspaces OVA](#) on page 177.

About this task

Install the Multimedia Contact Server software to provide inbound and outbound voice, email (including voice mail, SMS, faxes and scanned documents), and Web communications contact types in your contact center. Multimedia Contact Server also supports Instant Messaging in SIP-enabled contact centers.

Procedure

1. Insert the Contact Center DVD into the DVD drive of your server.
2. If the installation does not automatically start, double-click **Setup.exe**.
3. Click **Accept** to install the Microsoft .NET Framework on the server.
If you are prompted to accept the Microsoft .NET Framework license agreement, click **Accept**. If you are prompted to restart the server, click **Yes** and repeat step 2.
4. Contact Center software installer runs Operating System and hardware checks on the server. If the installer returns a Fail, the software installation cannot proceed until you

correct the problem. Review any failures returned by the System Readiness Check and consult *Avaya Aura® Contact Center Overview and Specification* to determine the actions to resolve the issue.

You can ignore warnings if the potential impact to the operation of the contact center is understood and not applicable.

5. The Contact Center software installer platform and server selection screen appears.

6. Select the type of multimedia server to install:

In an Avaya Communication Server 1000 (CS1000) based solution, in the **Select Voice Platform** section, select **Avaya Communication Server 1000 - AML**.

In a SIP-enabled solution, in the **Select Voice Platform** section, select **Avaya Aura - SIP**.

7. In the **Select Server Installation Option** section, select **Multimedia Contact Server Only**.

8. **(Optional)** If you want to install and configure Avaya Workspaces, select the **Configure Workspaces for Avaya Aura Contact Center** check box.

9. Click **Next**.

10. Under **Journal Database Drive**, select the drive for the database journal.

11. Under **Multimedia Contact Server Database Drive**, select the drive for the Contact Center Multimedia database.

12. **(Optional)** If you deploy on a physical server, under **Workspaces Drive**, select the drive for the Avaya Workspaces database.

Ignore this step if you deploy on a virtual server.

 **Note:**

On virtual installs, the Workspaces Drive option is not available on the Contact Center software installer.

13. In the **Service Packs** section, browse to and select the Service Pack.



14. Click **Install**.
15. The **AVAYA GLOBAL SOFTWARE LICENSE TERMS** window appears.
16. Read the terms of the license.
 - If you accept the terms, click **I ACCEPT THE LICENSE TERMS**. *The installation continues.*
 - If you do not accept the terms, click **I DECLINE THE LICENSE TERMS**. *The installation returns to the Select Destination Drive screen.* Click **Cancel** to stop the install.
 - To print the license terms, click **Print**.
17. The **MICROSOFT SOFTWARE LICENSE TERMS** window appears.
18. Read the terms of the license.
 - If you accept the terms, click **I ACCEPT THE LICENSE TERMS**. *The installation continues.*
 - If you do not accept the terms, click **I DECLINE THE LICENSE TERMS**. *The installation returns to the Select Destination Drive screen.* Click **Cancel** to stop the install.
 - To print the license terms, click **Print**.

19. The **Progress** window appears and displays the installation progress.
20. When the software is installed, you have the following options.
 - To continue configuring the server installation data:
 - a. Select **Launch Avaya Aura Contact Center Ignition Wizard**.
 - b. Click **Configure**. This starts the Avaya Aura® Contact Center Ignition Wizard.
 - To defer configuring the server installation data:
 - a. Clear **Launch Avaya Aura Contact Center Ignition Wizard**.
 - b. On the message box, click **Yes**.
 - c. On the main installer screen, click **Close**.
 - d. Follow the on-screen instructions and shut down the Contact Center server.

You must use the Ignition Wizard to initialize Avaya Aura® Contact Center, otherwise Avaya Aura® Contact Center is not operational. For more information about the Ignition Wizard, see the following procedure.

Configuring the Multimedia Contact Server software

Before you begin

- Ensure the Avaya Aura® Unified Communications platform is configured. For more information see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.
- You must configure the required language and locale of the Contact Center server operating system, if it is not a Latin-1 language, before configuring the Contact Center server using the Contact Center Ignition Wizard. For more information about configuring language and locale settings on the Contact Center server, see *Avaya Aura® Contact Center Server Administration*.
- Read the Contact Center Release Notes for the most recent instructions.

About this task

Configure the Contact Center Multimedia Contact Server software to provide inbound and outbound voice, email (including voice mail, SMS, faxes and scanned documents), and Web communications contact types in your contact center.

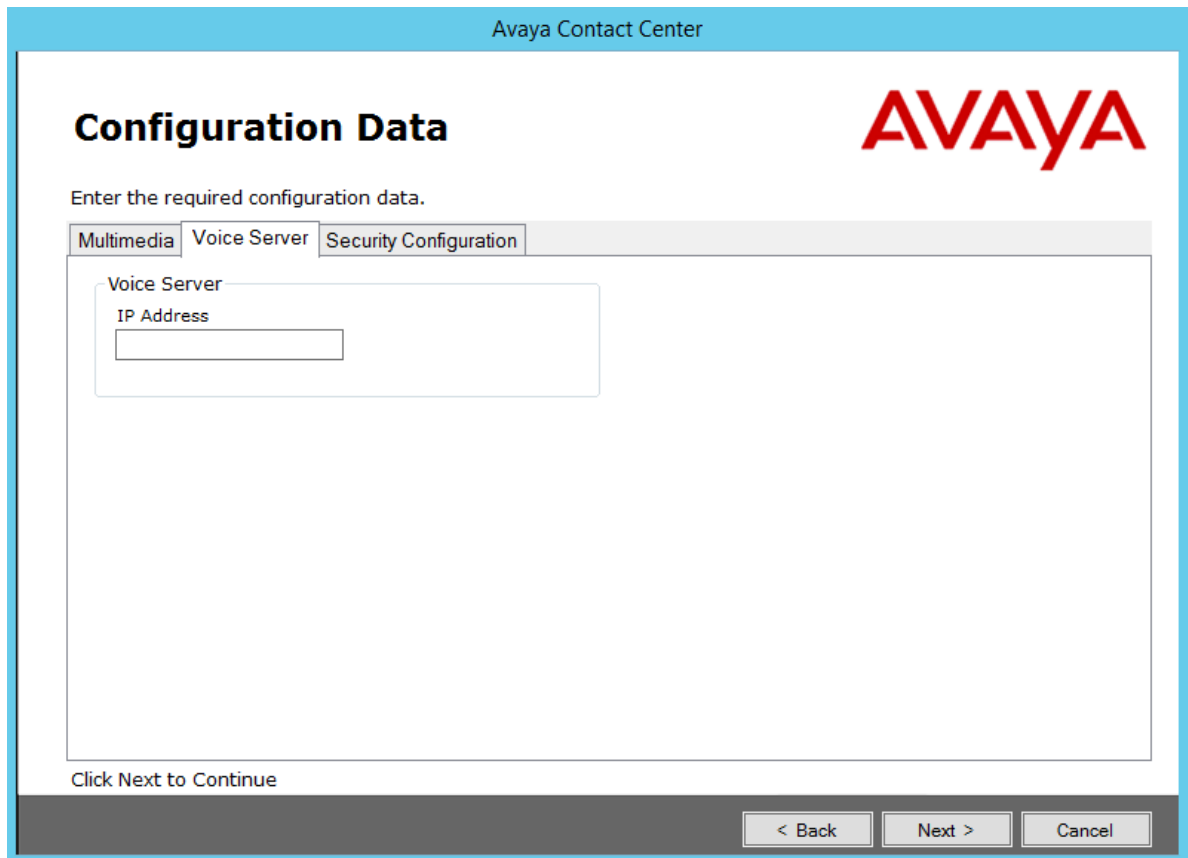
Procedure

1. Log on to the Contact Center server using the Administrator account details.
2. On the Contact Center Ignition Wizard screen, click **Next**. If the Contact Center Ignition Wizard is not visible, click the Ignition Wizard shortcut on the desktop.
3. On the **End-User License Agreement** screen, read the license agreement. Optionally, click **Print** to generate a local soft copy (in OpenXPS Document format) of the license agreement.

4. Select **I Accept the Terms of the End-User License Agreement** and click **Next**.
5. On the **Configuration Data** window, type the configuration details for each tab.
6. Select the **Multimedia** tab, and configure the Contact Center Multimedia details.

The screenshot shows the 'Configuration Data' window for the Avaya Contact Center. The window has a blue header bar with the text 'Avaya Contact Center'. Below the header, the title 'Configuration Data' is displayed in bold black text, followed by the instruction 'Enter the required configuration data.' and the Avaya logo in red. The window contains three tabs: 'Multimedia', 'Voice Server', and 'Security Configuration'. The 'Multimedia' tab is selected. Inside this tab, there are two sections: 'Incoming Mail Server' and 'Outgoing Mail Server'. The 'Incoming Mail Server' section has a 'Host Name' text box and a 'Protocol' dropdown menu with 'POP3' selected. The 'Outgoing Mail Server' section has a 'Host Name' text box and a 'Protocol' dropdown menu with 'SMTP' selected. At the bottom of the window, there is a dark gray bar with the text 'Click Next to Continue' and three buttons: '< Back', 'Next >', and 'Cancel'.

7. In the **Incoming Mail Server** box, type the name of the server on which email messages are received in your network.
8. From the **Protocol** list, select the communication protocol for the inbound email server. Select **POP3** or **IMAP**. The default protocol is POP3.
9. In the **Outgoing Mail Server** box, type the name of the server from on which email messages are sent. Your inbound and outbound mail servers can have the same name.
10. Select the **Voice Server** tab.



The image shows a screenshot of the Avaya Contact Center Configuration Data window. The window has a blue header bar with the text "Avaya Contact Center". Below the header, the title "Configuration Data" is displayed in bold black text. To the right of the title is the Avaya logo in red. Below the title, there is a prompt: "Enter the required configuration data." Below this prompt are three tabs: "Multimedia", "Voice Server", and "Security Configuration". The "Voice Server" tab is currently selected. Inside the "Voice Server" tab, there is a section labeled "Voice Server" with a sub-label "IP Address" and a text input box. Below the input box, there is a prompt: "Click Next to Continue". At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

11. In the **IP Address** box, type the IP address for the Contact Center Voice Contact Server.
12. **(Optional)** To configure optional Avaya Workspaces, select the **Workspaces** tab. See [Configuring Avaya Workspaces during the initial installation](#) on page 362 for the configuration details.
13. Select the **Security Configuration** tab, and configure the security details in the **Security Store Details** section.

The screenshot shows the 'Configuration Data' window for Avaya Contact Center. The 'Security Configuration' tab is selected. The 'Security Store Details' section contains fields for 'Full Computer Name (FQDN)' (CC7SIP.aaccdomain.com), 'Encryption Algorithm Level' (SHA256), 'Key Size' (2048), 'Security Store Password', and 'Confirm Store Password'. The 'Name of Organizational unit', 'Name of Organization', 'City or Locality', 'State or Province', and 'Two letter country code' fields are also present. The 'Subject Alternative Name' section has a 'Type' dropdown (DNS) and a 'Value' field. There are 'Add' and 'Remove' buttons for the Subject Alternative Name. A 'Skip Security Configuration' checkbox is at the bottom left, and a 'Create Store' button is at the bottom right. Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom.

14. If you do not want to enable security, select the **Skip Security Configuration** checkbox and skip to step [30](#) on page 188.

! Important:

A warning message appears. If you proceed without enabling security, you cannot fully commission your solution. For example, in SIP-enabled contact centers that use Voice, the SIP CTI link is disabled until you configure Contact Center TLS certificates to communicate securely with Application Enablement Services.

15. In the **Full Computer Name (FQDN)** box, type the full FQDN of the server on which you are creating the security store.

! Important:

The FQDN must be the full machine name of the server that the Security Store resides on. The FQDN name is case-sensitive.

16. In the **Name of Organizational unit** box, type the name of the department or division within the company.
17. In the **Name of Organization** box, type the company name.
18. In the **City or Locality** box, type the name of the city or district in which the contact center is located.

19. In the **State or Province** box, type the state or province in which the contact center is located.
20. In the **Two Letter Country Code** box, type the country code in which the contact center is located.
21. In the **Security Store password** box, type a password for accessing the new security store.
22. In the **Confirm Store password** box, confirm the password for accessing the new security store.

 **Important:**

Ensure you remember this password, because you need it when you log on to Security Manager after install. If you forget the password, you cannot access Security Manager.

23. If you are implementing High Availability in the contact center, generate the security store using Subject Alternative Names (SANs). In the **Subject Alternative Name** section, for each SAN you want to add:
 - a. From the **Type** drop-down list, select DNS.
 - b. In the **Value** field, type the FQDN for the server.
 - c. Click **Add**.

For a High Availability system, add the current server FQDN and the Managed name for the HA pair.

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

The default value for **Encryption Algorithm** is SHA256 and the default value for **Key Size** is 2048.

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

25. Click **Create Store**.
26. You can now use the **Security Configuration** tab to create and save a Certificate Signing Request (CSR) file.

The screenshot shows the 'Configuration Data' window for the Avaya Contact Center. The 'Security Configuration' tab is selected. The window title is 'Avaya Contact Center'. The main heading is 'Configuration Data'. Below it, it says 'Enter the required configuration data.' There are three tabs: 'Multimedia', 'Voice Server', and 'Security Configuration'. The 'Security Configuration' tab is active. The main content area has a title 'Store created – Generate Identity Security Certificate by signing the Certificate Signing Request provided.' Below this, there is a section for 'Certificate Signing Request file' with a text input field and a 'Create CSR File' button. Below that, there is an 'Add' button and a section for 'Imported Trusted Certificate Authority Root Certificate(s)' with a list box and a 'Remove' button. Below that, there is a section for 'Imported Identity Security Certificate' with a text input field and a 'Remove' button. On the right side, there is a 'Status' panel with instructions: 'Ensure that a removable or network drive is available.', 'Create the Certificate Signing Request file and save it to a removable or network drive.', and 'Alternatively, to defer Security Configuration and continue with the Installation Wizard.' There is a 'Reset' button at the bottom of the status panel. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. A 'Click Next to Continue' message is also present.

27. Click **Create CSR File**.

28. From the **Save In** drop-down list, select a shared location in which to save the CSR file and click **Save**.

You must now send the Certificate Signing Request file to a Certificate Authority and receive a signed certificate and root certificate to import to the security store.

29. Click **Add** to import certificates. In the **Open** dialog box, navigate to the location of a certificate and click **Open**. To remove the imported certificate, select the required certificate from the list and click **Remove**.

You can import either a chained certificate, or separate root and signed certificates. Root certificates appear in the **Imported Trusted Certificate Authority Root Certificate(s)** section. A signed certificate appears in the **Imported Identity Security Certificate** section.

If a chained certificate contains both root and signed certificates, you can add root certificates and signed certificate simultaneously by importing just one chained certificate.

If a chained certificate contains root certificates only, you can use the chained certificate to add all root certificates at a time. To add a signed certificate, click **Add** and navigate to the required signed certificate.

If you have separate root and signed certificates, you must add them one by one by clicking the **Add** button. Always add a signed certificate last.

! Important:

When adding a chained certificate, the system can prompt you to enter the password you have created for accessing the security store. See step [21](#) on page 186.

30. Click **Next**.
31. Review and verify the summary information, and click **Configure**.
32. If prompted, restart the server.

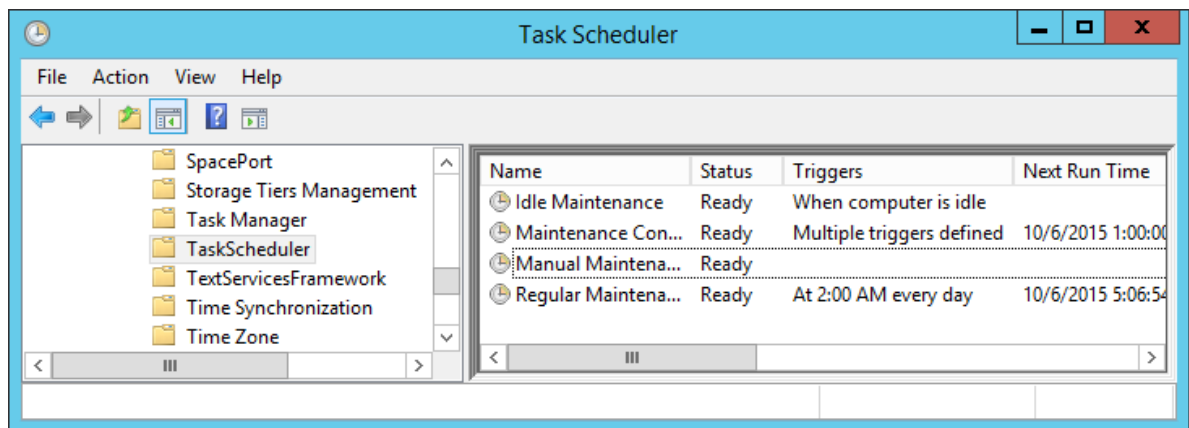
Enabling Windows Server Automatic Maintenance

About this task

Enable Windows Server Automatic Maintenance after deploying Contact Center software.

Procedure

1. Log on to the Contact Center server as an administrator.
2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Enable**.
5. In the **Name** column, right-click **Regular Maintenance** and then click **Enable**.



6. From the **File** menu, click **Exit**.

Turning off Web Services security

About this task

Turn off Web Services security before you restore a CCMM database from a system that did not have security enabled. If you are migrating from an Avaya Aura® Contact Center Release 7.x system that has Web Services security turned on, you can skip this procedure.

Before you begin

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

Procedure

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



Important:

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

2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. On the Store Access dialog, type the password for the security store, and click **OK**.
4. On the Security Manager screen, select the **Security Configuration** tab.
5. Click **Security Off**.
6. Click **Apply**.
7. On the Security Change Confirmation dialog, click **Confirm**.
8. Click **Log Out**.
9. Restart the Contact Center server.

Next steps

Complete the migration procedures in this book. After the migration, to complete your security configuration, follow the procedures in *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* or *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000*.

Restoring the Multimedia Contact Server database

Before you begin

- Create a new backup of the original Multimedia Contact Server database.
- On the new server, map a drive to the location of the backed up Multimedia Contact Server database.

 **Important:**

When you migrate configuration information from the old server to the new server, do not run the two application servers simultaneously. Both applications are configured the same, so they attempt to access and control the same resources. Continuing to run the old applications in the Contact Center can result in unpredictable behavior.

About this task

Restore the Multimedia Contact Server database to the new server. After the Multimedia Contact Server database is restored, the Contact Center Manager Administration name and email attachment paths are configured for your solution.

Procedure

1. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
2. In the Database Maintenance dialog box, in the Main Menu pane, click **Backup Locations**.
3. In the right pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which you stored the Multimedia Contact Server database backup.
5. In the **UNC Path** box, type the location of the Multimedia Contact Server database in the format \\Computer Name\Folder\Backup Location. This must precisely match the location you specified when you backed up the Database.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** field, type the user password.
8. Click **Save**.
9. Click **OK**.
10. In the Database Maintenance dialog box, in the Main Menu pane, click **Restore**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Application** section, select **CCMM**.
13. In the **Restore contents** section, select **Data**. If you are restoring an AACC Release 6.4 or Release 7.x database, select **Offline** also.
14. From the **Backup Location** list, select the network drive containing the backed up Multimedia Contact Server database.
15. Click **Restore**.
16. Click **Yes**.

Configuring the Contact Center Multimedia new details

About this task

Configure the Contact Center Multimedia (CCMM) Dashboard and Administration details.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Multimedia Dashboard**.
3. On the CCMM Dashboard, under **Server Availability**, right-click **Contact Center Manager Administration** and select **Edit**.
4. On the **Administrator Login** dialog, in the **User Name** box, type `GeneralAdmin`.
5. In the **Password** box, type the password. The default password is “__ccmm!”.
6. Click **Login**.
7. On the **Administrator Login** dialog, in the text box, type the name for the current Voice and Multimedia Contact Server.
8. Click **Save**.
9. Log on to the new Contact Center Manager Administration Web interface with administrative privileges.
10. On the **Launchpad**, click **Multimedia**.
11. In the left pane, select the Contact Center Multimedia to which you want to log on.
12. Under **CCMM Administration**, select **General Administration**.
13. Select **Server Settings**.
14. Update the server names to match the new Contact Center solution.
15. Under **CCMM Administration**, on the main menu, select **E-mail > General Settings**.
16. Under **Attachment Files**, ensure the **Inbound URL**, **Inbound Share**, **Outbound URL**, and **Outbound Share** locations match the new Contact Center solution.
17. Restart the Contact Center server.

Configuring Multimedia data management

About this task

When you migrate from a multimedia-enabled AACC Release 6.3 or earlier, Contact Center creates a new offline database and applies new data management tasks and utilities. To ensure efficient use of the Multimedia database drive on the new Contact Center server, configure Multimedia data management.

Procedure

Use the CCMM Data Management tool to create and schedule cleanup tasks to clear closed contacts from the MULTIMEDIA database. For more information on using the CCMM Data Management tool, see *Maintaining Avaya Aura® Contact Center*.

Commissioning the Contact Center solution

About this task

Commission the Contact Center solution.

Procedure

1. After migrating your server and restoring the server databases, some of the old configuration settings might not match your new solution. Commission your new server in the new solution. For more information, refer to *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000* or *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications*.
2. Use the procedures in *Avaya Aura® Contact Center Server Administration* to configure your licensed features.

Chapter 10: Multimedia Contact Server patch installation

This chapter describes how to install Avaya Aura® Contact Center patches on Multimedia Contact Server. Apply patches to resolve product issues. When installing patches, follow the instructions in the patch Release Notes.

A Multimedia Contact Server includes the following server software:

- Contact Center Multimedia (CCMM)

If your Avaya Aura® Contact Center is licensed for Standby Servers, you can hot patch your software to minimize down time. You must ensure that you patch both the active and standby servers to the same patch level. For information about hot patching, see [Common procedures](#) on page 353.

Multimedia Contact Server patch installation prerequisites

- Download the most recent documentation. See [Downloading the most recent documentation](#) on page 45.
- Download and review the latest Avaya Aura® Contact Center Release Notes. The Release Notes contain information about known issues, patches, and workarounds specific to a release and patch line-up of Contact Center. For more information about the Contact Center Release Notes, see the Avaya website (<http://support.avaya.com>).

Disabling Windows Server Automatic Maintenance

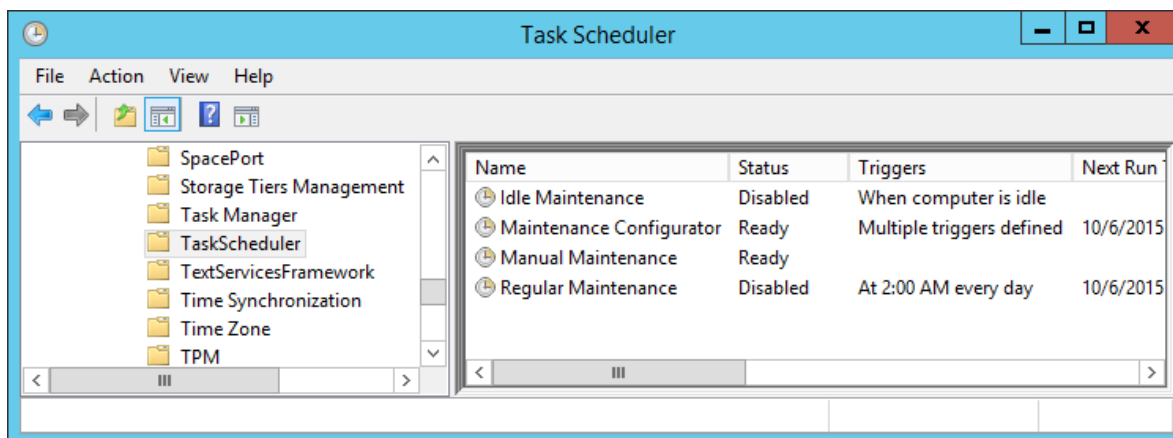
About this task

Disable Windows Server Automatic Maintenance while updating Contact Center software. Windows Server Automatic Maintenance can occasionally interfere with the real-time requirements for Contact Center. You must therefore temporarily disable Automatic Maintenance to update Contact Center software. Re-enable it after the update.

Procedure

1. Log on to the Contact Center server as an administrator.

2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Disable**.
5. In the **Name** column, right-click **Regular Maintenance** and then click **Disable**.



6. From the **File** menu, click **Exit**.

Installing Multimedia Contact Server Release Packs, Feature Packs and Service Packs

Before you begin

- Download the most recent Contact Center Release Pack, Feature Pack and Service Packs.
- Download the most recent Contact Center software patches.
- Back up the Contact Center databases.
- Temporarily stop Microsoft Windows Server Automatic Maintenance while you update Voice and Multimedia Contact Server software.
- Avoid installation from shared locations, because it might lead to installation failure. To ensure successful installation, mount the Release Bundle or install it locally.
- If you deploy in a virtual environment and want to install Avaya Workspaces, you must manually deploy three virtual machines using the Avaya Workspaces Open Virtual Appliance (OVA). See [Deploying the Avaya Workspaces OVA](#) on page 177.

About this task

Install the most recent Multimedia Contact Server Release Packs, Feature Packs or Service Packs to take advantage of new features, and to ensure that you have the most current application updates.

Procedure

1. Open the Release Pack, Feature Pack or Service Pack ZIP file.
2. Browse to the Avaya Release Pack Installer directory.
3. Double-click `setup.exe` to launch the Contact Center Release Pack Installer.
4. If you downloaded GA patches along with the Release Pack:
 - a. Select **Yes**.
 - b. Click **Browse**.
 - c. On the Browse for Folder screen, browse to the folder where you downloaded the patches, and click **OK**.
5. **(Optional)** If you want to configure Avaya Workspaces:
 - For non-HA solutions, select **Yes**.
 - For HA solutions, if installing on the Active server, select **Yes**.
 - For HA solutions, if installing on the Standby server, select **No**. You must only configure Avaya Workspaces on your Active server.
6. On the Contact Center Release Pack Installer screen, click **Next**.
7. On the Avaya Global License Terms screen, click **I ACCEPT THE LICENSE TERMS**.
8. On the MICROSOFT SOFTWARE LICENSE TERMS screen, click **I ACCEPT THE LICENSE TERMS**.

The Avaya Release Pack Installer shuts down Contact Center and installs the Release Pack, Feature Pack or Service Pack.
9. When the software update completes successfully, click **Restart**.

Contact Center reboots the server.

Next steps

If you select to configure Avaya Workspaces, when Contact Center restarts, the Contact Center Update Configurator opens so that you can configure Avaya Workspaces. For more information, see [Configuring Avaya Workspaces using the Update Configurator](#) on page 365.

Installing Multimedia Contact Server software patches

Before you begin

- Download the most recent Contact Center patches.
- Ensure that you have a recent backup of the Contact Center databases. Avaya recommends that you schedule a daily backup of the Contact Center databases at an off peak time. For more information on scheduling backups, see *Maintaining Avaya Aura® Contact Center*.
- Temporarily stop Microsoft Windows Server Automatic Maintenance while you update Contact Center software.

About this task

Install the most recent Multimedia Contact Server software patches to ensure that you have the most current application updates.

Procedure

1. From the **Start** menu, in the Avaya area, click **Update Manager**.
2. Click **Install**.
3. Click **Browse** and navigate to the folder where you downloaded the patches.
4. Click **Scan for Patches**.

The Contact Center Updates section displays the available patches.

5. Select the appropriate patches.
6. Click **Install Patch(es)**.

The Update Manager installs the patch and displays a confirmation message.

7. Click **Close**.
8. Verify that the newly installed patch appears under **Installed Updates**.
9. If the System Management and Monitoring Component (SMMC) is installed on the server, verify that it starts. For more information about starting SMMC, see [Starting SMMC](#) on page 358.

Next steps

Re-enable Microsoft Windows Server Automatic Maintenance.

Enabling Windows Server Automatic Maintenance

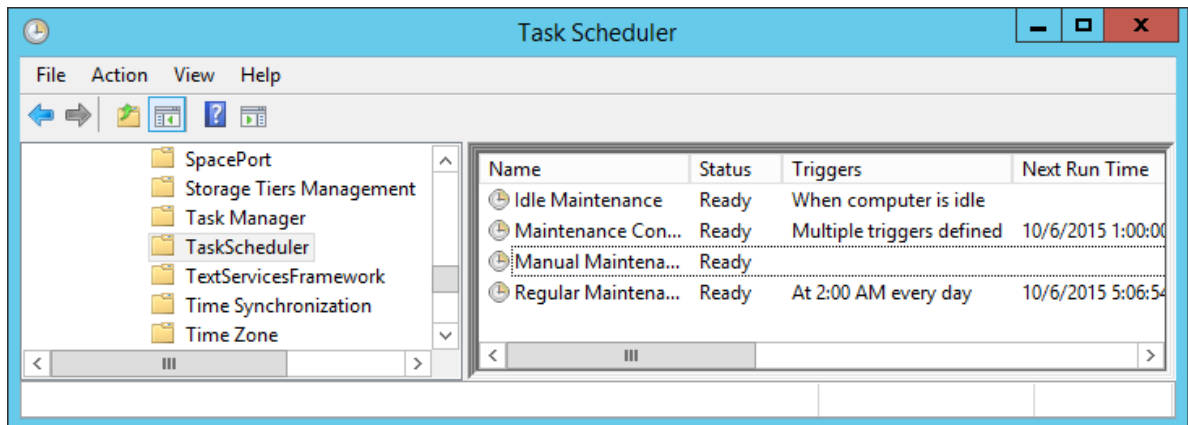
About this task

Enable Windows Server Automatic Maintenance after updating Contact Center software.

Procedure

1. Log on to the Contact Center server as an administrator.
2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Enable**.

5. In the **Name** column, right-click **Regular Maintenance** and then click **Enable**.



6. From the **File** menu, click **Exit**.

Part 4: Voice and Multimedia Contact Server with Avaya Aura® Media Server migrations and patches

- [Voice and Multimedia Contact Server with Avaya Aura Media Server migration](#) on page 199
- [Voice and Multimedia Contact Server with Avaya Aura Media Server upgrade and patch installation](#) on page 251

Chapter 11: Voice and Multimedia Contact Server with Avaya Aura® Media Server migration

This chapter describes how to migrate Avaya Aura® Contact Center Release 6.x to a new server running Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server Release 7.1.x. This chapter also describes how to migrate Voice and Multimedia Contact Server with Avaya Aura® Media Server Release 7.x from one Windows server to another.

Existing server	New server
Avaya Aura® Contact Center Release 6.x on Windows Server 2008 R2	Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server Release 7.1.x on Windows Server 2016 or 2019
Avaya Aura® Contact Center Multimedia Complement for Elite Release 6.x on Windows Server 2008 R2	
Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server Release 7.0 on Windows Server 2012 R2	
Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server Release 7.1.x on Windows Server 2016 or 2019	

Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server does not support High Availability.

This chapter describes how to migrate to a Voice and Multimedia Contact Server with Avaya Aura® Media Server in a solution with an Avaya Aura® Unified Communications platform.

You can use the procedures in this chapter to:

- Migrate data from your existing Release 6.2 or 6.3 single server with Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit, Contact Center Multimedia and Avaya Aura® Media Server (Windows version) to a new Release 7.1.x Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server.
- Migrate Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit, Contact Center Multimedia, and Avaya Aura® Media Server (Windows version) from Avaya Aura® Contact Center Release 6.x to a new server with Release 7.1.x Voice and Multimedia Contact Server with Avaya Aura® Media Server.

- Migrate an Avaya Aura® Contact Center Multimedia Complement for Elite server to a new Release 7.1.x Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server.
- Migrate a Voice and Multimedia Contact Server with Avaya Aura® Media Server Release 7.1.x to a new server. For example, to move Voice and Multimedia Contact Server with Avaya Aura® Media Server software from one server to a new larger and faster server.

A Voice and Multimedia Contact Server with Avaya Aura® Media Server includes the following server software:

- Contact Center Manager Server (CCMS)
- Contact Center Manager Server Utility
- Contact Center License Manager (LM)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center Multimedia (CCMM)
- Avaya Aura® Media Server

Voice and Multimedia Contact Server with Avaya Aura® Media Server migration prerequisites

- Ensure that your hardware meets all requirements as described in *Avaya Aura® Contact Center Overview and Specification*.

Important:

On your Voice and Multimedia Contact Server with Avaya Aura® Media Server, you must enable CPU Virtualization or Virtualization Technology in the Windows server BIOS. The available virtualization settings can vary by server manufacturer and BIOS version. Refer to the server manufacturer's documentation to determine which virtualization settings to configure.

- If you are migrating from AACC Release 6.3 or earlier, archive contacts from the CCMM database.
- Prepare your new server for software installation. For more information see, [Common server preparation procedures](#) on page 45.

Voice and Multimedia Contact Server with Avaya Aura® Media Server migration procedures

About this task

This task flow shows you the sequence of procedures you perform to migrate to an Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server.

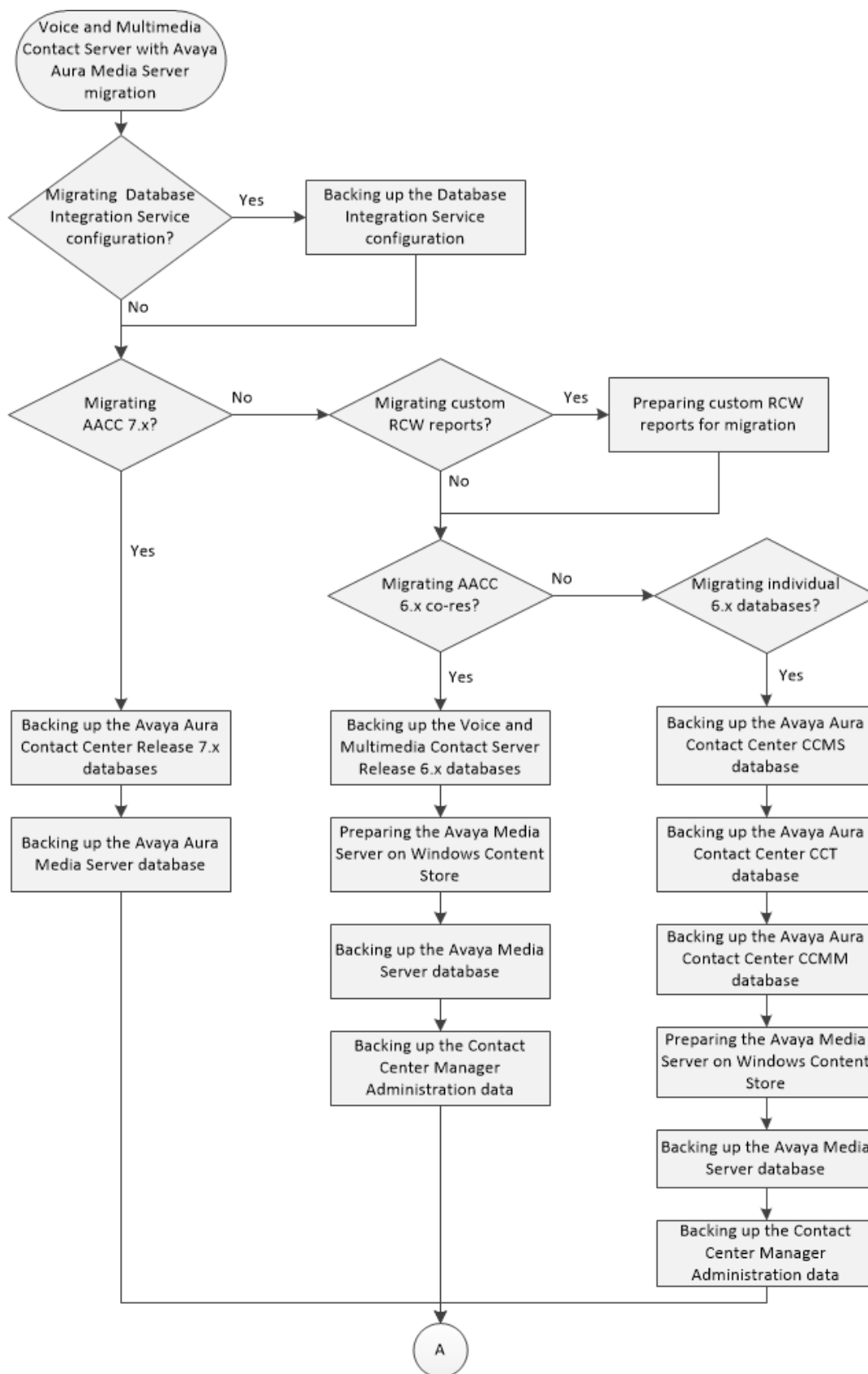


Figure 10: Voice and Multimedia Contact Server with AAMS migration procedures

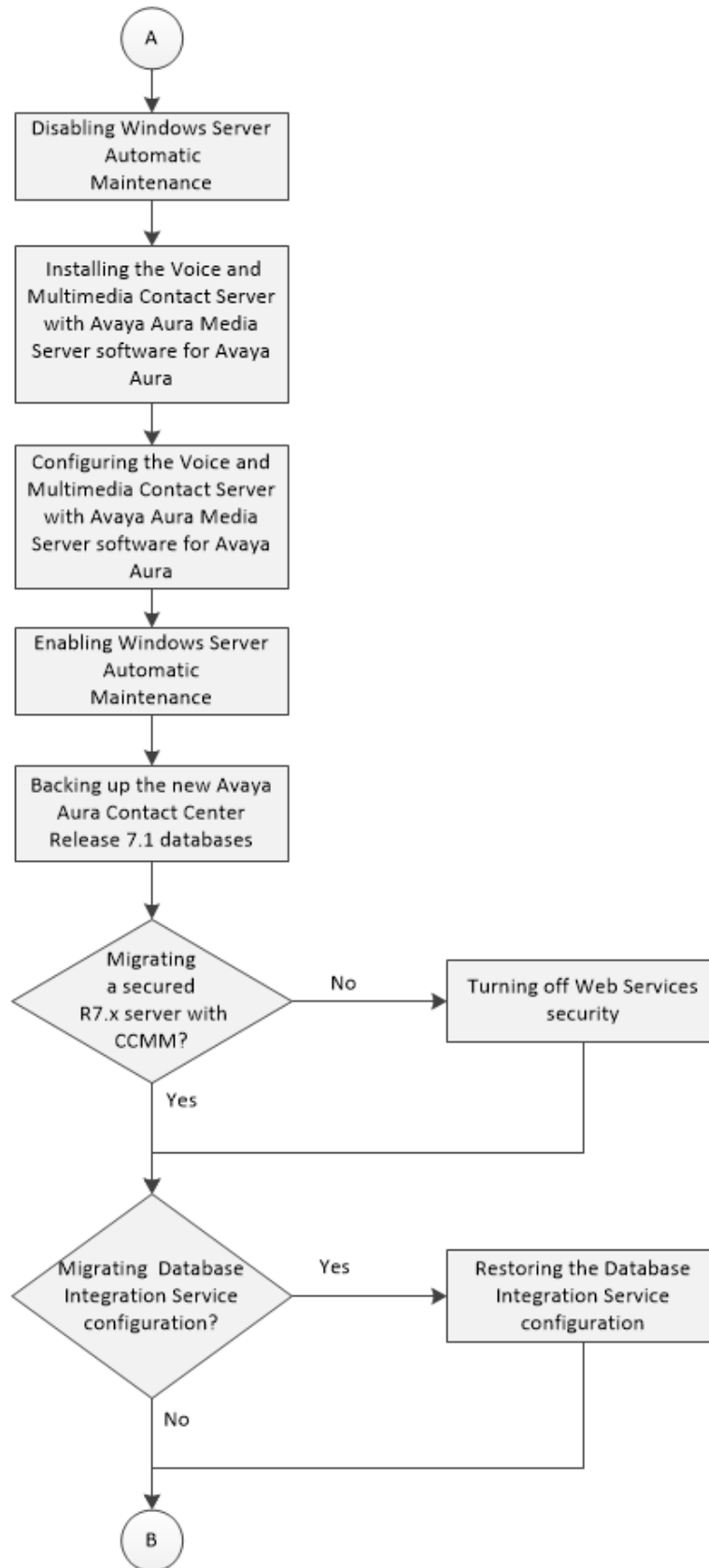


Figure 11: Voice and Multimedia Contact Server with AAMS migration procedures

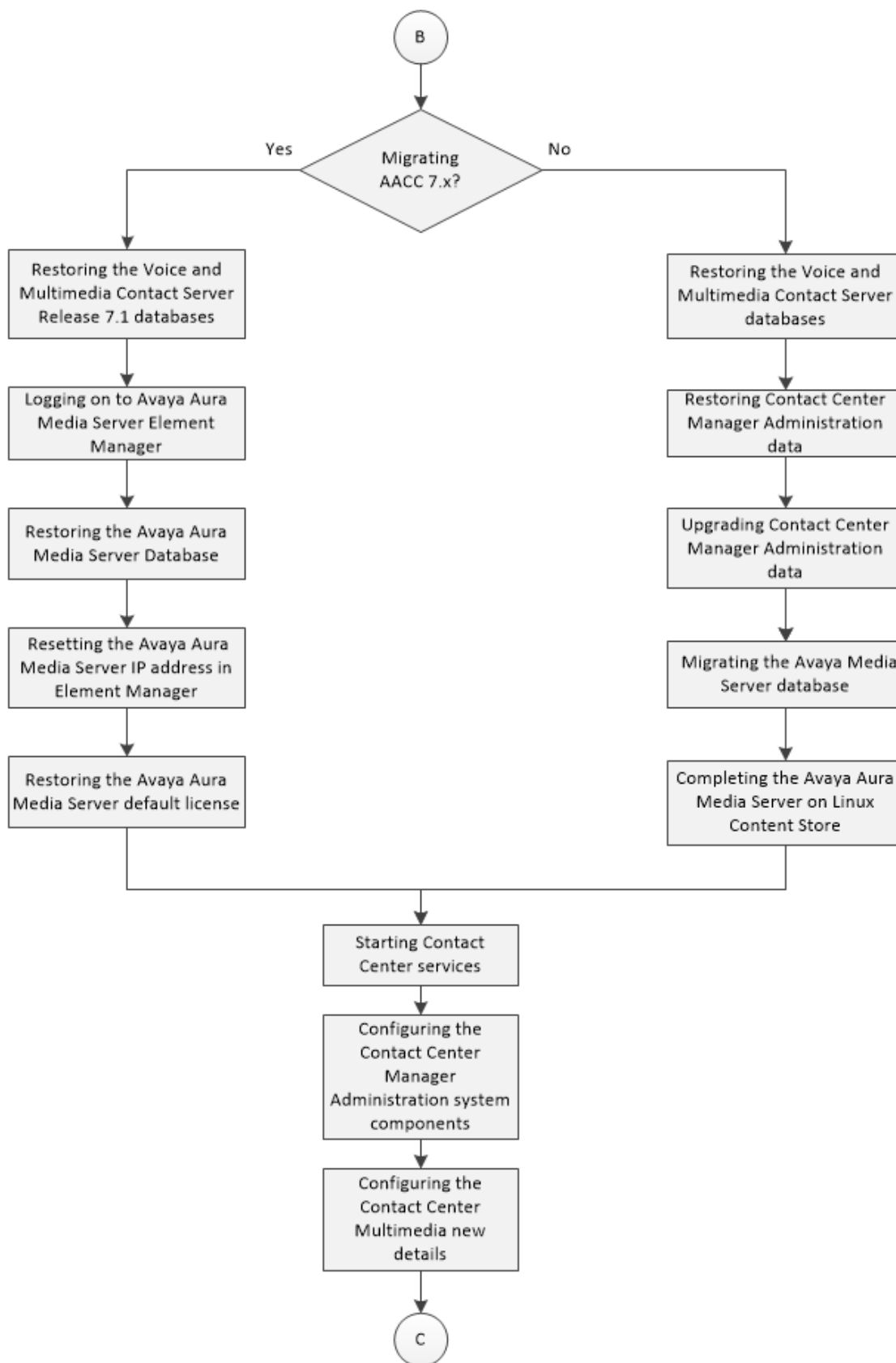


Figure 12: Voice and Multimedia Contact Server with AAMS migration procedures

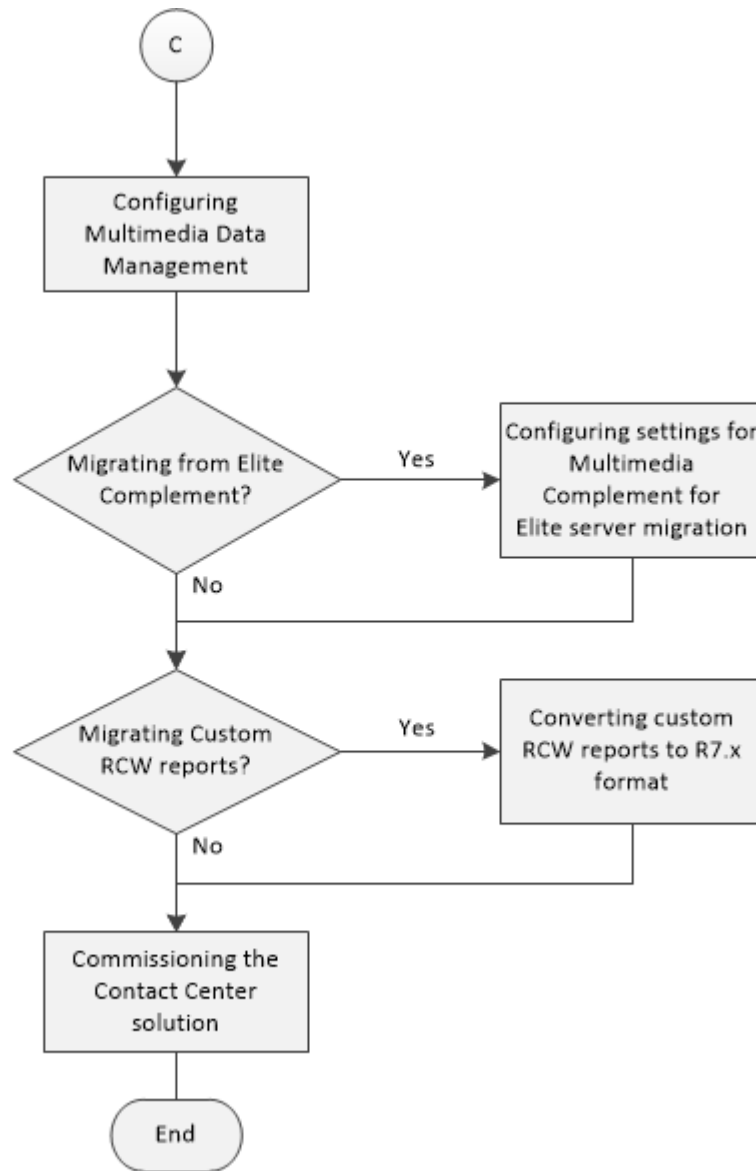


Figure 13: Voice and Multimedia Contact Server with AAMS migration procedures

Backing up the Database Integration Service configuration

Before you begin

- When you migrate the Database Integration Service to a new Contact Center server, you must manually re-configure any custom DSNs that you use in your solution.

About this task

Back up the Database Integration Service configuration to migrate the content to the new Contact Center server. Avaya recommends that you save the configuration file to a network location that you can access from the new server.

Procedure

1. On the server, click **Start** > **Run**.
2. In the Open box, type `regedit`.
3. Click **OK**.
4. If you are migrating from a Windows 2008 server (Release 6.x Avaya Aura® Contact Center):
 - a. In the Registry Editor, open the key
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Avaya\ICCM\HAI
 - b. From the **File** menu, select **Export**.
 - c. In the Export Registry File dialog box, type a name and location in which to store the configuration file.
 - d. Click **Save**.
5. Close the Registry Editor.

Preparing custom RCW reports for migration

About this task

You can migrate custom historical reports built using Report Creation Wizard (RCW) in earlier releases to equivalent SSRS reports on Contact Center 7.1. Export the original reports from Crystal format (.rpt) to intermediate files and save them in a network location. After installing the new server you can restore and convert the saved files to SSRS format.

Contact Center 7.x Service Packs include a utility to export the reports. The utility can be found in the "Install Software\CCMA\RCW_Migration_Utility" folder in the Service Pack. This is one version of the utility: AACC 6.x.

Before you begin

Important:

Custom formulas do not migrate to the new server. If the original reports use custom formulas on the existing server, the formulas do not migrate with the custom reports.

Contact Center creates a placeholder formula for each custom formula. The placeholder displays an asterisk character on the migrated report. If possible, the placeholder formula includes the original Crystal Syntax formula text as a comment. You must edit the placeholder formulas, entering valid SSRS expressions for the formula text, to complete the migration. The

placeholder formula is limited to 32,000 characters, so it is possible that very long formulas can be truncated.

Document all the custom formulas on the existing server, to assist with re-creating them on the new server after migrating the Contact Center databases.

Procedure

1. From the `\Install Software\CCMA` directory on the most recent AACC R7.x Service Pack, copy the utility for exporting Crystal reports.
You must copy the version of the utility that corresponds to the Contact Center version from which you are migrating.
2. On the Contact Center server from which you are migrating, extract the tool.
3. Run `MigrationRPTToRCWX.exe`.
4. On the Convert RTP to RCWX screen, click **Browse**, and choose a folder in which to store the output files for the converted reports.
5. Click **Run** to start the conversion.
6. When the export completes, copy the zip file to a network location from which you can copy it to the new Contact Center R7.1 server.

Next steps

Copy the zip files of exported reports to the new Contact Center server, and run the RCW import utility to convert each report to SSRS format.

Backing up the Avaya Aura® Contact Center Release 7.1 databases

About this task

Back up the Avaya Aura® Contact Center Release 7.1 databases so you can restore them on the new server after you install the Avaya Aura® Contact Center Release 7.1 software.

Procedure

1. Log on to the existing Avaya Aura® Contact Center Release 7.1 server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
4. In the right pane, click **Create**.
5. From the **Drive Letter** list, select the network drive on which to store the Voice Contact Server database.

6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.
7. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the user password.
9. Click **Save**.
10. Click **OK**.
11. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
12. In the **Media Type** section, select **Network Location**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.
15. Click **Yes**, to continue with the backup.

Backing up the Avaya Aura® Media Server database

Before you begin

- Configure the destination File Transfer Protocol (FTP) server and check that it is operational.
- Ensure that you have the address or host name, FTP account details, and path for the backup server.
- Avaya Aura® Media Server must be fully patched before backing up the database.

About this task

Create a location to store backups. You can specify an FTP server to which you can send Avaya Aura® Media Server Element Manager backups. Backup the Avaya Aura® Media Server data so you can restore it on the new server.

Procedure

1. Log on to the existing Avaya Aura® Media Server.
2. Access the Element Manager with administrator privileges.
3. Expand **Tools**.
4. Expand **Backup and Restore**.
5. Select **Backup Destinations**.
6. On the Backup Destinations window, click **Add**.
7. On the Backup Destination Properties window, in the **Destination Name** box, type a name for this backup destination.

8. In the **Host Name box**, **type** the host name or IP address of the FTP server.
9. In the **User Name box**, type the FTP user name for the destination server.
10. In the **Password box**, type the FTP password for the destination server.
11. In the **Destination Path box**, type the path on the destination server to specify to which directory the backup function writes.
12. Click **Test**. Element Manager tests the details entered by logging on to the specified FTP server.
13. Click **Save**.
14. Select **Backup Tasks**.
15. On the Backup Tasks window, click **Add**.
16. On the Add New Backup Task window, in the **Backup Task Name box**, type a name for this backup.
17. Select **Application Content**.
18. Select **System Configuration**.
19. Choose the backup destination that you created for the migration.
20. Select **Manually, as needed**.
21. Click **Save**.
22. In the Backup Tasks window, select the backup task you created.
23. Click **Run Now**.

The Confirm Backup window appears, showing the backup task name details about the backup.
24. Click **Confirm**.

The History Log Window appears. When the backup is complete, the backup details appear in the list.

Backing up the Voice and Multimedia Contact Server Release 6.x databases

About this task

Back up the Release 6.x Voice and Multimedia Contact Server databases so you can restore them on the new server after you install the Avaya Aura® Contact Center Release 7.1 software.

Procedure

1. On the existing Release 6.x Voice and Multimedia Contact Server, choose **Start > All Programs > Avaya > Contact Center > Database Utilities > Database Maintenance**.

2. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the right pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which to store the Voice and Multimedia Contact Server database.
5. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.
9. Click **OK**.
10. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. From the **Backup Location** list, select the network drive on which to store the backup.
13. Click **Backup**.
14. Click **Yes**, to continue with the backup.

Preparing the Avaya Media Server on Windows Content Store

Before you begin

- Read the Avaya Aura® Contact Center Release Notes.
- Apply the most recent Avaya Media Server service packs and Quick Fix Engineering (QFE) patches.
- Obtain the most recent version of the Avaya Aura® Contact Center Release 7.1 DVD. Read the Avaya Aura® Contact Center Release Notes to ensure that you are using the most recent version of Avaya Aura® Media Server software. The Avaya Aura® Contact Center DVD might not contain the most recent version of the Avaya Aura® Media Server software.
- Know the Avaya Aura® Contact Center SIP domain name.

About this task

Prepare the Avaya Media Server Content Store data for upgrade and migration to Avaya Aura® Media Server Release 8.0.

Procedure

1. Insert the Avaya Aura® Contact Center Release 7.1 DVD into the DVD drive of your Windows server.
2. On the DVD, navigate to the following folder: `\Install Software\AMS\Windows`
3. Locate and run the `prepareForAAMS77Migration` utility.
4. At the **Please enter ACC SIP Domain** prompt, enter the Avaya Aura® Contact Center SIP domain name.

The utility prepares the Avaya Media Server data for migration to Avaya Aura® Media Server Release 8.0.

Backing up the Avaya Media Server database

Before you begin

- Apply the most recent Avaya Media Server Release service packs and Quick Fix Engineering (QFE) patches.

About this task

Backup the Avaya Media Server data. Backup the Application Content data.

Procedure

1. Access the primary Media Server Element Manager with Administrator privileges.
2. Expand **Tools**.
3. Expand **Backup and Restore**.
4. Select **Backup Tasks**.
5. On the Backup Tasks window, click **Add**.
6. On the Add New Backup Task window, in the **Backup Task Name** box, type a name for this backup.
7. Select **Application Content**.
8. Ensure **System Configuration** is not selected. Clear **System Configuration**.
9. Choose the backup destination that you created for the migration, or the default backup location.
10. Select **Manually, as needed**.
11. Click **Save**.
12. In the Backup Tasks window, select the backup task you created.
13. Click **Run Now**.

The Confirm Backup window appears, showing the backup task name details about the backup.

14. Click **Confirm**.

The History Log Window appears. When the backup is complete, the backup details appear in the list.

15. Copy the backup to a secure network location.

Backing up the Avaya Aura® Contact Center CCMA data

Before you begin

- Map a network drive on which to back up your database. The network drive must be in NTFS format.
- Log on to the Contact Center Manager Administration server as an administrator.

About this task

Back up the Contact Center Manager Administration data on the source server Release 6.x to enable migration of the data to the new Contact Center server.

If your Contact Center Manager Administration uses High Availability replication, you must backup the data from the active CCMA.

Procedure

1. On the server with CCMA, choose **Start > All Programs > Avaya > Contact Center > Manager Administration > Configuration**.
2. In the left pane of the **Avaya Configuration** window, expand **Avaya > Applications > Backup & Restore**.
3. In the right pane, click **Backup & Restore**.
4. In the **Contact Center Manager Administration - Backup And Restore** dialog box, click **Backup** tab.
5. Select **Drive**.
6. Type the drive where the backed up database is stored.
7. Click **Next**.
8. In the **Perform Backup** section, select **Run Now**.
9. Click **Next**.
10. In the **Username** box, type a user name with administrative privileges for the server to which you store the backup.
11. In the **Password** box, type a password with administrative privileges for the server to which you store the backup.

12. From the **Domain** list, select the domain of the server to which you store the backup.
13. Click **Finish**.

Backing up the Avaya Aura® Contact Center CCMS database

About this task

Back up the Avaya Aura® Contact Center CCMS 6.x individual database so you can restore it on the new server after you install the Avaya Aura® Contact Center software.

Procedure

1. On the Contact Center Manager Server, choose **Start > All Programs > Avaya > Contact Center > Database Utilities > Database Maintenance**.
2. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the right pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which to store the Contact Center Manager Server database.
5. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.
9. Click **OK**.
10. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Applications** section, select **CCMS**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.
15. Click **Yes**, to continue with the backup.

Backing up the Avaya Aura® Contact Center CCT database

About this task

Back up the Avaya Aura® Contact Center CCT 6.x individual database so you can restore it on the new server after you install the Avaya Aura® Contact Center software.

Procedure

1. On the Communication Control Toolkit server, choose **Start > All Programs > Avaya > Contact Center > Database Maintenance**.
2. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the Backup Locations pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which you stored the Communication Control Toolkit database.
5. In the **UNC Path** box, type the location of the Communication Control Toolkit database in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.
9. Click **OK**.
10. In the Contact Center Database Maintenance window, in the Main Menu pane, select **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Applications** section, select **CCT**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.

Backing up the Avaya Aura® Contact Center CCMM database

Before you begin

Note:

If you back up a Contact Center Multimedia database without backing up the Contact Center Manager Server database, this can result in a mismatch in data when you restore. Avaya

recommends that you back up the Contact Center Manager Server database and the Contact Center Multimedia database at the same time.

About this task

Back up the Avaya Aura® Contact Center Contact Center Multimedia 6.x individual database so you can restore it on the new server after you install the new Contact Center software.

Procedure

1. In the Contact Center Multimedia server, choose **Start > All Programs > Avaya > Contact Center > Database Utilities > Database Maintenance**.
2. In the Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the Backup Locations pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which to store the Contact Center Multimedia database.
5. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.
9. Click **OK**.
10. In the Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Applications** section, select **CCMM**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.

Disabling Windows Server Automatic Maintenance

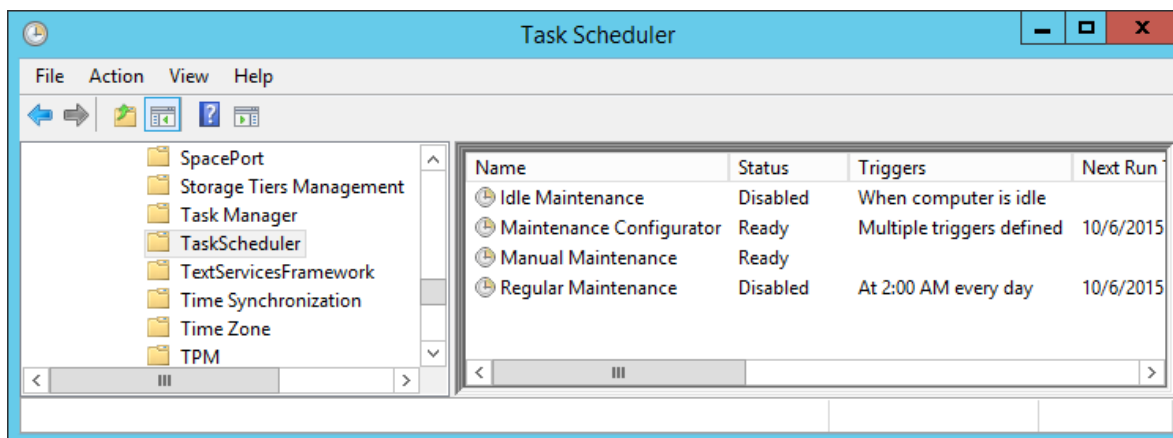
About this task

Disable Windows Server Automatic Maintenance while installing Contact Center software. Windows Server Automatic Maintenance can occasionally interfere with the real-time requirements for Contact Center. You must therefore temporarily disable Automatic Maintenance to install and configure Contact Center software. Re-enable it after deploying Contact Center.

Procedure

1. Log on to the Contact Center server as an administrator.

2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Disable**.
5. In the **Name** column, right-click **Regular Maintenance** and then click **Disable**.



6. From the **File** menu, click **Exit**.

Installing the Voice and Multimedia Contact Server with Avaya Aura® Media Server software for Avaya Aura® Unified Communications platform

Before you begin

- Ensure the Avaya Aura® Unified Communications platform is configured. For more information see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.
- Download the most recent Contact Center patches to the server.
- Avoid installation from shared locations, because it might lead to installation failure. To ensure successful installation, either mount a DVD or download a local copy of a build.
- Read the Contact Center Release Notes for the most recent instructions.

About this task

Install the Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server software and enable your contact center to route contacts to the agents that can answer the call with the correct skills.

Procedure

1. Insert the Contact Center DVD into the DVD drive of your server.

2. If the installation does not automatically start, double-click **Setup.exe**.

3. Click **Accept** to install the Microsoft .NET Framework on the server.

If you are prompted to accept the Microsoft .NET Framework license agreement, click **Accept**. If you are prompted to restart the server, click **Yes** and repeat step 2.

4. Contact Center software installer runs Operating System and hardware checks on the server. If the installer returns a Fail, the software installation cannot proceed until you correct the problem. Review any failures returned by the System Readiness Check and consult *Avaya Aura® Contact Center Overview and Specification* to determine the actions to resolve the issue.

You can ignore warnings if the potential impact to the operation of the contact center is understood and not applicable.

5. The Contact Center software installer platform and server selection screen appears.

6. In the **Select Voice Platform** section, select **Avaya Aura - SIP**.

7. In the **Select Server Installation Option** section, select **Voice and Multimedia Contact Server with Avaya Aura Media Server**.

8. **(Optional)** If you want to install and configure Avaya Workspaces, select the **Configure Workspaces for Avaya Aura Contact Center** check box.

9. Click **Next**.

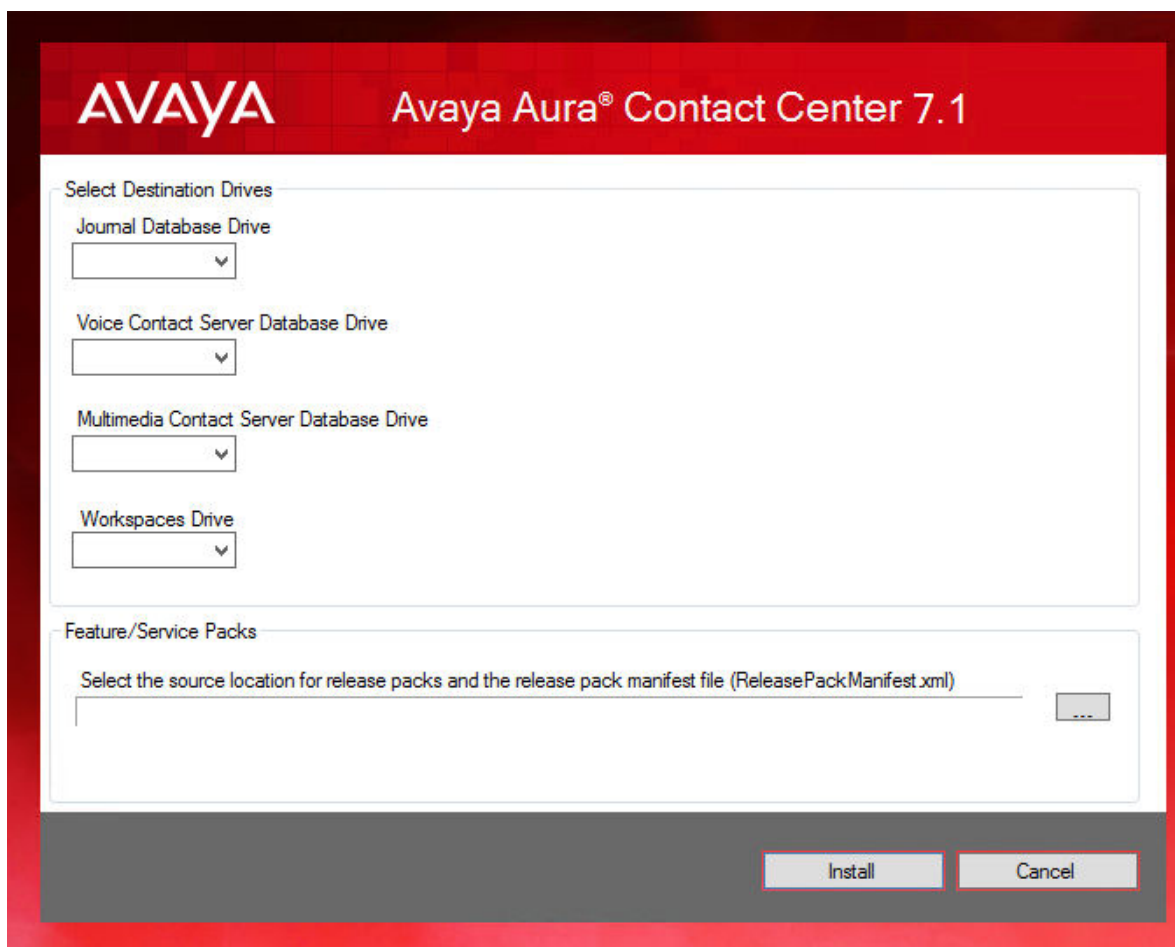
10. Under **Journal Database Drive**, select the drive for the database journal. The default drive partition is H:.

11. Under **Voice Contact Server Database Drive**, select the drive for the Contact Center Manager Server, Communication Control Toolkit, and Contact Center Manager Administration databases. The default drive partition is F:.

12. Under **Multimedia Contact Server Database Drive**, select the drive for the Contact Center Multimedia database. The default drive partition is G:.

13. **(Optional)** Under **Workspaces Drive**, select the drive for the Avaya Workspaces database.

14. In the **Service Packs** section, browse to and select the Service Pack.



15. Click **Install**.
16. The **AVAYA GLOBAL SOFTWARE LICENSE TERMS** window appears.
17. Read the terms of the license.
 - If you accept the terms, click **I ACCEPT THE LICENSE TERMS**. *The installation continues.*
 - If you do not accept the terms, click **I DECLINE THE LICENSE TERMS**. *The installation returns to the Select Destination Drive screen.* Click **Cancel** to stop the install.
 - To print the license terms, click **Print**.
18. The **MICROSOFT SOFTWARE LICENSE TERMS** window appears.
19. Read the terms of the license.
 - If you accept the terms, click **I ACCEPT THE LICENSE TERMS**. *The installation continues.*
 - If you do not accept the terms, click **I DECLINE THE LICENSE TERMS**. *The installation returns to the Select Destination Drive screen.* Click **Cancel** to stop the install.
 - To print the license terms, click **Print**.

20. The **Progress** window appears and displays the installation progress.
21. When the software is installed, click **Restart** to restart the Contact Center server.

After you restart the Contact Center server, you must use the Ignition Wizard to initialize Avaya Aura® Contact Center, otherwise Avaya Aura® Contact Center is not operational. For more information about the Ignition Wizard, see the following procedure.

Configuring the Voice and Multimedia Contact Server with Avaya Aura® Media Server software for Avaya Aura® Unified Communications platform

Before you begin

- Ensure the Avaya Aura® Unified Communications platform is configured. For more information see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.
- You must configure the required language and locale of the Contact Center server operating system, if it is not a Latin-1 language, before configuring the Contact Center server using the Contact Center Ignition Wizard. For more information about configuring language and locale settings on the Contact Center server, see *Avaya Aura® Contact Center Server Administration*.
- Read the Contact Center Release Notes for the most recent instructions.

About this task

Configure the Contact Center Voice and Multimedia Contact Server with Avaya Aura® Media Server software and enable your contact center to route contacts to the agents that can answer the call with the correct skills.

Procedure

1. Log on to the Contact Center server using the Administrator account details.
2. On the Contact Center Ignition Wizard screen, click **Next**. If the Contact Center Ignition Wizard is not visible, click the Ignition Wizard shortcut on the desktop.
3. On the **End-User License Agreement** screen, read the license agreement. Optionally, click **Print** to generate a local soft copy (in OpenXPS Document format) of the license agreement.
4. Select **I Accept the Terms of the End-User License Agreement** and click **Next**.
5. On the **Configuration Data** window, type the configuration details for each tab.
6. Select the **Core** tab, and configure the server details.

Avaya Contact Center

Configuration Data

Enter the required configuration data.

Core Licensing SIP Multimedia Security Configuration

Site Name
Site Name
CC7SIP

Real-Time Statistics Multicast IP Address
IP Address
234.5.6.10

System Account Configuration
Enter a password for the Contact Center administration Windows account.
Password
Confirm Password

Avaya Aura® Media Server
IP Address
Password
Confirm Password
Contact Center Media Services Locale
en_us

Click Next to Continue

< Back Next > Cancel

7. In the **Site Name** box, type the site name for the Contact Center server. The site name must not contain spaces or non-alphabetical characters except hyphen (-) and underscore (_). The first character must be a letter. The site name must be unique and can consist of 6 to 15 characters.
8. In the **Real-Time Statistics Multicast IP Address** box, type the Real-time Statistics Multicast IP Address of the server to associate with sending real-time data. The **IP Address** must be from 224.0.1.0 to 239.255.255.255. The default is 234.5.6.10.
9. In the **System Account Configuration** section, in the **Password** box, type a password for the Contact Center administration account. The password is checked against the server security policy for minimum password requirements. Avaya recommends that you enter a password that conforms to your corporate password policy.
10. In the **Confirm Password** box, type the password.
11. In the **Avaya Aura Media Server** section, in the **IP Address** box, type the IP address of the Avaya Aura® Media Server.

! Important:

You must ensure that this IP address is not in use, and must be in the same subnet as the Contact Center server.

12. In the **Password** box, type a password for the Avaya Aura® Media Server *cust* account.

13. In the **Confirm Password** box, re-type the password.
14. From the **Contact Center Media Services Locale** drop-down list, select the locale (including language and dialects) of the solution environment.
15. Select the **Licensing** tab, and configure the licensing details.

The screenshot shows the 'Avaya Contact Center' window with the 'Configuration Data' tab selected. The 'Licensing' sub-tab is active. The window contains the following fields and controls:

- License Type:** A dropdown menu with 'Local WebLM' selected.
- License File:** A section containing a 'License File Location' text box, a 'Browse' button, and a 'Skip' button.
- System HostID (MAC Address):** A text box containing '00:50:56:8D:48:8D'.
- License Manager Package:** A dropdown menu with 'Nodal Enterprise' selected.
- Features:** A list of checkboxes for optional features:
 - ☐ Networking
 - ☐ Instant Messaging
 - ☐ Web Based Statistics
 - ☐ Multiplicity
 - ☐ Open Queue
 - ☐ Open Interfaces Open Queue
 - ☐ Open Interfaces Universal Networking
 - ☐ Agent Greeting
 - ☐ Offsite Agent

At the bottom, there is a 'Click Next to Continue' instruction and three buttons: '< Back', 'Next >', and 'Cancel'.

16. From the **License Type** list, select **Local WebLM** to use the on-server WebLM license manager instance, or select **Remote WebLM** to use a separate Avaya WebLM server.
 - If you select **Local WebLM**, you cannot apply your Local WebLM license file until after you configure your contact center using the Ignition Wizard. You must apply your license file during the commissioning process.
 - If you select **Remote WebLM**, in the **IP Address** box, type the IP address for the remote Avaya WebLM server. In the **Port** box, type the port number for the remote Avaya WebLM server. The default port number is 52233.
17. From the **Licensing Package** list, select the license type that you have purchased. Select **Nodal Enterprise** for single-site contact centers.
18. From the list of **Optional Packages**, enable the licensed features that you have purchased.
19. Select the **Open Queue** check box.

20. Select the **SIP** tab, and configure the SIP details.

The screenshot shows the 'Configuration Data' form for the Avaya Contact Center, specifically the 'SIP' tab. The form is titled 'Enter the required configuration data.' and has tabs for 'Core', 'Licensing', 'SIP', 'Multimedia', and 'Security Configuration'. The 'SIP' tab is active. The form contains several sections: 'Switch Configuration' with a dropdown menu set to 'Avaya Aura'; 'SIP Voice Proxy Server' with fields for 'IP Address', 'Port' (5060), and 'Transport' (TCP); 'SIP CTI Proxy Server' with fields for 'IP Address', 'Port' (4723), and 'Transport' (TLS); 'Local SIP Subscriber' with a 'Domain Name' field; 'Backup SIP Voice Proxy Server' with fields for 'IP Address', 'Port' (5060), and 'Transport' (TCP); and 'SIP IM Proxy Server' with fields for 'IM Provider' (Aura Presence Services), 'XMPP Domain', and 'IP Address', 'Port', and 'Transport'. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'. A 'Click Next to Continue' button is also present.

21. In the **SIP Voice Proxy Server** section, in the **IP Address** box, type the IP address for the primary Avaya Aura® Session Manager.
22. In the **SIP Voice Proxy Server** section, in the **Port** box, type the server listening port number. The default port is 5060.
23. In the **SIP Voice Proxy Server** section, from the **Transport** list, select the SIP Network Transport communication protocol. The default is TCP.

*** Note:**

If there are Contact Center agents using SIP deskphones, or if your solution uses Avaya Aura® Presence Services 7.1 or later, you must ensure that the SIP Network Transport communication protocol is set to TLS.

24. In the **SIP CTI Proxy Server** section, in the **IP Address** box, type the IP address for the Avaya Aura® Application Enablement Services server.
25. In the **SIP CTI Proxy Server** section, in the **Port** box, type the SIP CTI Proxy Server port number. The default SIP CTI Proxy Server port is 4723.
26. In the **SIP CTI Proxy Server** section, from the **Transport** list, select the SIP Network Transport CTI communication protocol. The default Avaya Aura® Application Enablement Services communication protocol is TLS.

27. In the **Local SIP Subscriber** section, in the **Domain Name** box, type the SIP domain name for the SIP-enabled contact center. Typically the Avaya Aura® Contact Center SIP Domain Name matches your Active Directory domain name. The Avaya Aura® Contact Center SIP Domain Name matches the Session Manager contact center SIP domain name. The Local SIP Subscriber Domain Name must be different to the XMPP Domain name.
28. Do not configure the **Backup SIP Voice Proxy Server**.
29. In the **SIP IM Proxy Server** section, from the **IM Provider** list, select the Instant Messaging provider. Select Aura Presence Services or, if you are using Microsoft Skype for Business or Microsoft Lync, select Microsoft Lync. The **IM Provider** question is enabled if you select the **Instant Messaging** optional license package on the **Licensing** tab.
30. In the **SIP IM Proxy Server** section, if using an Avaya Aura® Presence Services server, in the **XMPP Domain** box, type the domain name of the Extensible Messaging and Presence Protocol (XMPP) server. The XMPP Domain name must be different to the Local SIP Subscriber Domain Name.
31. In the **SIP IM Proxy Server** section, in the **IP Address** box, type the IP address of the SIP IM Proxy Server.
32. In the **SIP IM Proxy Server** section, in the **Port** box, type the port number for the IM Proxy Server. The default port number for Avaya Aura® Presence Services is 5222. The default port number for Microsoft instant messaging servers is 5060.
33. In the **SIP IM Proxy Server** section, from the **Transport** list, select the SIP IM Proxy Server transport protocol.
34. Select the **Multimedia** tab, and configure the Contact Center Multimedia details.

The screenshot shows the 'Avaya Contact Center' configuration interface. The title bar is blue with the text 'Avaya Contact Center'. The main header area has 'Configuration Data' on the left and the 'AVAYA' logo on the right. Below the header, it says 'Enter the required configuration data.' There are five tabs: 'Core', 'Licensing', 'SIP', 'Multimedia', and 'Security Configuration'. The 'Security Configuration' tab is selected. Inside this tab, there are two sections: 'Incoming Mail Server' and 'Outgoing Mail Server'. The 'Incoming Mail Server' section has a 'Host Name' text box and a 'Protocol' dropdown menu with 'POP3' selected. The 'Outgoing Mail Server' section has a 'Host Name' text box and a 'Protocol' dropdown menu with 'SMTP' selected. At the bottom of the configuration area, it says 'Click Next to Continue'. At the very bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

35. In the **Incoming Mail Server** box, type the name of the server on which email messages are received in your network.
36. From the **Protocol** list, select the communication protocol for the inbound email server. Select **POP3** or **IMAP**. The default protocol is POP3.
37. In the **Outgoing Mail Server** box, type the name of the server from on which email messages are sent. Your inbound and outbound mail servers can have the same name.
38. **(Optional)** To configure optional Avaya Workspaces, select the **Workspaces** tab. See [Configuring Avaya Workspaces during the initial installation](#) on page 362 for configuration details.
39. Select the **Security Configuration** tab, and configure the security details in the **Security Store Details** section.

The screenshot shows the 'Avaya Contact Center' configuration interface. The 'Configuration Data' section is active, with the 'Security Configuration' tab selected. The 'Security Store Details' section contains fields for 'Full Computer Name (FQDN)' (CC7SIP.aaccdomain.com), 'Encryption Algorithm Level' (SHA256), 'Key Size' (2048), 'Security Store Password', and 'Confirm Store Password'. The 'Name of Organizational unit' and 'Name of Organization' fields are empty. The 'City or Locality' and 'State or Province' fields are also empty. The 'Two letter country code' field is empty. The 'Subject Alternative Name' section has a 'Type' dropdown set to 'DNS' and a 'Value' field. There are 'Add' and 'Remove' buttons. A 'Create Store' button is at the bottom right. A 'Skip Security Configuration' checkbox is at the bottom left. Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom.

40. If you do not want to enable security, select the **Skip Security Configuration** checkbox and skip to step [56](#) on page 228.

! Important:

A warning message appears. If you proceed without enabling security, you cannot fully commission your solution. The SIP CTI link is disabled until you configure Contact Center TLS certificates to communicate securely with Application Enablement Services.

41. In the **Full Computer Name (FQDN)** box, type the full FQDN of the server on which you are creating the security store.

! Important:

The FQDN must be the full machine name of the server that the Security Store resides on. The FQDN name is case-sensitive.

42. In the **Name of Organizational unit** box, type the name of the department or division within the company.
43. In the **Name of Organization** box, type the company name.
44. In the **City or Locality** box, type the name of the city or district in which the contact center is located.

45. In the **State or Province** box, type the state or province in which the contact center is located.
46. In the **Two Letter Country Code** box, type the country code in which the contact center is located.
47. In the **Security Store password** box, type a password for accessing the new security store.
48. In the **Confirm Store password** box, confirm the password for accessing the new security store.

 **Important:**

Ensure you remember this password, because you need it when you log on to Security Manager after install. If you forget the password, you cannot access Security Manager.

49. If you are implementing High Availability in the contact center, generate the security store using Subject Alternative Names (SANs). In the **Subject Alternative Name** section, for each SAN you want to add:
 - a. From the **Type** drop-down list, select DNS.
 - b. In the **Value** field, type the FQDN for the server.
 - c. Click **Add**.

For a High Availability system, add the current server FQDN and the Managed name for the HA pair.

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

The default value for **Encryption Algorithm** is SHA256 and the default value for **Key Size** is 2048.

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

51. Click **Create Store**.
52. You can now use the **Security Configuration** tab to create and save a Certificate Signing Request (CSR) file.

The screenshot shows the 'Avaya Contact Center' configuration interface. The 'Configuration Data' section is active, with the 'Security Configuration' tab selected. The page title is 'Configuration Data' with the Avaya logo. Below the title, it says 'Enter the required configuration data.' The tabs are 'Core', 'Licensing', 'SIP', 'Multimedia', and 'Security Configuration'. The main content area is titled 'Store created – Generate Identity Security Certificate by signing the Certificate Signing Request provided.' It contains a 'Certificate Signing Request file' section with a 'Create CSR File' button. Below this is an 'Add' button and a section for 'Imported Trusted Certificate Authority Root Certificate(s)' with a 'Remove' button. There is also a section for 'Imported Identity Security Certificate' with a 'Remove' button. On the right, a 'Status' box contains instructions: 'Ensure that a removable or network drive is available.', 'Create the Certificate Signing Request file and save it to a removable or network drive.', and 'Alternatively, to defer Security Configuration and continue with the Installation Wizard.' There is a 'Reset' button in the status box. At the bottom, there are navigation buttons: '< Back', 'Next >', and 'Cancel'. A 'Click Next to Continue' link is also present.

53. Click **Create CSR File**.

54. From the **Save In** drop-down list, select a shared location in which to save the CSR file and click **Save**.

You must now send the Certificate Signing Request file to a Certificate Authority and receive a signed certificate and root certificate to import to the security store.

55. Click **Add** to import certificates. In the **Open** dialog box, navigate to the location of a certificate and click **Open**. To remove the imported certificate, select the required certificate from the list and click **Remove**.

You can import either a chained certificate, or separate root and signed certificates. Root certificates appear in the **Imported Trusted Certificate Authority Root Certificate(s)** section. A signed certificate appears in the **Imported Identity Security Certificate** section.

If a chained certificate contains both root and signed certificates, you can add root certificates and signed certificate simultaneously by importing just one chained certificate.

If a chained certificate contains root certificates only, you can use the chained certificate to add all root certificates at a time. To add a signed certificate, click **Add** and navigate to the required signed certificate.

If you have separate root and signed certificates, you must add them one by one by clicking the **Add** button. Always add a signed certificate last.

! Important:

When adding a chained certificate, the system can prompt you to enter the password you have created for accessing the security store. See step [47](#) on page 226.

56. Click **Next**.
57. Review and verify the summary information and click **Configure**.
58. After the installation is complete, click **Finish**.
59. If prompted, restart the server.

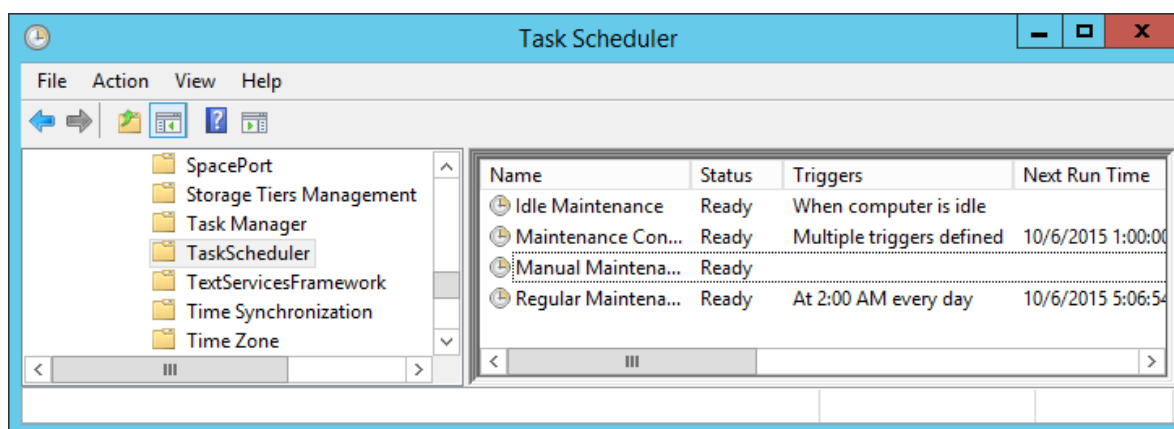
Enabling Windows Server Automatic Maintenance

About this task

Enable Windows Server Automatic Maintenance after deploying Contact Center software.

Procedure

1. Log on to the Contact Center server as an administrator.
2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Enable**.
5. In the **Name** column, right-click **Regular Maintenance** and then click **Enable**.



6. From the **File** menu, click **Exit**.

Backing up the new Avaya Aura® Contact Center Release 7.1 databases

About this task

After running the Ignition Wizard, backup the Avaya Aura® Contact Center Release 7.1 databases.

The backup databases capture the system in a known clean state and these might be required later if issues arise during data migration.

Procedure

1. Log on to the new Avaya Aura® Contact Center Release 7.1 server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
4. In the right pane, click **Create**.
5. From the **Drive Letter** list, select the network drive on which to store the databases.
6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.
7. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the user password.
9. Click **Save**.
10. Click **OK**.
11. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
12. In the **Media Type** section, select **Network Location**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.
15. Click **Yes**, to continue with the backup.

Turning off Web Services security

About this task

Turn off Web Services security before you restore a CCMM database from a system that did not have security enabled. If you are migrating from an Avaya Aura® Contact Center Release 7.x system that has Web Services security turned on, you can skip this procedure.

Before you begin

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

Procedure

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

Important:

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

2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. On the Store Access dialog, type the password for the security store, and click **OK**.
4. On the Security Manager screen, select the **Security Configuration** tab.
5. Click **Security Off**.
6. Click **Apply**.
7. On the Security Change Confirmation dialog, click **Confirm**.
8. Click **Log Out**.
9. Restart the Contact Center server.

Next steps

Complete the migration procedures in this book. After the migration, to complete your security configuration, follow the procedures in *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* or *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000*.

Restoring the Database Integration Service configuration

About this task

If you backed up the Database Integration Service configuration on your old server, restore the configuration to the registry on the new server. Contact Center automatically copies the configuration from the registry into the database on the next restart.

Procedure

1. On the Contact Center server, on the **Desktop** screen, right-click **Start** and select **Run**.
2. Type `regedit`.
3. Click **OK**.
4. On the **Registry Editor** dialog box, click **File** > **Import**.
5. On the **Import Registry File** dialog box, select the HAI configuration file that you saved from the old server.

6. Click **Open**.
7. On the **Registry Editor** message box, click **OK**.

Next steps

If you used custom DSNs in the Database Integration Service configuration on your old server, you must manually re-configure these DSNs on the new server.

Restoring the Voice and Multimedia Contact Server Release 7.1 databases

Before you begin

- Back up the old Voice and Multimedia Contact Server databases.
- On the new server, map a drive to the Voice and Multimedia Contact Server database backups.

Important:

When you migrate configuration information from the old server to the new server, do not run the two application servers simultaneously. Both applications are configured the same, so they attempt to access and control the same resources. Continuing to run the old applications in the Contact Center can result in unpredictable behavior.

About this task

Restore the Voice and Multimedia Contact Server Release 7.1 databases. After you complete this procedure, you must restart your server.

Important:

You must complete this procedure to ensure all databases are restored at the same time.

Procedure

1. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
2. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the Backup Locations pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which you stored the Voice and Multimedia Contact Server database backup.
5. In the **UNC Path** box, type the location of the Voice and Multimedia Contact Server databases in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.

8. Click **Save**.
9. Click **OK**.
10. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Restore**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Application** section, select **CCT**, **CCMS**, **CCMM**, **ADMIN**, and **CCMA**.
13. In the **Restore contents** section, select **Data** and **Offline**.
14. From the **Backup Location** list, select the network drive containing the backed up Contact Center server databases.
15. Click **Restore**.
16. Use the **Progress information** field to monitor the progress of the restoration.
17. On the **Database Maintenance** message box, click **OK**.
Wait for the restore to complete.
18. From the **Start** menu, in the Avaya area, click **Server Configuration**.
19. In the Server Configuration dialog box, click **Apply All**.
20. Click **Yes** to restart Contact Center.

Logging on to Avaya Aura® Media Server Element Manager

Before you begin

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

About this task

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

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

Note:

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

Procedure

1. Start a Web browser.

2. In the address box, type the following URL:

`https://SERVER_IP_ADDRESS:8443/em`

Where `SERVER_IP_ADDRESS` is the IP address of the Avaya Aura® Media Server.

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

Restoring the Avaya Aura® Media Server database

About this task

Restore the Avaya Aura® Media Server database backup data to the new server.

Important:

Perform this procedure only if you are migrating from an existing Avaya Aura® Contact Center Release 7.x system.

Procedure

1. Access the Element Manager with Administrator privileges.
2. Expand **Tools**.
3. Expand **Backup and Restore**.
4. Select **Restore**.
5. On the Restore window, from the **Restore Source** list, select **Upload Backup Files**.
6. Click **Browse**.
7. Select the Avaya Aura® Media Server backup that you want to restore.
8. Click **Upload Files**.
9. On the **Confirm Restore** page, review the information and click **Confirm** to proceed with the restore.
10. After the restore completes, exit Element Manager.
11. Reboot the Avaya Aura® Media Server server.

Resetting the Avaya Aura® Media Server IP address in Element Manager

About this task

When you migrate Avaya Aura® Media Server to a server with a different IP address, the Avaya Aura® Media Server database contains the IP address of the old server. You must update the IP address in Element Manager to make all administration functions work correctly.

Procedure

1. Log on to Avaya Aura® Media Server Element Manager with administrative privileges.
2. In the left pane, select **System Configuration > Network Settings > IP Interface Assignment**.
3. Under **IPv4 Interfaces**, set the **Signaling**, **Media**, and **Cluster** boxes to the IP address of the new server.
4. Click **Save**.

Restoring the Avaya Aura® Media Server default license

About this task

Restore the Avaya Aura® Media Server default license using Element Manager.

Procedure

1. Log on to Avaya Aura® Media Server Element Manager with administrative privileges.
2. In the left pane, select **Licensing > General Settings**.

The screenshot shows the Avaya Aura® Media Server Element Manager interface. The left navigation pane is expanded to show the 'Licensing' section, with 'General Settings' selected. The main content area displays the 'General Settings' page for Licensing. The 'Licensing' dropdown is set to 'WebLM Server'. The 'Server Host Name or IP Address' field contains 'localhost'. The 'Server Port' field contains '52233'. The 'URL Suffix' field contains '/WebLM/LicenseServer'. There is an 'Open WebLM Server' button. At the bottom of the form are 'Save', 'Cancel', and 'Restore Defaults' buttons.

3. Click **Restore Defaults**.
4. Click **Confirm**.

Restoring the Voice and Multimedia Contact Server databases

Before you begin

- Back up the old Voice and Multimedia Contact Server databases.
- On the new server, map a drive to the Voice and Multimedia Contact Server database backups.

Important:

When you migrate configuration information from the old server to the new server, do not run the two application servers simultaneously. Both applications are configured the same, so they attempt to access and control the same resources. Continuing to run the old applications in the Contact Center can result in unpredictable behavior.

About this task

Restore the Voice and Multimedia Contact Server databases to the new server. The Database Maintenance utility can restore all application databases at one time. Restore the data for the CCMS, CCT, and CCMM databases. You must restore the CCMS, CCT, and CCMM databases as a matched set, and all databases must be stored in the same backup location.

Procedure

1. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
2. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the Backup Locations pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which you stored the Voice and Multimedia Contact Server database backup.
5. In the **UNC Path** box, type the location of the Voice and Multimedia Contact Server databases in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.
9. Click **OK**.
10. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Restore**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Application** section, select **CCT**, **CCMS**, and **CCMM**.
13. In the **Restore contents** section, select **Data**. If you are restoring an AACC Release 6.4 database, select **Offline** also.

14. From the **Backup Location** list, select the network drive containing the backed up Voice and Multimedia Contact Server databases.
15. Click **Restore**.
16. Click **Yes**.
17. Use the **Progress information** field to monitor the progress of the restoration.
18. On the **Database Maintenance** message box, click **OK**.
19. From the **Start** menu, in the Avaya area, click **Server Configuration**.
20. In the **Server Configuration** dialog box, click **Apply All**.
21. Click **Yes** to restart Contact Center.

Restoring Contact Center Manager Administration data

Before you begin

- Know the network location (in Universal Naming Convention (UNC) format) of the drive for the backed up data.

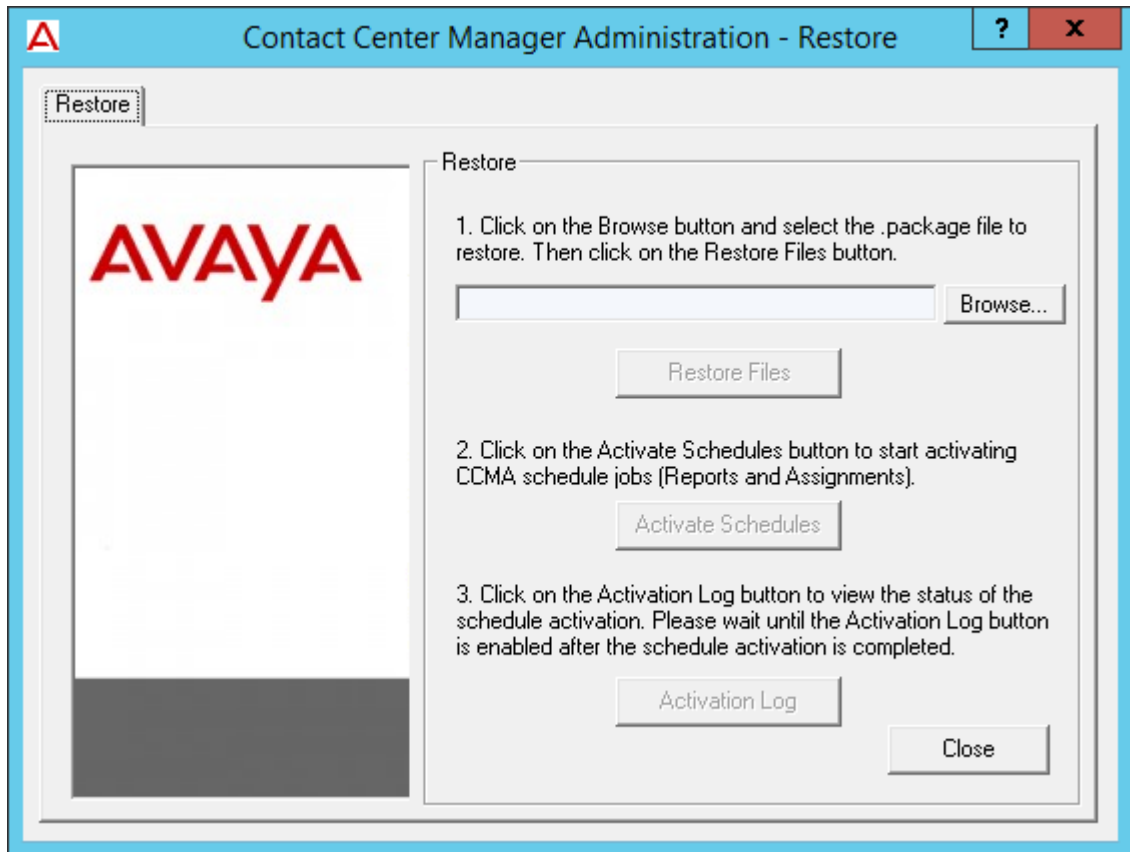
About this task

Restore the Contact Center Manager Administration data to migrate the data to the new server. Use this procedure if you are restoring Avaya Aura® Contact Center Contact Center Manager Administration data. You must restore the CCMA database as part of a matched set; the CCMA data must be restored to the same server as its corresponding databases (for example, CCMS, CCT, or CCMM).

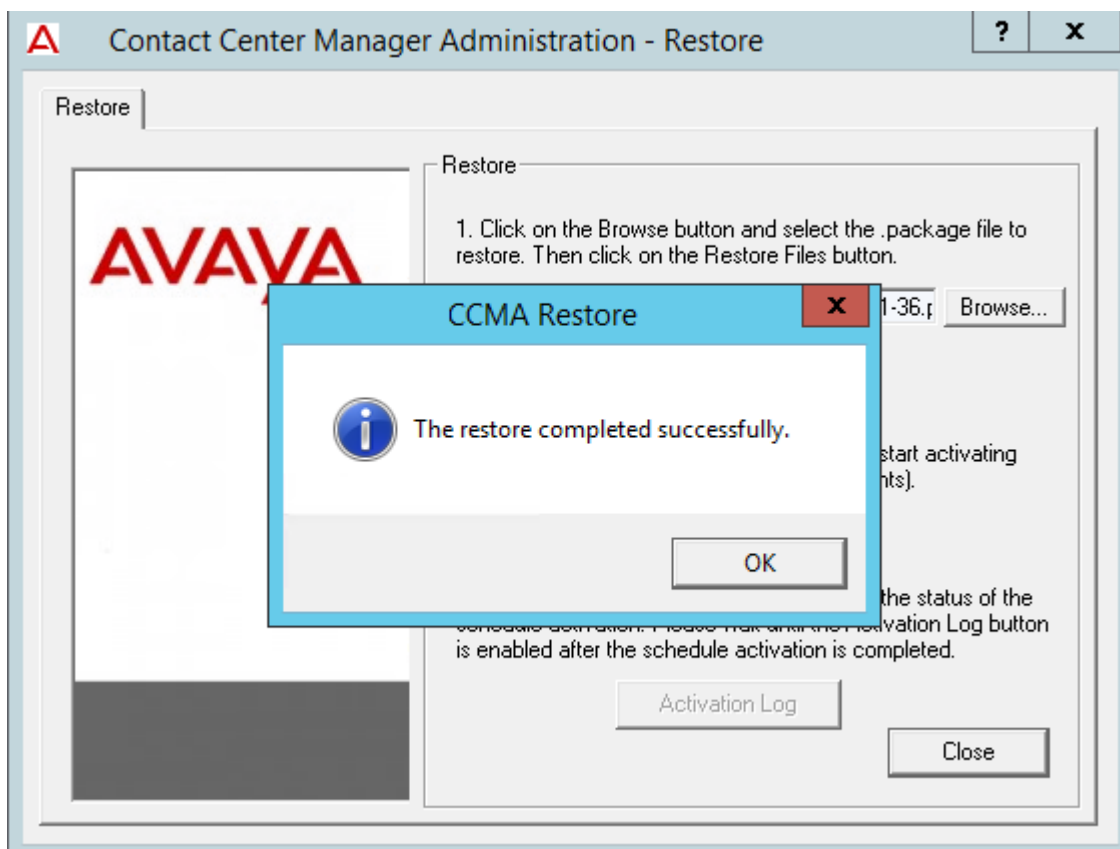
Procedure

1. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.
2. In the left pane of the Avaya Configuration window, expand **Avaya > Applications > Restore**.
3. In the right pane, click **Restore**.
4. On the **Restore** message box, click **OK**.

5. In the **Contact Center Manager Administration - Restore** dialog box, click the **Restore** tab.



6. To select a backup file to restore from, click **Browse**.
 7. In the **Select a backup file** dialog box, select the required .package file.
 8. Click **Open**.
 9. To restore the backup file data onto the administration data server, click **Restore Files**.
- The restore completed successfully message box appears.



10. Click **OK**.

Upgrading the Contact Center Manager Administration data

Before you begin

- Restore the backed up Contact Center Manager Administration (CCMA) data.

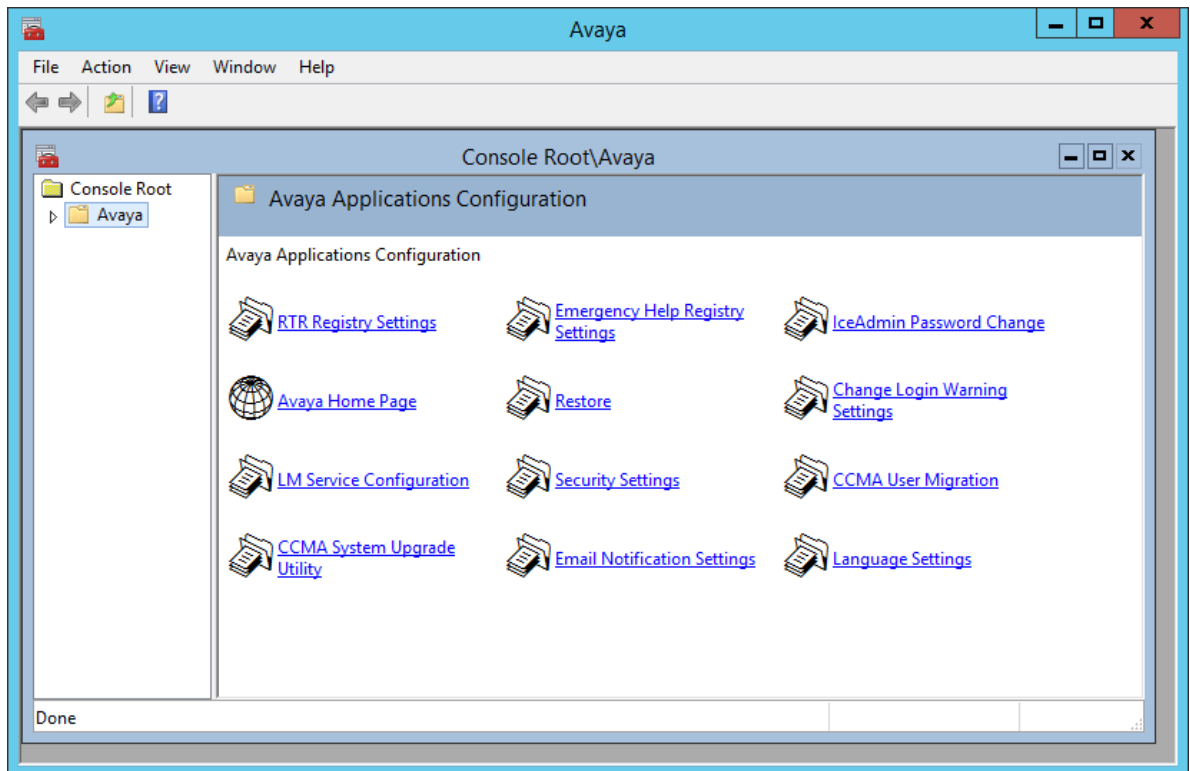
About this task

Upgrade Contact Center Manager Administration (CCMA) data to the Intersystems Caché database format used by Avaya Aura® Contact Center Release 7.1.

Procedure

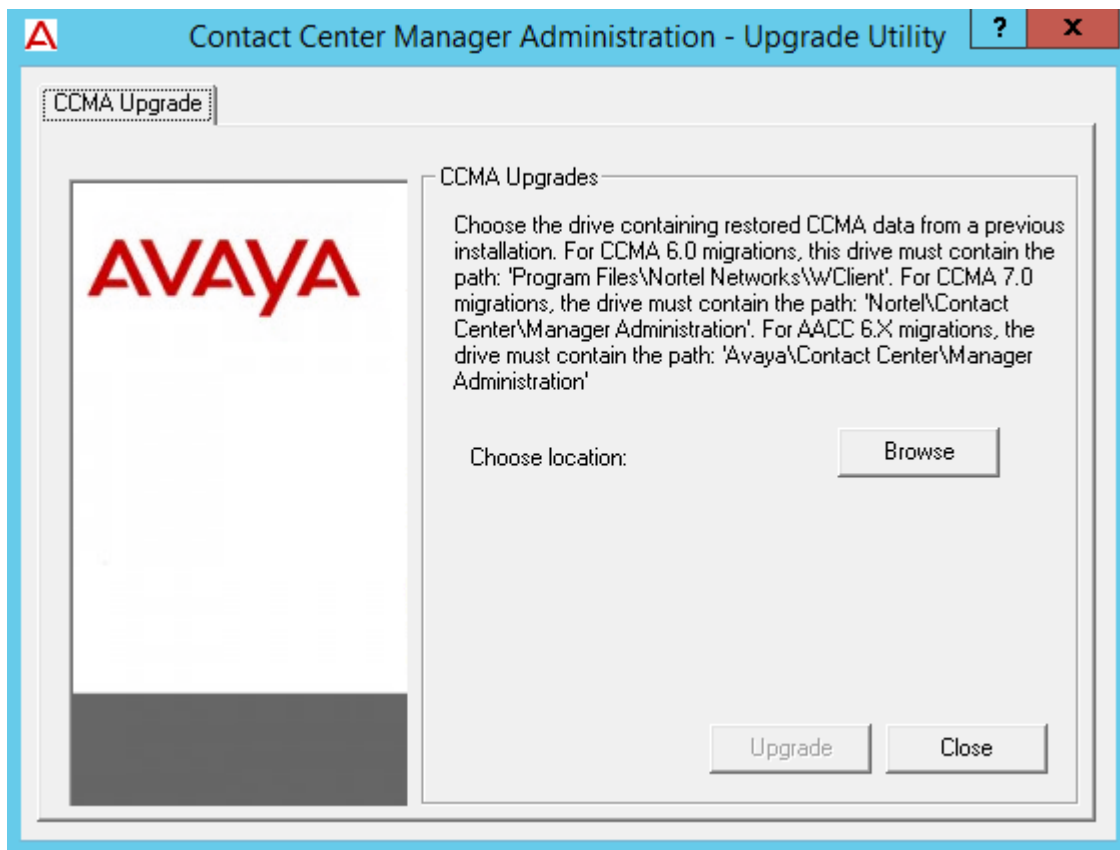
1. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.

2. In the left pane, click **Avaya** > **Applications** > **CCMA System Upgrade Utility**.



3. In the right pane, click **CCMA System Upgrade Utility**.

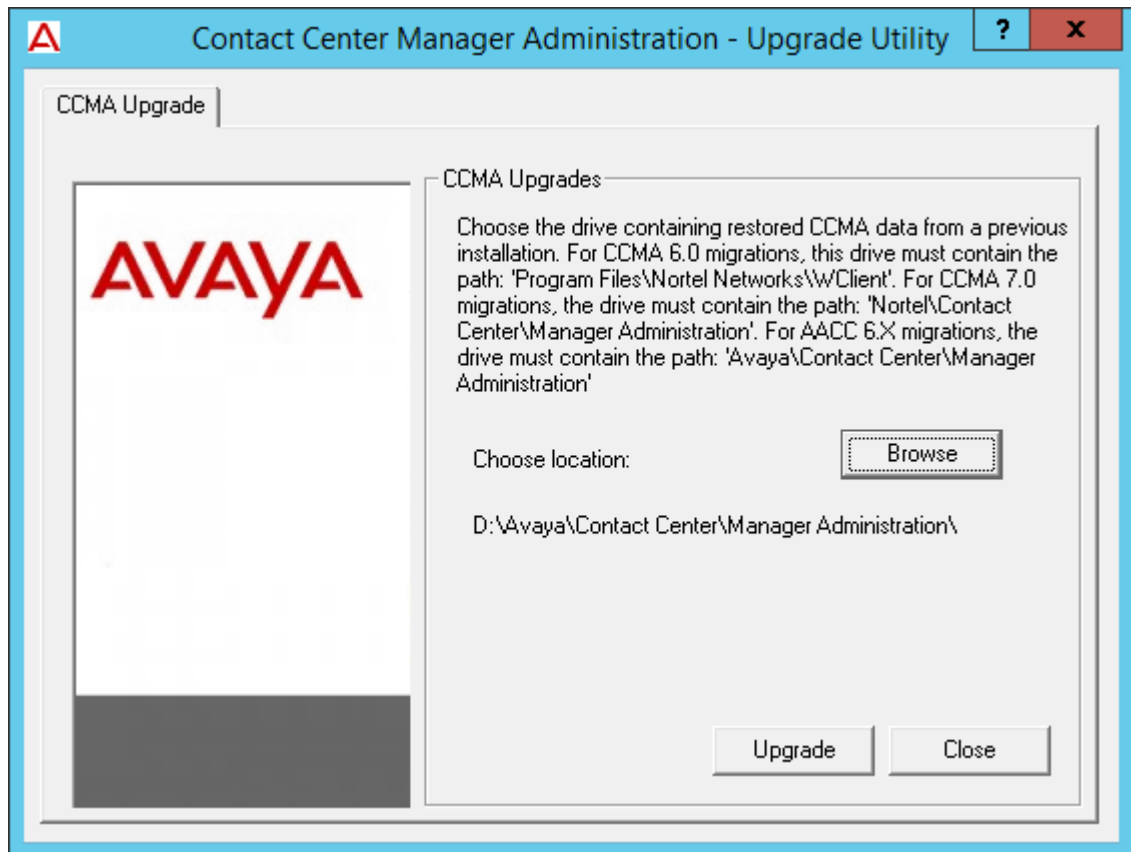
4. Click **Yes** on the confirmation dialog box.



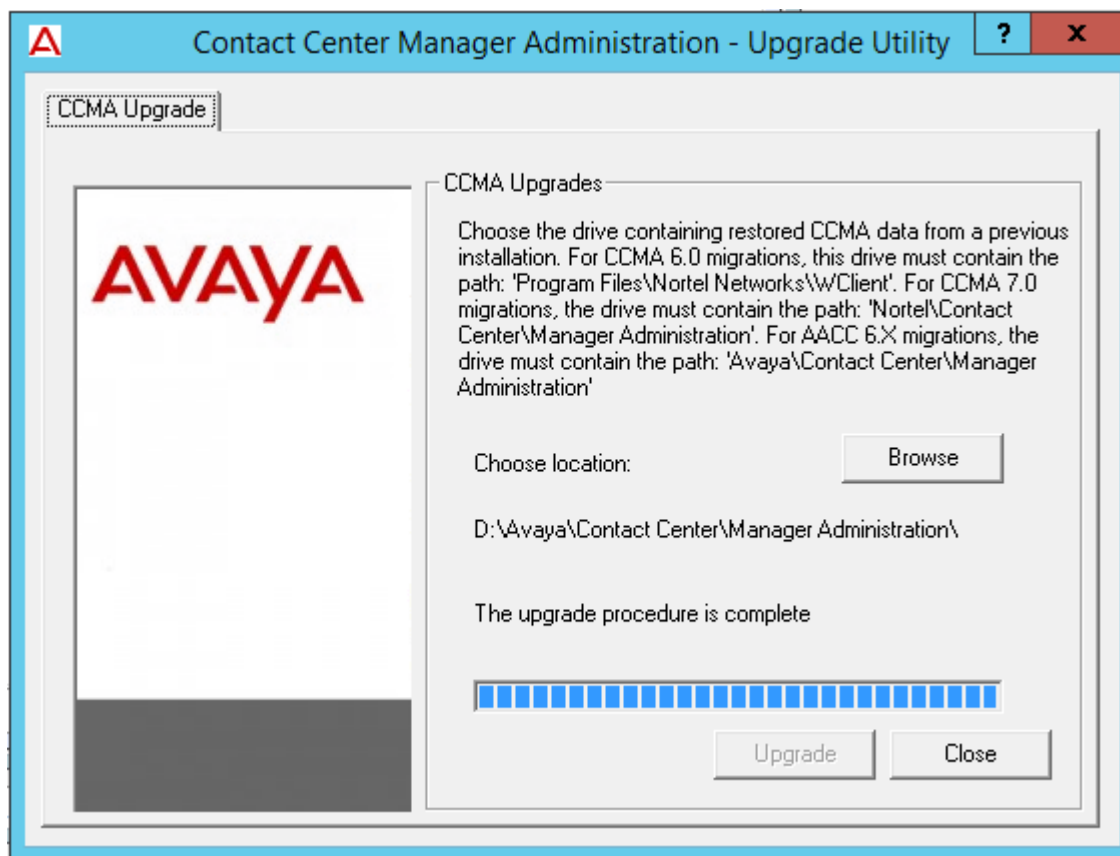
5. On the Upgrade Utility, click **Browse** and follow the instructions on the **CCMA Upgrades** screen to choose a location.

Select only the drive letter as the location of the restored CCMA data. The upgrade utility automatically detects and appends the correct directory structure for the old system data.

Example of upgrading from an Avaya Aura® Contact Center Release 6.4 system:



6. Click **Upgrade**.



7. Close the Upgrade Utility application. Click **Close**.

Migrating the Avaya Media Server database

About this task

Migrate the old Avaya Media Server backup data to the data format used by the current release of Avaya Aura® Media Server.

Procedure

1. Copy the Avaya Media Server backup Application Content file to the new Avaya Aura® Media Server server. The backup file name derives from the name that you entered in Element Manager for the backup task.
2. Using an SSH client, log on to the new Avaya Aura® Media Server server Linux shell console using the *cust* account.
3. Using the command line, navigate to the folder containing the backup file.
4. Upgrade and restore the backup. On the command line, enter:

```
amsupgrade <backupfile name>
```

Where `<backupfile name>` is the Avaya Media Server backup Application Content file.

5. After the upgrade utility completes, reboot the Avaya Aura® Media Server server.

Completing the Avaya Aura® Media Server on Linux Content Store

Before you begin

- Read the Avaya Aura® Contact Center Release Notes.
- This procedure requires `sroot` access. Obtain Enhanced Access Security Gateway (EASG) access to Avaya Aura® Media Server so that you can log on as `sroot`. For more information about enabling EASG, see *Deploying and Updating Avaya Aura® Media Server Appliance* or Avaya Aura® Media Server Release Notes.
- Obtain the most recent version of the Avaya Aura® Contact Center Release 7.1 DVD. Read the Avaya Aura® Contact Center Release Notes to ensure that you are using the most recent version of Avaya Aura® Media Server software.

About this task

Complete the Avaya Aura® Media Server Content Store data upgrade or migration process. This procedure removes any music content groups from the SIP domain namespace that are duplicated in the *streamsource* namespace.

Alternatively, you can choose to manually remove any music content groups from the SIP domain namespace that are duplicated in the *streamsource* namespace. For more information, see Avaya Aura® Contact Center Release Notes.

Procedure

1. Obtain the most recent version of the Avaya Aura® Contact Center Release 7.1 DVD.
2. Insert the DVD into the DVD drive of your desktop computer.
3. On your desktop computer, navigate to the `\\Install Software\AMS\Linux` folder on the DVD.
4. Using a Secure Copy (SCP) utility, configured to use a *Text* transfer mode, copy the `completeAAMS77Migration.py` script from the DVD to the existing Avaya Media Server Linux server. Copy the script file using *Text* transfer mode. Do not copy the script file using *Binary* transfer mode.
5. On your Linux server, use the `su` command to change to the `sroot` user account. For example:


```
su - sroot
```
6. On your Linux server, navigate to the folder containing the `completeAAMS77Migration.py` shell script.

7. Start the python script. For example,

```
python completeAAMS77Migration.py
```

The utility completes the Avaya Aura® Media Server Content Store data migration or upgrade.

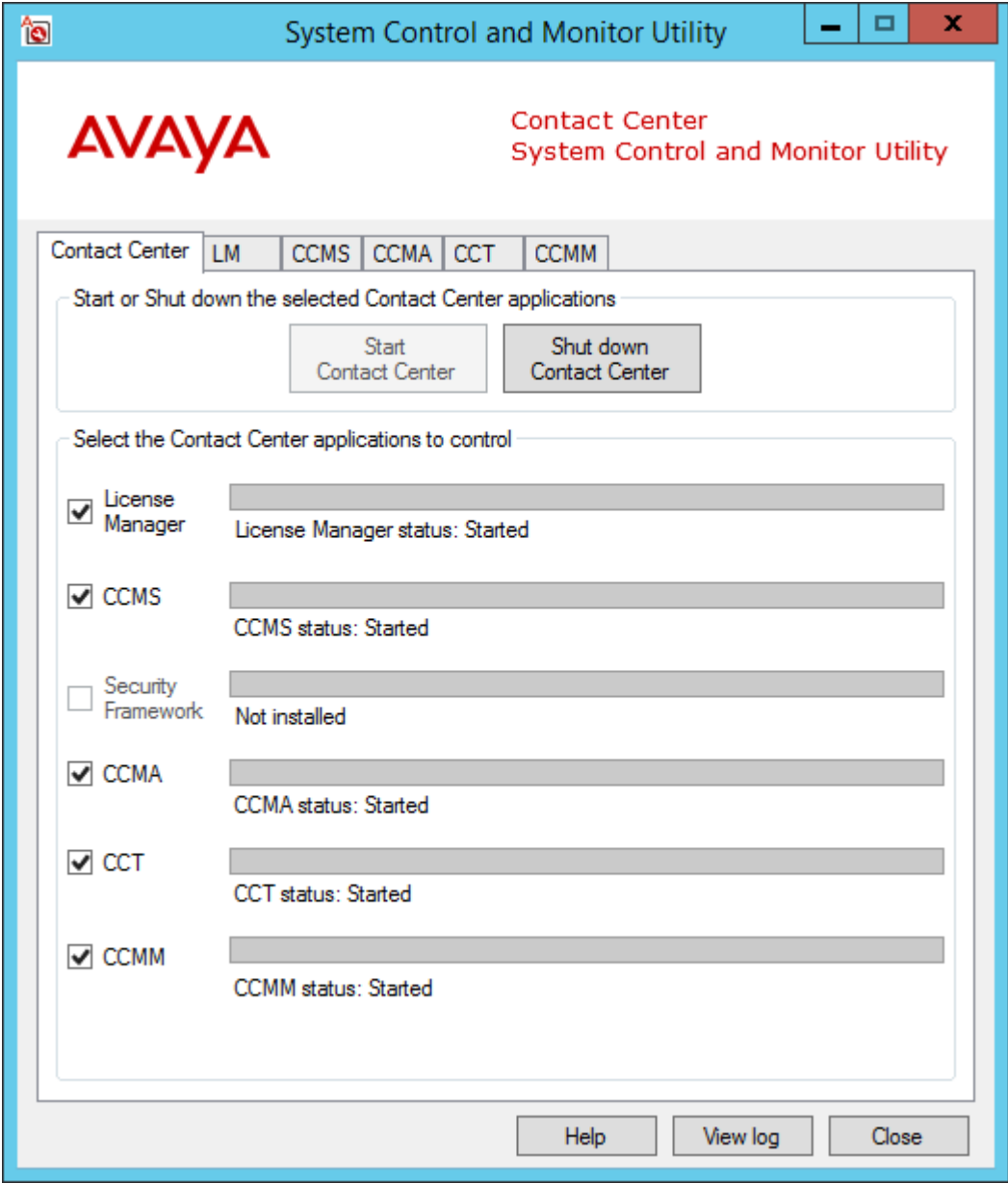
Starting Contact Center services

About this task

Start the Contact Center services to begin re-configuration after migrating or upgrading a system. The database restore and upgrade utilities automatically stop Contact Center services. Start Contact Center services to continue commissioning the solution.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **System Control and Monitor Utility**.
3. Click the **Contact Center** tab.
4. Click **Start Contact Center**.



Wait for Contact Center services to start.

Configuring the Contact Center Manager Administration system components

About this task

Configure the Contact Center Manager Administration (CCMA) system components for the new solution. Ensure the Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), and Contact Center Multimedia (CCMM) settings are correct for the new solution.

To access CCMA and other Contact Center components, you must use the Microsoft Edge browser in Internet Explorer mode.

Procedure

1. In your browser, type the URL of the server and then press **Enter**.
The default URL is `https://<server name>`, where `<server name>` is the host name of the Avaya Aura® Contact Center Release 7.1.x server. If you turned off Web Services security, use `http://<server name>`.
2. On the main login page, in the **User ID** field, type the username.
The default user ID is `webadmin`.
3. In the **Password** box, type the password.
The default password is `webadmin`.
4. Click **Log In**.
5. On the launchpad, click **Configuration**.
6. In the left pane, right-click the CCMS server name and then click **Edit Properties**.
7. Update the Contact Center Manager Server details to match your new solution and then click **Submit**.
8. In the left pane, right-click the CCMS server name and then click **Refresh Server**.
9. On both Contact Center Manager Administration dialogs, click **Yes**.
10. In the left pane, right-click **CCT** and then click **Edit Properties**.
11. Update the Communication Control Toolkit details to match your new solution and then click **Submit**.
12. In the left pane, right-click **CCMM** and then click **Edit Properties**.
13. Update the Contact Center Multimedia details to match your new solution and then click **Submit**.
14. Log off from CCMA.
15. Using the System Control and Monitor Utility (SCMU), restart Avaya Aura® Contact Center services.

Configuring the Contact Center Multimedia new details

About this task

Configure the Contact Center Multimedia (CCMM) Dashboard and Administration details.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **Multimedia Dashboard**.
3. On the CCMM Dashboard, under **Server Availability**, right-click **Contact Center Manager Administration** and select **Edit**.
4. On the **Administrator Login** dialog, in the **User Name** box, type `GeneralAdmin`.
5. In the **Password** box, type the password. The default password is “__ccmm!”.
6. Click **Login**.
7. On the **Administrator Login** dialog, in the text box, type the name for the current Voice and Multimedia Contact Server.
8. Click **Save**.
9. Log on to the new Contact Center Manager Administration Web interface with administrative privileges.
10. On the **Launchpad**, click **Multimedia**.
11. In the left pane, select the Contact Center Multimedia to which you want to log on.
12. Under **CCMM Administration**, select **General Administration**.
13. Select **Server Settings**.
14. Update the server names to match the new Contact Center solution.
15. Under **CCMM Administration**, on the main menu, select **E-mail > General Settings**.
16. Under **Attachment Files**, ensure the **Inbound URL**, **Inbound Share**, **Outbound URL**, and **Outbound Share** locations match the new Contact Center solution.
17. Restart the Contact Center server.

Configuring Multimedia data management

About this task

When you migrate from a multimedia-enabled AACC Release 6.3 or earlier, Contact Center creates a new offline database and applies new data management tasks and utilities. To ensure efficient use of the Multimedia database drive on the new Contact Center server, configure Multimedia data management.

Procedure

Use the CCMM Data Management tool to create and schedule cleanup tasks to clear closed contacts from the MULTIMEDIA database. For more information on using the CCMM Data Management tool, see *Maintaining Avaya Aura® Contact Center*.

Configuring settings for Multimedia Complement for Elite server migration

About this task

If you are migrating from an existing Avaya Aura® Contact Center Multimedia Complement for Elite server, perform the following steps on the new Voice and Multimedia Contact Server to complete the migration.

Procedure

1. Update the Local Settings, SIP Network Settings, and SIP Local Subscriber data on the new server using the Server Configuration utility.
2. Ensure that the licensing details are configured correctly on the new server.
3. Log on to CCMA Configuration, right-click on each server and select **Edit Properties**. Update the server details for the new solution.
4. Open the CCMM Administration utility and perform the following steps:
 - a. Click **General Administration > Server Settings**. Ensure that the server details are correct for the new solution.
 - b. Click **E-mail > General Settings**. Ensure that the details are correct for the new solution.
5. Open the Multimedia Dashboard. Ensure that the Computer Name for the CCMA and CCMM servers are correct for the new solution.
6. Restart the server.
7. On each client computer, uninstall Agent Desktop. Install Agent Desktop using the new server name.

Note:

At this point in the migration, existing agents can process Multimedia contacts as before.

8. Using the Configuration Tool or CCMA Management, add a Voice URI for each agent and assign each agent to a voice skillset. After you reconfigure the agent details, agents must log out and log back on to complete these configuration changes.

+ Tip:

Use the Configuration Tool to perform a bulk change.

Converting custom RCW reports to Contact Center R7.1 format

About this task

Copy the zip file of converted RCW reports to the Contact Center R7.1 server, and convert each report to SSRS format.

Before you begin

Prepare the RCW reports for migration on the old server, and copy them to a network location.

Custom formulas do not migrate to the new server. If the original reports use custom formulas on the existing server, the formulas do not migrate with the custom reports.

Contact Center creates a placeholder formula for each custom formula. The placeholder displays an asterisk character on the migrated report. If possible, the placeholder formula includes the original Crystal Syntax formula text as a comment. You must edit the placeholder formulas, entering valid SSRS expressions for the formula text, to complete the migration. The placeholder formula is limited to 32,000 characters, so it is possible that very long formulas can be truncated.

Document all the custom formulas on the existing server, to assist with re-creating them on the new server after migrating the Contact Center databases.

Procedure

1. Log on to the Contact Center R7.1 server.
2. Run the RCW report utility `d:\avaya\contact center\manager administration\server\bin\MigrationRCWImporter.exe`
3. On the RCW Importer screen, click **Browse**, and browse to and select the zip file of converted RCW reports.
4. Click **Run** to start the conversion.
The RCW Importer utility unpacks the reports to the RCW\Private folder.
5. Log on to Contact Center Manager Administration.
6. On the **Launchpad**, click **Historical Reporting**.
7. In the left pane, click the Contact Center Manager Server.
8. From the **Report** menu, select **Report Creation Wizard**.
9. Select **Open Existing Report**.
10. For each `.rcwx` report in the list:
 - a. Select the report and click **Next**.

Contact Center opens the report in RCW.

- b. Click the **Preview Report** button.
- c. On the Preview Data Filter screen, click **Preview**.

Check that the report opens correctly in the preview.

- d. If you saw errors in the preview, correct the data fields and formulas as applicable.
- e. Click the **Save Report** button.
- f. On the Save RCW Report window, click **Save**.

Do not change the default file location: the .rdl file must save in the same location as the .rcwx file.

Contact Center saves the report in .rdl format.

Commissioning the Contact Center solution

About this task

Commission the Contact Center solution.

Procedure

1. After migrating your server and restoring the server databases, some of the old configuration settings might not match your new solution. Commission your new server in the new solution. For more information, refer to *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000* or *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications*.
2. Use the procedures in *Avaya Aura® Contact Center Server Administration* to configure your licensed features.

Chapter 12: Voice and Multimedia Contact Server with Avaya Aura® Media Server upgrade and patch installation

This chapter describes how to upgrade and install patches on the Voice and Multimedia Contact Server with Avaya Aura® Media Server server. Apply patches to resolve product issues.

You can patch Avaya Aura® Media Server using Avaya Aura® Media Server Quick Fix Engineering (QFE) patches. Avaya Aura® Media Server QFE patches are not installed or maintained by the Avaya Contact Center Update Manager, they are independent of Avaya Aura® Contact Center. You must always install QFE patches sequentially, as QFE patches are dependent on previous patches.

A Voice and Multimedia Contact Server with Avaya Aura® Media Server includes the following server software:

- Contact Center Manager Server (CCMS)
- Contact Center Manager Server Utility
- Contact Center License Manager (LM)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center Multimedia (CCMM)
- Avaya Aura® Media Server
- Avaya Workspaces (optional)

 **Note:**

Avaya Aura® Contact Center and Avaya Aura® Media Server have independent patches, service packs, readme files, upgrade procedures, and naming conventions.

Complete the procedures in this section in sequential order.

Voice and Multimedia Contact Server with Avaya Aura® Media Server patch installation prerequisites

- If you are upgrading to Avaya Aura® Contact Center Release 7.0 Feature Pack 3 or later, you must enable CPU Virtualization or Virtualization Technology in the Windows server BIOS on your Voice and Multimedia Contact Server with Avaya Aura® Media Server. The available virtualization settings can vary by server manufacturer and BIOS version. Refer to the server manufacturer's documentation to determine which virtualization settings to configure.
- Download the most recent documentation. See [Downloading the most recent documentation](#) on page 45.
- Download and review the latest Avaya Aura® Contact Center Release Notes. The Release Notes contain information about known issues, patches, and workarounds specific to a release and patch line-up of Contact Center. For more information about the Contact Center Release Notes, see the Avaya website (<http://support.avaya.com>).

Disabling Windows Server Automatic Maintenance

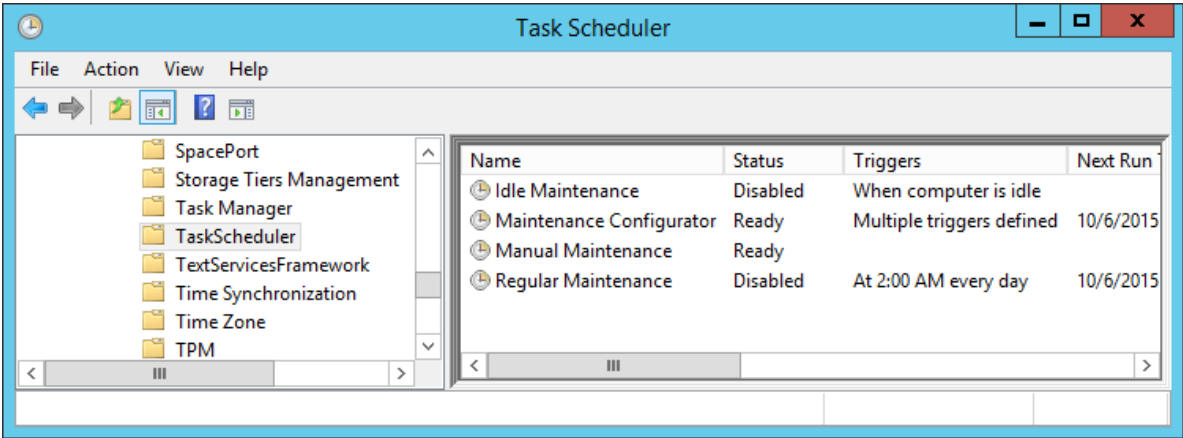
About this task

Disable Windows Server Automatic Maintenance while updating Contact Center software. Windows Server Automatic Maintenance can occasionally interfere with the real-time requirements for Contact Center. You must therefore temporarily disable Automatic Maintenance to update Contact Center software. Re-enable it after the update.

Procedure

1. Log on to the Contact Center server as an administrator.
2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Disable**.

5. In the **Name** column, right-click **Regular Maintenance** and then click **Disable**.



6. From the **File** menu, click **Exit**.

Installing Voice and Multimedia Contact Server with Avaya Aura® Media Server Release Packs, Feature Packs and Service Packs

Before you begin

- Download the most recent Contact Center Release Pack, Feature Pack and Service Packs.
- Download the most recent Contact Center software patches.
- Back up the Contact Center databases.
- Temporarily stop Microsoft Windows Server Automatic Maintenance while you update Voice and Multimedia Contact Server software.
- Avoid installation from shared locations, because it might lead to installation failure. To ensure successful installation, mount the Release Bundle or install it locally.

About this task

Install the most recent Voice and Multimedia Contact Server with Avaya Aura® Media Server Release Packs, Feature Packs and Service Packs to take advantage of new features, and to ensure that you have the most current application updates. When you install Avaya Aura® Contact Center Release 7.0 Feature Pack 3 or later from a previous release, the Contact Center Update Configurator utility updates Avaya Aura® Media Server to the latest supported version and applies all necessary configuration.

From Release 7.0 Feature Pack 3, on a Voice and Multimedia Contact Server with Avaya Aura® Media Server, the Linux version of Avaya Aura® Media Server is installed on a Hyper-V instance on Microsoft Windows Server.

 **Important:**

- The Update Configurator utility runs only when upgrading from Release 7.0 Feature Pack 2 or earlier.
- If you are upgrading from Release 7.0 Feature Pack 3 or later, you must upgrade Avaya Aura® Media Server manually using the OVA upgrade procedure. For more information, see [Updating Avaya Aura Media Server OVA to Release 7.1](#) on page 294.

Procedure

1. Open the Release Pack, Feature Pack or Service Pack ZIP file.
2. Browse to the Avaya Release Pack Installer directory.
3. Double-click `setup.exe`.

Contact Center displays the Contact Center Release Pack Installer screen.

4. If you downloaded GA patches along with the Release Pack:
 - a. Select **Yes**.
 - b. Click **Browse**.
 - c. On the Browse for Folder screen, browse to the folder where you downloaded the patches, and click **OK**.
5. **(Optional)** If you want to configure Avaya Workspaces, select **Yes** and select a drive from the drop-down list.
6. On the Contact Center Release Pack Installer screen, click **Next**.
7. On the Avaya Global License Terms screen, click **I ACCEPT THE LICENSE TERMS**.
8. On the MICROSOFT SOFTWARE LICENSE TERMS screen, click **I ACCEPT THE LICENSE TERMS**.

The Release Pack Installer shuts down Contact Center and installs the Feature Pack or Service Pack.

9. When the software update completes successfully, click **Restart**.
Contact Center reboots the server.
10. When Contact Center starts, the Contact Center Update Configurator opens.
11. In the **IP Address** box, type the IP address of the Avaya Aura® Media Server.

 **Important:**

You must ensure that this IP address is not in use, and must be in the same subnet as the Contact Center server.

12. In the **Password** box, type a password for the Avaya Aura® Media Server *cust* account.
13. In the **Confirm Password** box, re-type the password.
14. **(Optional)** To configure optional Avaya Workspaces, use the following procedure:
[Configuring Avaya Workspaces using the Update Configurator](#) on page 365.

15. Click **Configure**.

Result

When the Contact Center Update Configurator completes, click **Yes** to restart the server.

Next steps

Configure Avaya Aura® Media Server name resolution to ensure that Avaya Aura® Media Server can resolve the hostname and Fully Qualified Domain Name (FQDN) of the CCMA server. For more information about Avaya Aura® Media Server name resolution, see *Avaya Aura® Contact Center Server Administration*.

Installing Voice and Multimedia Contact Server software patches

Before you begin

- Download the most recent Contact Center patches.
- Ensure that you have a recent backup of the Contact Center databases. Avaya recommends that you schedule a daily backup of the Contact Center databases at an off peak time. For more information on scheduling backups, see *Maintaining Avaya Aura® Contact Center*.
- Temporarily stop Microsoft Windows Server Automatic Maintenance while you update Voice and Multimedia Contact Server software.

About this task

Install the most recent Voice and Multimedia Contact Server software patches to ensure that you have the most current application updates.

Procedure

1. From the **Start** menu, in the Avaya area, click **Update Manager**.
2. Click **Install**.
3. Click **Browse** and navigate to the folder where you downloaded the patches.
4. Click **Scan for Updates**.

The Contact Center Updates section displays the available patches.

5. Select the appropriate patches.
6. Click **Install Selected Updates**.

The Update Manager installs the patch and displays a confirmation message.

7. Click **Close**.
8. Verify that the newly installed patch appears under **Installed Updates**.

9. If the System Management and Monitoring Component (SMMC) is installed on the server, verify that it starts. For more information about starting SMMC, see [Starting SMMC](#) on page 358.

Next steps

Re-enable Microsoft Windows Server Automatic Maintenance.

Installing Avaya Aura® Media Server patches on Linux

Before you begin

- Download the most recent Avaya Aura® Media Server QFE patches and store them in the QFE subdirectory. QFE patches are ZIP files, but do not unzip them. The Avaya Aura® Media Server patching utility uses the QFE ZIP files. For a Linux server, the default QFE folder location is `/opt/avaya/app/amsinst/ma/MAS/qfe`.
- Back up Avaya Aura® Media Server before applying patches.

About this task

Install a new QFE patch to apply a change to the Avaya Aura® Media Server system.

Review *Avaya Aura® Contact Center Release Notes* and follow the instructions in each Avaya Aura® Media Server patch Readme file.

Procedure

1. Navigate to Element Manager for the Avaya Aura® Media Server node you want to patch.
2. In the navigation pane, click **System Status** > **Element Status**.
3. Click **Stop** and confirm the operation on the following page.
4. Close Element Manager.
5. Open a Linux terminal on the server you want to patch.
6. Change to the root user by running the `su -` command.
7. Run the `amspatch list all` command to obtain the correct name for the new QFE patch:

The name of the file is not necessarily the same as the name of the patch.

8. Under the **QFE Name** column, note the name of the patch.
9. Install the patches in numerical order.
 - To install a new patch on the system, run the `amspatch apply <patchname>` command, where `<patchname>` is the name of the patch.
 - To install all downloaded QFE patches on the system, run the `amspatch apply all` command.

10. When the patch application is complete, open the Element Manager navigation pane, and click **Tools > Software Inventory**.
11. Verify the patch version listed in the **Patch Level** column.
12. Navigate to **System Status > Element Status** and then click **Start**.
13. Confirm the operation.
14. Navigate to **System Status > Alarms** and check for service-impacting alarms.

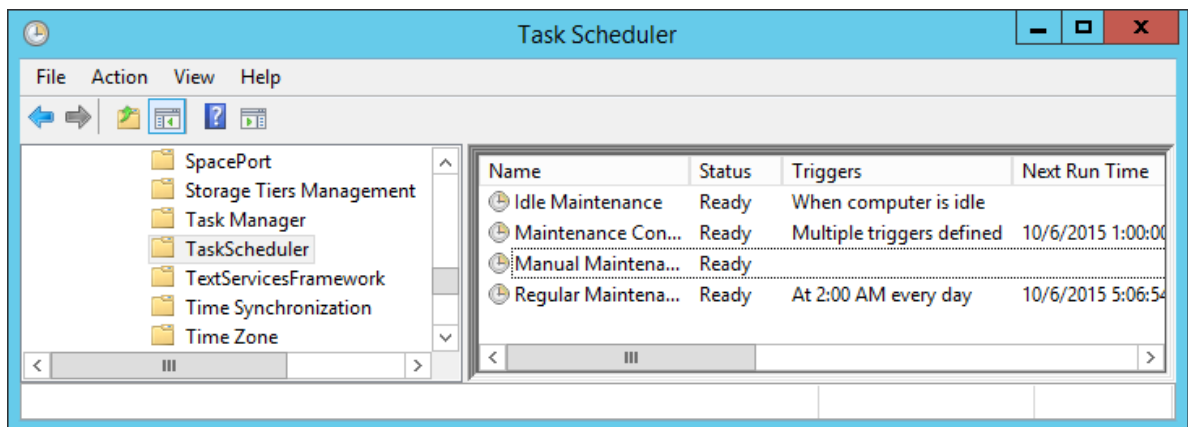
Enabling Windows Server Automatic Maintenance

About this task

Enable Windows Server Automatic Maintenance after updating Contact Center software.

Procedure

1. Log on to the Contact Center server as an administrator.
2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Enable**.
5. In the **Name** column, right-click **Regular Maintenance** and then click **Enable**.



6. From the **File** menu, click **Exit**.

Part 5: Avaya Aura[®] Media Server upgrades, migrations, and patches

- [Avaya Aura Media Server overview](#) on page 259
- [Avaya Aura Media Server to Avaya Aura Media Server migration](#) on page 263
- [Avaya Media Server to Avaya Aura Media Server migration](#) on page 278
- [Co-resident Avaya Aura Media Server replacement](#) on page 292
- [Avaya Aura Media Server OVA upgrade and patch installation](#) on page 294

Chapter 13: Avaya Aura® Media Server overview

You can upgrade, migrate, and patch Avaya Aura® Media Server software. SIP-enabled Avaya Aura® Contact Center solutions include and use Avaya Aura® Media Server software.

Avaya Aura® Media Server upgrades, migrations, and patches

Avaya Aura® Media Server is a software based media processing platform. All SIP-enabled Avaya Aura® Contact Center solutions require one or more Avaya Aura® Media Server systems.

Each release of Avaya Aura® Contact Center integrates with a newer, enhanced version of Avaya Aura® Media Server:

- AACC 7.1.2.2 integrates with Avaya Aura® Media Server Release 8.0.x and 10.1.x.
- AACC Release 7.0 Feature Pack 3 integrates with Avaya Aura® Media Server Release 7.8.
- AACC Release 7.0 Feature Pack 2 integrates with Avaya Aura® Media Server Release 7.7.0.391.
- AACC Release 7.0 Feature Pack 1 integrates with Avaya Aura® Media Server Release 7.7.0.348.
- AACC Release 7.0 integrates with Avaya Aura® Media Server Release 7.7.
- AACC Release 6.4 integrates with Avaya Media Server Release 7.6.
- AACC Release 6.3 integrates with Avaya Media Server Release 7.5.
- AACC Release 6.2 integrates with Avaya Media Server Release 7.0.
- AACC Release 6.1/6.0 integrates with Media Application Server software.

You can upgrade or migrate Avaya Aura® Media Server software. The latest versions of Avaya Aura® Media Server are supported on Red Hat Enterprise Linux (RHEL) 64-bit servers. Therefore, if you are upgrading from a previous version of AACC to AACC Release 7.1.x and Avaya Aura® Media Server is installed standalone on a Linux server, you must migrate Avaya Aura® Media

Server software. If you are upgrading from AACC 7.0.3 to AACC Release 7.1.x and you are using an Avaya Aura® Media Server OVA, you can upgrade Avaya Aura® Media Server software.

- For an upgrade, you reuse an existing RHEL 64-bit server with a previous version of software on it and upgrade the Avaya Aura® Media Server software on that same server. When you upgrade the Avaya Aura® Media Server OVA, the operating system is automatically updated.
- For a migration, you install a new RHEL 64-bit server with Avaya Aura® Media Server software and import the data from the previous server.

The Avaya Aura® Contact Center Release Notes contain information about known issues, patches, procedures, and workarounds specific to a release and patch line-up of Avaya Aura® Contact Center and Avaya Aura® Media Server. For more information about the Avaya Aura® Contact Center Release Notes, see <https://support.avaya.com>.

Avaya Aura® Contact Center and Avaya Aura® Media Server have independent patches, service packs, upgrade and patching procedures, and naming conventions.

Avaya Aura® Media Server supports High Availability only on the Linux operating system. Avaya Aura® Media Server does not support High Availability on the Microsoft Windows Server operating systems. All Avaya Aura® Media Server systems in a contact center solution must be the same release. All Avaya Aura® Media Server systems in a High Availability pair or cluster must be the same release and patch level.

Upgrades

If you migrate Avaya Aura® Contact Center software to Release 7.1.x, you must also upgrade or migrate all media servers in the solution to either Avaya Aura® Media Server Release 8.0.x or 10.1.x. Ensure that you upgrade or migrate all Avaya Aura® Media Server systems in the solution to the same release.

The following table lists the supported Avaya Aura® Media Server upgrade options:

Existing version of Avaya Aura® Media Server	Direct upgrade	Notes
Media Application Server (AACC 6.0 or 6.1)	No	You must first upgrade to Media Server Release 7.6 and apply the most recent patches. Run the data preparation utility. Next, upgrade to Avaya Aura® Media Server Release 7.7 and apply the most recent patches. Finally, you must migrate to either Avaya Aura® Media Server Release 8.0.x or 10.1.x.
Avaya Media Server Release 7.0 (AACC 6.2)	No	You must first upgrade to Media Server Release 7.6 and apply the most recent patches. Run the data preparation utility. You must then upgrade to Avaya Aura® Media Server Release 7.7 and apply the most recent patches. Finally, you must migrate to

Table continues...

Existing version of Avaya Aura® Media Server	Direct upgrade	Notes
Avaya Media Server Release 7.5 (AACC 6.3)	No	Avaya Aura® Media Server Release 8.0.x or 10.1.x.
Avaya Media Server Release 7.6 (AACC 6.4)	No	Apply the most recent Media Server Release 7.6 patches and run the data preparation utility. You must then upgrade to Avaya Aura® Media Server Release 7.7 and apply the most recent patches. Finally, migrate to Avaya Aura® Media Server Release 8.0.x or 10.1.x.
Avaya Aura® Media Server Release 7.7 (AACC 7.0)	No	Apply the most recent Avaya Aura® Media Server Release 7.7 patches. You must then migrate to Avaya Aura® Media Server Release 8.0.x or 10.1.x.
Avaya Aura® Media Server Release 7.8 (AACC 7.0.3)	Yes	Apply the most recent Avaya Aura® Media Server Release 7.8 patches. You can then upgrade or migrate to Avaya Aura® Media Server Release 8.0.x or 10.1.x., depending on your installation.

The Avaya Aura® Media Server 8.0.x or 10.1.x OVA supports direct upgrades only on a fully-patched Avaya Aura® Media Server 7.7 or 7.8 server.

If your existing contact center solution is not using the Avaya Aura® Media Server OVA, then you must use the migration procedures. Avaya Media Server to Avaya Aura® Media Server migrations support migrating the Application Content data and do not support migrating the System Configuration data.

Upgrading from Avaya Aura® Media Server on Windows to Avaya Aura® Media Server on Linux is not supported. Similarly, you cannot upgrade from Avaya Aura® Media Server on Linux to Windows.

Before upgrading Avaya Aura® Media Server software, ensure that the existing server hardware can support the newer version of software.

Upgrading to Release 7.1.x

When you install Avaya Aura® Contact Center Release 7.1.x, you must also upgrade Avaya Aura® Media Server to the correct version. For more information about updating Avaya Aura® Media Server on Windows, see [Voice and Multimedia Contact Server with Avaya Aura Media Server upgrade and patch installation](#) on page 251. For information about Linux, see [Avaya Aura Media Server OVA upgrade and patch installation](#) on page 294.

Important:

Avaya Aura® Media Server includes enhancements to the music streaming feature. If you are using RSS or SHOUTcast streaming, you must reconfigure music streaming after the upgrade.

Migrations

The following Avaya Aura® Media Server migrations are supported:

- Avaya Aura® Media Server Release 7.7, 7.8, or 8.0.x on Windows to Avaya Aura® Media Server Release 8.0.x or 10.1.x on Windows Server 2016 or Windows Server 2019. When you migrate, the Linux version of Avaya Aura® Media Server is deployed on a Hyper-V instance on Windows Server.
- Avaya Aura® Media Server Release 7.7, 7.8, or 8.0.x on Linux to Avaya Aura® Media Server Release 8.0.x or 10.1.x on a Red Hat Enterprise Linux 64-bit server.

For the migration, install Avaya Aura® Media Server software on the new server. Then back up the data from the existing server and restore it on the new server.

Avaya Aura® Contact Center does not support the following:

- Migrating Avaya Aura® Media Server from Linux to the Microsoft Windows operating system.
- Migrating an Avaya Aura® Media Server database from Linux to Microsoft Windows.

Avaya Media Server to Avaya Aura® Media Server migrations support migrating the Application Content data but not the System Configuration data.

The following Media Server migrations support only Application Content migration:

- Media Server Release 7.5 or 7.6 on Windows 2008 to Avaya Aura® Media Server on Windows Server 2016 or 2019.
- Media Server Release 7.5 or 7.6 on Windows 2008 to Avaya Aura® Media Server on RHEL.
- Avaya Aura® Media Server Release 7.7 on Windows 2012 to Avaya Aura® Media Server on RHEL.
- Media Server Release 7.5 or 7.6 on Linux to Avaya Aura® Media Server on RHEL.
- Media Server Release 7.6 OVA to the Avaya Aura® Media Server 8.0.x or 10.1.x OVA.

Patches

You can apply Avaya Aura® Media Server patches to resolve product issues. Some Avaya Aura® Media Server patches are simple Quick Fix Engineering (QFE) patches, and some patches are more complex. You must read each Avaya Aura® Media Server patch Readme file and the Avaya Aura® Contact Center Release Notes to determine the correct procedures for each patch.

Chapter 14: Avaya Aura[®] Media Server to Avaya Aura[®] Media Server migration

This section describes how to migrate Avaya Aura[®] Media Server Release 7.7, 7.8, or 8.0 software to Avaya Aura[®] Media Server Release 8.0.x or 10.1, from one RHEL 64-bit server to another. For information about supported RHEL versions, see the [Red Hat website](#).

You can migrate Avaya Aura[®] Media Server software to a new server for a number of reasons:

- Migrate Avaya Aura[®] Media Server to a new server if the old server hardware is faulty.
- Migrate Avaya Aura[®] Media Server to a faster server to support additional agents.
- Migrate Avaya Aura[®] Media Server to a faster server to support Call Recording.
- Migrate Avaya Aura[®] Media Server to a faster server to support High Availability.

Complete the procedures in this section in sequential order.

Backing up the Avaya Aura[®] Media Server database

Before you begin

If you are backing up Avaya Aura[®] Media Server Release 7.7, apply the most recent service packs and QFE patches.

About this task

Back up Avaya Aura[®] Media Server data.

Procedure

1. Access the primary Avaya Aura[®] Media Server Element Manager with Administrator privileges.
2. Expand **Tools**.
3. Expand **Backup and Restore**.
4. Select **Backup Tasks**.
5. On the Backup Tasks window, click **Add**.

6. On the Add New Backup Task window, in the **Backup Task Name** box, type a name for this backup.
7. Select **Application Content**.
8. Select **System Configuration**.
9. Choose the backup destination that you created for the migration, or the default backup location.
10. Select **Manually, as needed**.
11. Click **Save**.
12. In the Backup Tasks window, select the backup task you created.
13. Click **Run Now**.
14. When prompted, click **Confirm**.

The History Log window is displayed. When the backup is complete, the backup details are displayed in the list.

15. Copy the backup to a secure network location. By default, Avaya Aura® Media Server backups are stored in the %MASHOME%\platdata\EAM\Backups folder.

Installing the Linux server

Before you begin

Ensure your new server hardware meets all the requirements described in *Avaya Aura® Contact Center Overview and Specification*.

About this task

Install the Linux server operating system so that you can install the Avaya Aura® Media Server software. Standalone Avaya Aura® Media Server supports the RHEL 64-bit operating system. For more information, see *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS*.

Procedure

1. Place the Linux installation disk in the DVD drive of the server.
2. Restart the server by powering it off and then powering it on again.
3. On the Red Hat Enterprise Linux page, select **Install Red Hat Enterprise Linux**.
4. On the What language would you like to use during the installation process page, select **English (English)** and then select the locale.

Avaya Aura® Media Server supports the English operating system only.

5. Click **Continue**.

The installer displays the Installation Summary page.

6. Click **Software Selection** and then click the **Infrastructure Server** option.
7. Click **Done**.

The installer returns to the Installation Summary page.

8. Click **Installation Destination** and select the disk on which to install the Avaya Aura® Media Server software.
9. Click **Done**.

The installer returns to the Installation Summary page.

10. Click **Network & Host Name** and select the Ethernet interface that you are connecting to your physical network.
11. Click **Configure**.
12. On the Editing page, configure the following settings for the selected interface:
 - a. Click the **IPv4 Settings** tab.
 - b. From the **Method** drop-down list, click **Manual**.
 - c. Click **Add**.
 - d. Enter the IP Address, Netmask, and Gateway details for the server.
 - e. In the **DNS servers** field, type the IP address of the DNS server for your network.
 - f. In the **Search domains** field, type the domain for this server.

Editing eth0

Connection name: eth0

General Ethernet 802.1X Security DCB Proxy **IPv4 Settings** IPv6 Settings

Method: Manual

Addresses

Address	Netmask	Gateway
10.134.128.21	255.255.255.0	10.134.128.254

Add Delete

DNS servers: 10.134.128.252

Search domains: aaccdomain.com

DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

Routes...

Cancel Save

g. On the IPv6 Settings tab, from the **Method** drop-down list, click **Ignore**.

h. Click **Save**.

13. In the **Host name** field, enter the server FQDN.

14. Click **Apply**.

15. Enable the configured network adapter by setting the switch to **ON**.

16. Click **Done**.

The installer returns to the Installation Summary page.

17. Configure **Date & Time** and **Keyboard** settings.

The time zone and daylight saving settings of the Avaya Aura® Media Server(s) must match the time zone and daylight saving settings of the Contact Center servers in this SIP-enabled contact center solution.

18. Click **Begin Installation**.

19. Under **User Settings**, click **Root Password**.

20. In the **Root Password** field, type the password for the root user and confirm the password.

21. Click **Finish configuration**.

22. When the installation is complete, click **Reboot** to reboot the server.

Next steps

Log on to the server and verify that the Ethernet connection is operating correctly. You can use the `ifconfig`, `ping`, and `ifup` commands to check and start the connection. Use the `nmtui` command to verify your network configuration details. If the connection does not work, refer to your Red Hat documentation for troubleshooting guidance.

Adding a Linux user group and user

About this task

Create a Linux user and account group that you can use to log on to Avaya Aura® Media Server Element Manager.

For example, create a user group named *mediaservergroup*, and then create a user *msuser* as a member of that group. Use this account to access Avaya Aura® Media Server Element Manager.

Procedure

1. On the Linux server, open a Linux terminal.
2. Use the `su` command to change to the root user account. For example:

```
su -
```
3. Use the Linux `groupadd` command to create a new group. For example:

```
groupadd mediaservergroup
```
4. Use the Linux `useradd` command to create a new user in the group you created. For example:

```
useradd msuser -G mediaservergroup
```
5. Use the Linux `passwd` command to configure the password for the user. For example:

```
passwd msuser
```

Installing Avaya Aura® Media Server software on Linux

Before you begin

- Download and review the Avaya Aura® Contact Center Release Notes. The Release Notes contain the known issues, patches, and workarounds specific to a release and patch line-up of Avaya Aura® Contact Center.
- Download Avaya Aura® Media Server software. Read the Avaya Aura® Contact Center Release Notes to ensure that you are using the most recent version of Avaya Aura® Media Server software.
- You must configure a YUM repository. The Avaya Aura® Media Server installer automatically installs all required packages.

- Log on to the Linux server.

About this task

Install the Avaya Aura® Media Server software to provide media processing for contacts in a SIP-enabled contact center environment.

Procedure

1. Read the Avaya Aura® Contact Center Release Notes to determine the most recent version of the Avaya Aura® Media Server software to install.
2. On your Linux server, use the su command to change to the root user account. For example:

```
su -
```
3. Use the mkdir command to create a temporary folder on the Linux server. For example:

```
mkdir /tmp/AvayaMS
```
4. Obtain the most recent version of the Avaya Aura® Media Server installation file. The installation file can have a more recent version number and date stamp than the file used in this procedure. You can download the installation file from the Avaya support website at <http://support.avaya.com>.
5. Using a Secure Copy (SCP) utility, copy the installation file from your desktop computer to the temporary directory you created on the Linux server.
6. On the Linux server, navigate to the temporary directory you created. For example:

```
cd /tmp/AvayaMS
```
7. Grant executable permissions to the Avaya Aura® Media Server installation file.
8. Start the Avaya Aura® Media Server installer by running the installation file.
9. If you see a list of required RHEL packages to download and if the system prompts you to install the required packages, press **Y** and then press **Enter**.
10. The installer displays the Install Overview. Press **Enter** to continue.
11. The installer displays the license agreement. Press **Enter** to continue to page through the license agreement screens.
12. To accept the License Agreement and continue with the install, enter **Y**.
13. When prompted **Install Element Manager?**, enter **Y** to install the Element Manager.
14. When prompted for the Linux group name; press **Enter** to accept the default or specify the user group you created earlier. For example, select mediaservergroup so members of this group can log on and use Avaya Aura® Media Server Element Manager.
 - Press **Enter** to accept the default.
 - Specify an existing user group. Select an existing user group so members of that group can log on and use Avaya Aura® Media Server Element Manager. For example, select the mediaservergroup user group.

15. When prompted **Where would you like to install?**, press Enter to accept the default of `/opt/avaya/mediaserver`.
16. At the **Configuration Summary** section, enter 1 to continue with the installation. Enter 2 to change your installation options.
17. When the install completes copying files, press Enter to exit the install.

Configuring the Linux server for Avaya Aura® Media Server

Before you begin

- Install Avaya Aura® Media Server software.
- Download and review the Avaya Aura® Contact Center Release Notes. The Release Notes contain the known issues, patches, and workarounds specific to a release and patch line-up of Avaya Aura® Contact Center.
- Obtain the most recent version of the Avaya Aura® Contact Center Release 7.1 DVD. Read the Avaya Aura® Contact Center Release Notes to ensure that you are using the most recent version of Avaya Aura® Media Server software.
- Know the IP address of a Network Time Protocol (NTP) server.

About this task

Configure the Linux server to support Avaya Aura® Media Server. The Avaya Aura® Contact Center DVD contains a Linux shell script for Avaya Aura® Media Server. Copy this shell script to the Avaya Aura® Media Server Linux server and use it to perform the following configuration steps:

- Install a firewall policy file suitable for Avaya Aura® Media Server.
- Create a non-administrative user account for accessing Avaya Aura® Media Server Element Manager.
- Configure a Network Time Protocol (NTP) server.

Procedure

1. Obtain the most recent version of the Avaya Aura® Contact Center Release 7.1 DVD.
2. Insert the Avaya Aura® Contact Center DVD into the DVD drive of your desktop computer.
3. On your desktop computer, navigate to the `\\Install Software\\AMS\\Linux` folder on the DVD.
4. Using a Secure Copy (SCP) utility, configured to use a *Binary* transfer mode, copy the `sysconfig.sh` shell script from the DVD to the Avaya Aura® Media Server Linux server. Copy the script file using *Binary* transfer mode. Do not copy the script file using *Text* transfer mode.
5. On your Linux server, use the `su` command to change to the root user account. For example:

```
su -
```

6. On your Linux server, navigate to the folder containing the `sysconfig.sh` shell script.
7. Grant executable permissions to the shell script. For example,

```
chmod +x sysconfig.sh
```
8. Start the shell script. For example,

```
./sysconfig.sh
```
9. The script displays an Overview screen. Press `Enter` to continue.
10. The script copies the Avaya Aura® Media Server firewall policy file to the Linux server.
11. At the **NTP Server address (Optional)** prompt, enter the IP address for your Network Time Protocol (NTP) server.

Logging on to Avaya Aura® Media Server Element Manager

Before you begin

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

About this task

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

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

Note:

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

Procedure

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

```
https://SERVER_IP_ADDRESS:8443/em
```

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

5. Click **Sign In**.

Restoring the Avaya Aura® Media Server database

About this task

Restore the Avaya Aura® Media Server database backup data to the new server.

Important:

Perform this procedure only if you are migrating from an existing Avaya Aura® Contact Center Release 7.x system.

Procedure

1. Access the Element Manager with Administrator privileges.
2. Expand **Tools**.
3. Expand **Backup and Restore**.
4. Select **Restore**.
5. On the Restore window, from the **Restore Source** list, select **Upload Backup Files**.
6. Click **Browse**.
7. Select the Avaya Aura® Media Server backup that you want to restore.
8. Click **Upload Files**.
9. On the **Confirm Restore** page, review the information and click **Confirm** to proceed with the restore.
10. After the restore completes, exit Element Manager.
11. Reboot the Avaya Aura® Media Server server.

Configuring the Avaya Aura® Media Server system parameters

About this task


Apply the manual configuration to integrate the new Avaya Aura® Media Server with the contact center.

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

Procedure

1. Log on to Avaya Aura® Media Server Element Manager with administrator privileges.
 2. In the navigation pane, click **System Configuration > Signaling Protocols > SIP**.
 3. Click the **Nodes and Routes** link.
 4. Click **Add**.
 5. On the **Add SIP Trusted Node** page, in the **Host or Server Address** box, type the IP address of the Avaya Aura® Contact Center server.

If the Avaya Aura® Contact Center server uses the High Availability feature, type the managed IP address of the Avaya Aura® Contact Center High Availability pair.
 6. Click **Save**.
 7. In the navigation pane, click **System Configuration > Network Settings > General Settings**.
 8. Click **SOAP**.
 9. In the **Trusted Nodes** box, enter the IP address of the Avaya Aura® Contact Center server.

If the Avaya Aura® Contact Center server uses the High Availability feature, type the managed IP address of the Avaya Aura® Contact Center High Availability pair.
 10. Select **Enable Trusted SOAP Nodes**.
 11. Click **Save**.
 12. If this solution uses SRTP, skip to [step 15](#) on page 272. If this solution does not use SRTP, in the navigation pane, click **System Configuration > Media Processing > Media Security**.
 13. On the **Media Security** page, from the **Security Policy** list, if SRTP is not used, select **Security Disabled**.
 14. Click **Save**.
 15. In the navigation pane, click **System Configuration > Media Processing > Audio Codecs**.
 16. On the **Audio Codecs** page, ensure that the codecs you want to support appear in the **Enabled** list.
-  **Important:**
- If you are using Avaya Contact Recorder (ACR) for call recording, you must ensure that you enable the G.729 codec. ACR call recording has no impact on the quality of voice calls between agents and customers.
17. Click **Save**.

Configuring Avaya Aura® Media Server name resolution

About this task

Configure Avaya Aura® Media Server to resolve the hostname and Fully Qualified Domain Name (FQDN) of the Contact Center Manager Administration server. The Contact Center Manager Administration (CCMA) software is installed on the Contact Center server.

Procedure

1. Log on to Element Manager with administrative privileges.
2. Navigate to **EM > System Configuration > Network Settings > Name Resolution**.
3. Click **Add**.
4. In the **IP Address** box, enter the Contact Center Manager Administration IP address.
5. In the **Hostname** box, enter the Contact Center Manager Administration hostname.
6. Click **Save**.

Resetting the Avaya Aura® Media Server IP address in Element Manager

About this task

When you migrate Avaya Aura® Media Server to a server with a different IP address, the Avaya Aura® Media Server database contains the IP address of the old server. You must update the IP address in Element Manager to make all administration functions work correctly.

Procedure

1. Log on to Avaya Aura® Media Server Element Manager with Administrative privileges.
2. In the left pane, select **System Configuration > Network Settings > IP Interface Assignment**.
3. Under **IPv4 Interfaces**, set the **Signaling**, **Media**, and **Cluster** boxes to the IP address of the new server.
4. Click **Save**.
5. After migrating your server and restoring the server databases, some of the old configuration settings might not match your new solution. Commission your new server in the new solution.

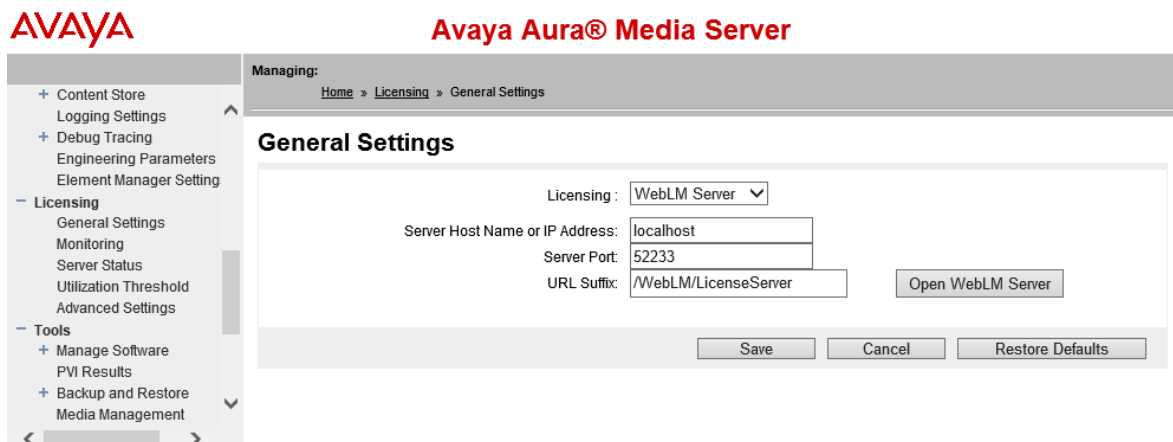
Restoring the Avaya Aura® Media Server default license

About this task

Restore the Avaya Aura® Media Server default license using Element Manager.

Procedure

1. Log on to Avaya Aura® Media Server Element Manager with administrative privileges.
2. In the left pane, select **Licensing > General Settings**.



3. Click **Restore Defaults**.
4. Click **Confirm**.

Configuring the Linux Avaya Aura® Media Server in CCMA

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Configuration component.

About this task

Add the new Linux Avaya Aura® Media Server to CCMA so that Contact Center can start using the new server resources.

Procedure

1. In the left pane, expand the CCMS server that uses the existing Windows Media Server.
The server expands to show its resources.
2. Select the **Media Servers** folder.
3. In the right pane, in the **Server Name** box, type the name for the new Avaya Aura® Media Server.

Avaya recommends that you use the Avaya Aura® Media Server network name.

4. In the **IP address** box, type the IP address of the new Avaya Aura® Media Server.
5. In the **Port Number** box, type the port number for the Avaya Aura® Media Server server.

 **Important:**

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

6. If this is the only Avaya Aura® Media Server in the solution, or if it is designated as the Master Content Store, select **Master Content Store**.
7. Click any other row in the grid to save your changes.
8. In the left pane, select the **Media Services and Routes** folder.
9. From the **Service Name** list, select **ACC_APP_ID**.
10. In the **Routes (Target Media Servers)** list, from the **Available** list, select the new Linux Avaya Aura® Media Server.
11. Click the > arrow key.
12. Click **Submit**.
13. If you are using WebLM, you must restart the Contact Center License Manager service, then afterwards restart the Avaya Aura® Media Server you added.

Removing the existing Avaya Aura® Media Server from CCMA

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Configuration component.

About this task

Remove the existing Avaya Aura® Media Server from CCMA so that Contact Center stops using the old server resources.

Procedure

1. In the left pane, expand the CCMS server that uses the existing Media Server.
The server expands to show its resources.
2. In the left pane, select the **Media Services and Routes** folder.
3. From the **Service Name** list, select **ACC_APP_ID**.
4. In the **Routes (Target Media Servers)** list, from the **Selected** list, select the existing Avaya Aura® Media Server.

5. Click the < arrow key.
6. Click **Submit**.
7. In the left pane, select the **Media Servers** folder.
8. In the right pane, select the Avaya Aura® Media Server, and press **Delete**.
9. On the **Confirm Delete** window, click **Yes**.

Restarting Contact Center License Manager

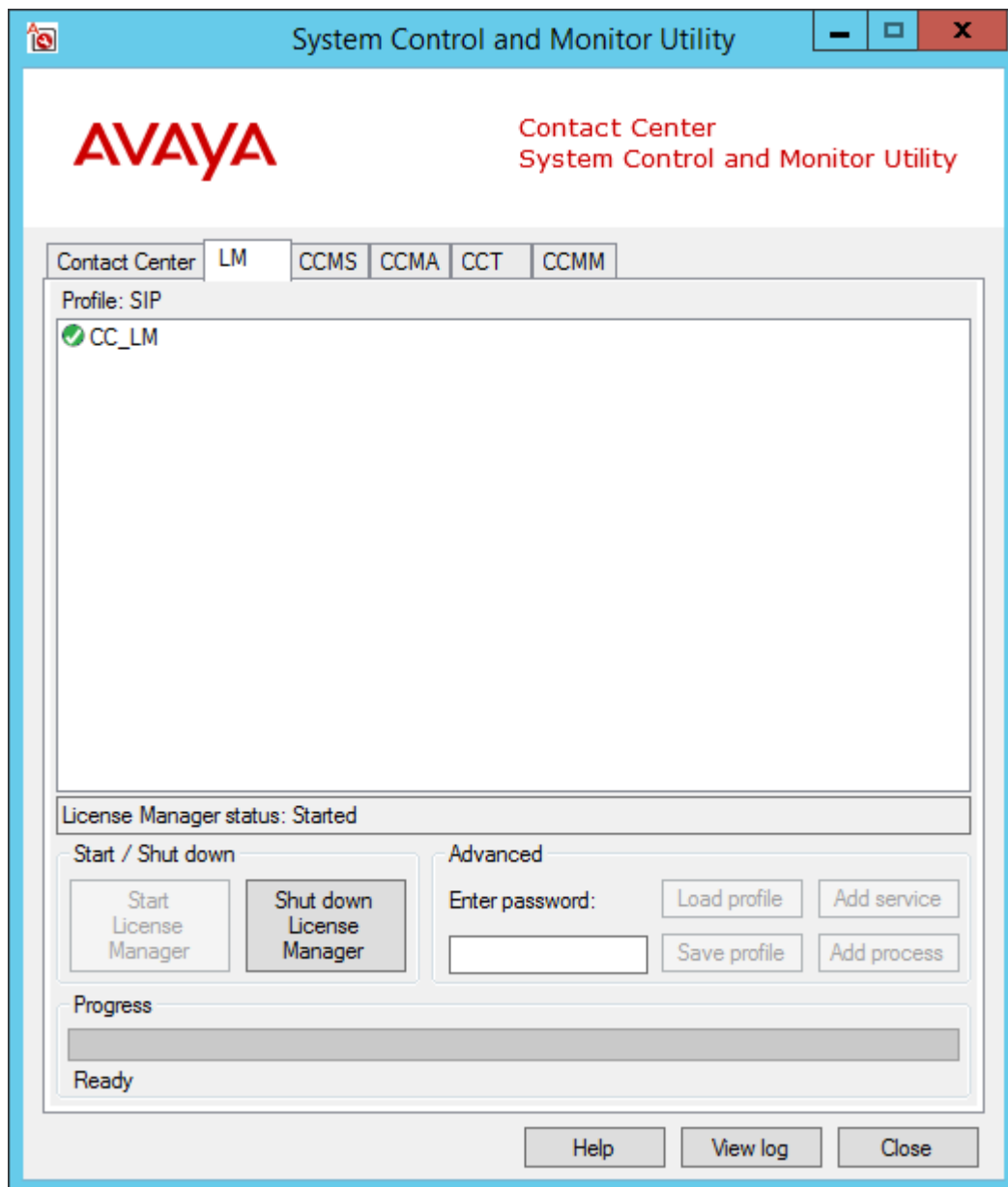
About this task

Restart Contact Center License Manager to push licenses to the Avaya Aura® Media Server instances configured in Contact Center Manager Administration.

Procedure

1. Log on to the Contact Center server.
2. From the **Start** menu, in the Avaya area, click **System Control and Monitor Utility**.
3. Click the **LM** tab.
4. Click **Shut down License Manager**.

5. Click **Start License Manager**.



6. Click **Close**.

Chapter 15: Avaya Media Server to Avaya Aura® Media Server migration

This section describes how to migrate Avaya Media Server Release 7.5 or 7.6 to Avaya Aura® Media Server Release 8.0.x or 10.1 on an RHEL 64-bit Linux server. For information about supported RHEL versions, see the [Red Hat website](#).

Complete the procedures in this section in sequential order.

Preparing the Avaya Media Server on Linux Content Store

Before you begin

- Apply the most recent Avaya Media Server service packs and Quick Fix Engineering (QFE) patches.
- Obtain the most recent version of the Avaya Aura® Contact Center Release 7.1.x DVD. Read the Avaya Aura® Contact Center Release Notes to ensure that you are using the most recent version of Avaya Aura® Media Server software.
- Know the Avaya Aura® Contact Center SIP domain name.

About this task

Prepare the Avaya Media Server Content Store data for upgrade and migration to Avaya Aura® Media Server Release 8.0.x or 10.1.x.

Procedure

1. Obtain the most recent version of the Avaya Aura® Contact Center Release 7.1.x DVD.
2. Insert the DVD into your computer's DVD drive.
3. On your computer, navigate to the `\\Install Software\AMS\Linux` folder on the DVD.
4. Using a Secure Copy (SCP) utility configured to use the Text transfer mode, copy the `prepareForAAMS77Migration.py` script from the DVD to the existing Avaya Media Server Linux server.

Copy the script file using Text transfer mode. Do not copy the script file using Binary transfer mode.

5. On your Linux server, use the `su -` command to change to the root user account.

6. On your Linux server, navigate to the folder containing the `prepareForAAMS77Migration.py` shell script.

7. Grant executable permissions to the shell script.

For example, run: `chmod +x prepareForAAMS77Migration.py`

8. Start the data preparation script.

For example, run `./prepareForAAMS77Migration.py`

9. At the **Please enter ACC SIP Domain** prompt, enter the Avaya Aura® Contact Center SIP domain name.

The utility prepares the data for migration.

Backing up the Avaya Media Server database

Before you begin

- Apply the most recent Avaya Media Server Release 7.5 or 7.6 service packs and Quick Fix Engineering (QFE) patches.

About this task

Backup the Avaya Media Server data. Backup the Application Content data.

Procedure

1. Access the primary Media Server Element Manager with Administrator privileges.
2. Expand **Tools**.
3. Expand **Backup and Restore**.
4. Select **Backup Tasks**.
5. On the Backup Tasks window, click **Add**.
6. On the Add New Backup Task window, in the **Backup Task Name** box, type a name for this backup.
7. Select **Application Content**.
8. Clear **System Configuration**.
9. Choose the backup destination that you created for the migration, or the default backup location.
10. Select **Manually, as needed**.
11. Click **Save**.
12. In the Backup Tasks window, select the backup task you created.

13. Click **Run Now**.

The Confirm Backup window appears, showing the backup task name details about the backup.

14. Click **Confirm**.

The History Log Window appears. When the backup is complete, the backup details appear in the list.

15. Copy the backup to a secure network location. By default, Avaya Media Server backups are stored in the %MASHOME%\platdata\EAM\Backups folder.

Installing the Linux server

Before you begin

Ensure your new server hardware meets all the requirements described in *Avaya Aura® Contact Center Overview and Specification*.

About this task

Install the Linux server operating system so that you can install the Avaya Aura® Media Server software. Standalone Avaya Aura® Media Server supports the RHEL 64-bit operating system. For more information, see *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS*.

Procedure

1. Place the Linux installation disk in the DVD drive of the server.
2. Restart the server by powering it off and then powering it on again.
3. On the Red Hat Enterprise Linux page, select **Install Red Hat Enterprise Linux**.
4. On the What language would you like to use during the installation process page, select **English (English)** and then select the locale.

Avaya Aura® Media Server supports the English operating system only.

5. Click **Continue**.

The installer displays the Installation Summary page.

6. Click **Software Selection** and then click the **Infrastructure Server** option.

7. Click **Done**.

The installer returns to the Installation Summary page.

8. Click **Installation Destination** and select the disk on which to install the Avaya Aura® Media Server software.

9. Click **Done**.

The installer returns to the Installation Summary page.

10. Click **Network & Host Name** and select the Ethernet interface that you are connecting to your physical network.
11. Click **Configure**.
12. On the Editing page, configure the following settings for the selected interface:
 - a. Click the **IPv4 Settings** tab.
 - b. From the **Method** drop-down list, click **Manual**.
 - c. Click **Add**.
 - d. Enter the IP Address, Netmask, and Gateway details for the server.
 - e. In the **DNS servers** field, type the IP address of the DNS server for your network.
 - f. In the **Search domains** field, type the domain for this server.

Editing eth0

Connection name: eth0

General Ethernet 802.1X Security DCB Proxy **IPv4 Settings** IPv6 Settings

Method: Manual

Addresses

Address	Netmask	Gateway
10.134.128.21	255.255.255.0	10.134.128.254

Add Delete

DNS servers: 10.134.128.252

Search domains: aaccdomain.com

DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

Routes...

Cancel Save

- g. On the IPv6 Settings tab, from the **Method** drop-down list, click **Ignore**.
 - h. Click **Save**.
13. In the **Host name** field, enter the server FQDN.
14. Click **Apply**.
15. Enable the configured network adapter by setting the switch to **ON**.

16. Click **Done**.

The installer returns to the Installation Summary page.

17. Configure **Date & Time** and **Keyboard** settings.

The time zone and daylight saving settings of the Avaya Aura® Media Server(s) must match the time zone and daylight saving settings of the Contact Center servers in this SIP-enabled contact center solution.

18. Click **Begin Installation**.

19. Under **User Settings**, click **Root Password**.

20. In the **Root Password** field, type the password for the root user and confirm the password.

21. Click **Finish configuration**.

22. When the installation is complete, click **Reboot** to reboot the server.

Next steps

Log on to the server and verify that the Ethernet connection is operating correctly. You can use the `ifconfig`, `ping`, and `ifup` commands to check and start the connection. Use the `nmtui` command to verify your network configuration details. If the connection does not work, refer to your Red Hat documentation for troubleshooting guidance.

Adding a Linux user group and user

About this task

Create a Linux user and account group that you can use to log on to Avaya Aura® Media Server Element Manager.

For example, create a user group named *mediaservergroup*, and then create a user *msuser* as a member of that group. Use this account to access Avaya Aura® Media Server Element Manager.

Procedure

1. On the Linux server, open a Linux terminal.
2. Use the `su` command to change to the root user account. For example:

```
su -
```

3. Use the Linux `groupadd` command to create a new group. For example:

```
groupadd mediaservergroup
```

4. Use the Linux `useradd` command to create a new user in the group you created. For example:

```
useradd msuser -G mediaservergroup
```

5. Use the Linux `passwd` command to configure the password for the user. For example:

```
passwd msuser
```

Installing Avaya Aura® Media Server software on Linux

Before you begin

- Download and review the Avaya Aura® Contact Center Release Notes. The Release Notes contain the known issues, patches, and workarounds specific to a release and patch line-up of Avaya Aura® Contact Center.
- Download Avaya Aura® Media Server software. Read the Avaya Aura® Contact Center Release Notes to ensure that you are using the most recent version of Avaya Aura® Media Server software.
- You must configure a YUM repository. The Avaya Aura® Media Server installer automatically installs all required packages.
- Log on to the Linux server.

About this task

Install the Avaya Aura® Media Server software to provide media processing for contacts in a SIP-enabled contact center environment.

Procedure

1. Read the Avaya Aura® Contact Center Release Notes to determine the most recent version of the Avaya Aura® Media Server software to install.
2. On your Linux server, use the su command to change to the root user account. For example:


```
su -
```
3. Use the mkdir command to create a temporary folder on the Linux server. For example:


```
mkdir /tmp/AvayaMS
```
4. Obtain the most recent version of the Avaya Aura® Media Server installation file. The installation file can have a more recent version number and date stamp than the file used in this procedure. You can download the installation file from the Avaya support website at <http://support.avaya.com>.
5. Using a Secure Copy (SCP) utility, copy the installation file from your desktop computer to the temporary directory you created on the Linux server.
6. On the Linux server, navigate to the temporary directory you created. For example:


```
cd /tmp/AvayaMS
```
7. Grant executable permissions to the Avaya Aura® Media Server installation file.
8. Start the Avaya Aura® Media Server installer by running the installation file.
9. If you see a list of required RHEL packages to download and if the system prompts you to install the required packages, press **Y** and then press **Enter**.

10. The installer displays the Install Overview. Press `Enter` to continue.
11. The installer displays the license agreement. Press `Enter` to continue to page through the license agreement screens.
12. To accept the License Agreement and continue with the install, enter `Y`.
13. When prompted **Install Element Manager?**, enter `Y` to install the Element Manager.
14. When prompted for the Linux group name; press `Enter` to accept the default or specify the user group you created earlier. For example, select `mediaservergroup` so members of this group can log on and use Avaya Aura® Media Server Element Manager.
 - Press `Enter` to accept the default.
 - Specify an existing user group. Select an existing user group so members of that group can log on and use Avaya Aura® Media Server Element Manager. For example, select the `mediaservergroup` user group.
15. When prompted **Where would you like to install?**, press `Enter` to accept the default of `/opt/avaya/mediaserver`.
16. At the **Configuration Summary** section, enter `1` to continue with the installation. Enter `2` to change your installation options.
17. When the install completes copying files, press `Enter` to exit the install.

Configuring the Linux server for Avaya Aura® Media Server

Before you begin

- Install Avaya Aura® Media Server software.
- Download and review the Avaya Aura® Contact Center Release Notes. The Release Notes contain the known issues, patches, and workarounds specific to a release and patch line-up of Avaya Aura® Contact Center.
- Obtain the most recent version of the Avaya Aura® Contact Center Release 7.1 DVD. Read the Avaya Aura® Contact Center Release Notes to ensure that you are using the most recent version of Avaya Aura® Media Server software.
- Know the IP address of a Network Time Protocol (NTP) server.

About this task

Configure the Linux server to support Avaya Aura® Media Server. The Avaya Aura® Contact Center DVD contains a Linux shell script for Avaya Aura® Media Server. Copy this shell script to the Avaya Aura® Media Server Linux server and use it to perform the following configuration steps:

- Install a firewall policy file suitable for Avaya Aura® Media Server.
- Create a non-administrative user account for accessing Avaya Aura® Media Server Element Manager.
- Configure a Network Time Protocol (NTP) server.

Procedure

1. Obtain the most recent version of the Avaya Aura® Contact Center Release 7.1 DVD.
2. Insert the Avaya Aura® Contact Center DVD into the DVD drive of your desktop computer.
3. On your desktop computer, navigate to the `\\Install Software\AMS\Linux` folder on the DVD.
4. Using a Secure Copy (SCP) utility, configured to use a *Binary* transfer mode, copy the `sysconfig.sh` shell script from the DVD to the Avaya Aura® Media Server Linux server. Copy the script file using *Binary* transfer mode. Do not copy the script file using *Text* transfer mode.
5. On your Linux server, use the `su` command to change to the root user account. For example:

```
su -
```
6. On your Linux server, navigate to the folder containing the `sysconfig.sh` shell script.
7. Grant executable permissions to the shell script. For example,

```
chmod +x sysconfig.sh
```
8. Start the shell script. For example,

```
./sysconfig.sh
```
9. The script displays an Overview screen. Press `Enter` to continue.
10. The script copies the Avaya Aura® Media Server firewall policy file to the Linux server.
11. At the **NTP Server address (Optional)** prompt, enter the IP address for your Network Time Protocol (NTP) server.

Migrating the Avaya Media Server database

About this task

Migrate the old Avaya Media Server backup data to the data format used by the current release of Avaya Aura® Media Server.

Procedure

1. Copy the Avaya Media Server backup Application Content file to the new Avaya Aura® Media Server server. The backup file name derives from the name that you entered in Element Manager for the backup task.
2. Using an SSH client, log on to the new Avaya Aura® Media Server server Linux shell console using the `cust` account.
3. Using the command line, navigate to the folder containing the backup file.
4. Upgrade and restore the backup. On the command line, enter:

```
amsupgrade <backupfile name>
```

Where `<backupfile name>` is the Avaya Media Server backup Application Content file.

5. After the upgrade utility completes, reboot the Avaya Aura® Media Server server.

Completing the Avaya Aura® Media Server on Linux Content Store

Before you begin

- Read the Avaya Aura® Contact Center Release Notes.
- This procedure requires `sroot` access. Obtain Enhanced Access Security Gateway (EASG) access to Avaya Aura® Media Server so that you can log on as `sroot`. For more information about enabling EASG, see *Deploying and Updating Avaya Aura® Media Server Appliance* or Avaya Aura® Media Server Release Notes.
- Obtain the most recent version of the Avaya Aura® Contact Center Release 7.1 DVD. Read the Avaya Aura® Contact Center Release Notes to ensure that you are using the most recent version of Avaya Aura® Media Server software.

About this task

Complete the Avaya Aura® Media Server Content Store data upgrade or migration process. This procedure removes any music content groups from the SIP domain namespace that are duplicated in the *streamsource* namespace.

Alternatively, you can choose to manually remove any music content groups from the SIP domain namespace that are duplicated in the *streamsource* namespace. For more information, see Avaya Aura® Contact Center Release Notes.

Procedure

1. Obtain the most recent version of the Avaya Aura® Contact Center Release 7.1 DVD.
2. Insert the DVD into the DVD drive of your desktop computer.
3. On your desktop computer, navigate to the `\\Install Software\AMS\Linux` folder on the DVD.
4. Using a Secure Copy (SCP) utility, configured to use a *Text* transfer mode, copy the `completeAAMS77Migration.py` script from the DVD to the existing Avaya Media Server Linux server. Copy the script file using *Text* transfer mode. Do not copy the script file using *Binary* transfer mode.
5. On your Linux server, use the `su` command to change to the `sroot` user account. For example:

```
su - sroot
```
6. On your Linux server, navigate to the folder containing the `completeAAMS77Migration.py` shell script.

7. Start the python script. For example,

```
python completeAAMS77Migration.py
```

The utility completes the Avaya Aura® Media Server Content Store data migration or upgrade.

Logging on to Avaya Aura® Media Server Element Manager

Before you begin

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

About this task

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

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

Note:

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

Procedure

1. Start a Web browser.
2. In the address box, type the following URL:
`https://SERVER_IP_ADDRESS:8443/em`
Where SERVER_IP_ADDRESS is the IP address of the Avaya Aura® Media Server.
3. In the **User ID** box, type the Avaya Aura® Media Server User ID log on account name. The default user account name is `Admin`.
4. In the **Password** box, type the Element Manager password. Use the `Admin` account password. The default password is `Admin123$`.
5. Click **Sign In**.

Configuring the Avaya Aura® Media Server system parameters

About this task

Apply the manual configuration to integrate the new Avaya Aura® Media Server with the contact center.

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

Procedure

1. Log on to Avaya Aura® Media Server Element Manager with administrator privileges.
2. In the navigation pane, click **System Configuration > Signaling Protocols > SIP**.
3. Click the **Nodes and Routes** link.
4. Click **Add**.
5. On the **Add SIP Trusted Node** page, in the **Host or Server Address** box, type the IP address of the Avaya Aura® Contact Center server.

If the Avaya Aura® Contact Center server uses the High Availability feature, type the managed IP address of the Avaya Aura® Contact Center High Availability pair.
6. Click **Save**.
7. In the navigation pane, click **System Configuration > Network Settings > General Settings**.
8. Click **SOAP**.
9. In the **Trusted Nodes** box, enter the IP address of the Avaya Aura® Contact Center server.

If the Avaya Aura® Contact Center server uses the High Availability feature, type the managed IP address of the Avaya Aura® Contact Center High Availability pair.
10. Select **Enable Trusted SOAP Nodes**.
11. Click **Save**.
12. If this solution uses SRTP, skip to [step 15](#) on page 288. If this solution does not use SRTP, in the navigation pane, click **System Configuration > Media Processing > Media Security**.
13. On the **Media Security** page, from the **Security Policy** list, if SRTP is not used, select **Security Disabled**.
14. Click **Save**.
15. In the navigation pane, click **System Configuration > Media Processing > Audio Codecs**.
16. On the **Audio Codecs** page, ensure that the codecs you want to support appear in the **Enabled** list.

 **Important:**

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

17. Click **Save**.

Configuring Avaya Aura® Media Server name resolution

About this task

Configure Avaya Aura® Media Server to resolve the hostname and Fully Qualified Domain Name (FQDN) of the Contact Center Manager Administration server. The Contact Center Manager Administration (CCMA) software is installed on the Contact Center server.

Procedure

1. Log on to Element Manager with administrative privileges.
2. Navigate to **EM > System Configuration > Network Settings > Name Resolution**.
3. Click **Add**.
4. In the **IP Address** box, enter the Contact Center Manager Administration IP address.
5. In the **Hostname** box, enter the Contact Center Manager Administration hostname.
6. Click **Save**.

Configuring the Linux Avaya Aura® Media Server in CCMA

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Configuration component.

About this task

Add the new Linux Avaya Aura® Media Server to CCMA so that Contact Center can start using the new server resources.

Procedure

1. In the left pane, expand the CCMS server that uses the existing Windows Media Server.
The server expands to show its resources.
2. Select the **Media Servers** folder.

3. In the right pane, in the **Server Name** box, type the name for the new Avaya Aura® Media Server.

Avaya recommends that you use the Avaya Aura® Media Server network name.

4. In the **IP address** box, type the IP address of the new Avaya Aura® Media Server.
5. In the **Port Number** box, type the port number for the Avaya Aura® Media Server server.

 **Important:**

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

6. If this is the only Avaya Aura® Media Server in the solution, or if it is designated as the Master Content Store, select **Master Content Store**.
7. Click any other row in the grid to save your changes.
8. In the left pane, select the **Media Services and Routes** folder.
9. From the **Service Name** list, select **ACC_APP_ID**.
10. In the **Routes (Target Media Servers)** list, from the **Available** list, select the new Linux Avaya Aura® Media Server.
11. Click the > arrow key.
12. Click **Submit**.
13. If you are using WebLM, you must restart the Contact Center License Manager service, then afterwards restart the Avaya Aura® Media Server you added.

Removing the existing Avaya Media Server from CCMA

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Configuration component.

About this task

Remove the existing Avaya Media Server from CCMA so that Contact Center stops using the old server resources.

Procedure

1. In the left pane, expand the CCMS server that uses the existing Media Server.
The server expands to show its resources.
2. In the left pane, select the **Media Services and Routes** folder.
3. From the **Service Name** list, select **ACC_APP_ID**.

4. In the **Routes (Target Media Servers)** list, from the **Selected** list, select the existing Avaya Media Server.
5. Click the < arrow key.
6. Click **Submit**.
7. In the left pane, select the **Media Servers** folder.
8. In the right pane, select the Avaya Media Server, and press **Delete**.

Chapter 16: Co-resident Avaya Aura® Media Server replacement

This chapter describes how to replace your co-resident Avaya Aura® Media Server Hyper-V instance with a standalone Linux-based Avaya Aura® Media Server. Replace a co-resident Avaya Aura® Media Server Hyper-V instance to increase your contact center call and agent capacity or to change your contact center configuration to High Availability (HA).

Avaya Aura® Contact Center supports two configurations of Avaya Aura® Media Server:

- Co-resident on an Avaya Aura® Contact Center Voice and Multimedia Contact Server
- Standalone on the Red Hat Enterprise Linux (RHEL) R7.x 64-bit operating system

You can replace an existing co-resident Avaya Aura® Media Server Hyper-V instance by migrating to the Linux server and then commissioning Avaya Aura® Media Server on the Linux server. The procedures for this replacement are the same as an Avaya Aura® Media Server to Avaya Aura® Media Server Linux migration. You must then remove the Avaya Aura® Media Server Hyper-V instance from your Windows server.

Review your Avaya Aura® Contact Center license to ensure that it contains the capacities and features you want when you replace your co-resident Avaya Aura® Media Server Hyper-V instance.

Prerequisites

Perform all of the procedures in Chapter 14 in sequential order. See [Avaya Aura Media Server to Avaya Aura Media Server migration](#) on page 263.

Uninstalling co-resident Avaya Aura® Media Server from the Windows server

About this task

Uninstall the co-resident Avaya Aura® Media Server Hyper-V instance from the Windows server to enable HA on your contact center, or to achieve higher agent count and capacity.

Procedure

1. Log on to the Windows server with Administrator privileges.
2. Navigate to the following folder:
`C:\Program Files (x86)\Avaya\UniversalInstaller`
3. Double-click on `UniversalInstall`.
4. On the **Select Remove Option** window, select **Remove Avaya Aura Media Server only**.
5. Click **Next**.
6. Follow the on-screen instructions.
7. If you are prompted, restart the server.

Chapter 17: Avaya Aura® Media Server OVA upgrade and patch installation

This chapter describes how to upgrade the Avaya Aura® Media Server Release 7.8 OVA to an Avaya Aura® Media Server Release 8.0.x or 10.1.x OVA.

This chapter also describes how to install patches on Avaya Aura® Media Server. Install an Avaya Aura® Media Server QFE patch to deliver and apply a patch to the Avaya Aura® Media Server. You must always install QFE patches sequentially, as QFE patches are dependent on previous patches.

Some Avaya Aura® Media Server patches are simple QFE patches. Some Avaya Aura® Media Server patches are more complex and some patches support Avaya Aura® Media Server version upgrades. You must read each Avaya Aura® Media Server patch Readme file and the Avaya Aura® Contact Center Release Notes to determine the correct procedures for each patch. The Release Notes contain the known issues, patches, procedures, and workarounds specific to a release and patch line-up of Avaya Aura® Contact Center and Avaya Aura® Media Server.

Prerequisites to Avaya Aura® Media Server patch installation

- Download the most recent Avaya Aura® Media Server QFE patches from <https://support.avaya.com>.
- Download and review the *Avaya Aura® Contact Center Release Notes*. The Release Notes contain the known issues, patches, and workarounds specific to a release and patch line-up of Avaya Aura® Contact Center. For more information about the Release Notes, see <https://support.avaya.com>.

Updating Avaya Aura® Media Server OVA to Release 7.1

About this task

Each Avaya Aura® Contact Center release includes a new version of Avaya Aura® Media Server. Follow the steps in this procedure to update an OVA to the new version of Avaya Aura® Media Server.

You must lock Avaya Aura® Media Server before applying patches and unlock it after you install the patches. In a multiple node configuration, apply a patch one node at a time, allowing the calls to be handled by other nodes in the Contact Center. Follow the procedure for each node.

Before you begin

- Download and review the Avaya Aura® Contact Center Release Notes. The Release Notes contain the known issues, patches, procedures, and workarounds specific to a release and patch line-up of Avaya Aura® Contact Center. For more information about the Avaya Aura® Contact Center Release Notes, see <http://support.avaya.com>.
- Back up the Avaya Aura® Media Server before updating to the latest release.
- Download the Avaya Aura® Media Server OVA system update and Media Server software update ISO files from the Avaya Support site, <https://support.avaya.com>.

Procedure

1. Log on to Element Manager.
2. In the system tree, select **Tools > Manage Software > Update > Upload Updates**.
3. Select **Choose File** and navigate to the location of the system update ISO file. For example, select `MediaServer_System_Update_8.0.0.xx_xxxx.xx.xx.iso`.
4. In the left pane, select **Upload**.

The page refreshes when the update completes, and displays the filename details.

5. Select **Choose File** and navigate to the location of the software update ISO file. For example, select `MediaServer_Update_8.0.0.xx_xxxx.xx.xx.iso`.
6. In the left pane, select **Upload**.

The page refreshes when the update completes, and displays the filename details.

7. Click **Install Updates** and wait for the upgrade to complete.
8. When the upgrade completes, log on to Element Manager.
9. In the system tree, select **System Status > Element Status**.
10. Verify that the software versions are correct.

Installing Avaya Aura® Media Server patches on Linux

Before you begin

- Download the most recent Avaya Aura® Media Server QFE patches and store them in the QFE subdirectory. QFE patches are ZIP files, but do not unzip them. The Avaya Aura® Media Server patching utility uses the QFE ZIP files. For a Linux server, the default QFE folder location is `/opt/avaya/app/amsinst/ma/MAS/qfe`.
- Back up Avaya Aura® Media Server before applying patches.

About this task

Install a new QFE patch to apply a change to the Avaya Aura® Media Server system.

Review *Avaya Aura® Contact Center Release Notes* and follow the instructions in each Avaya Aura® Media Server patch Readme file.

Procedure

1. Navigate to Element Manager for the Avaya Aura® Media Server node you want to patch.
2. In the navigation pane, click **System Status > Element Status**.
3. Click **Stop** and confirm the operation on the following page.
4. Close Element Manager.
5. Open a Linux terminal on the server you want to patch.
6. Change to the root user by running the `su -` command.
7. Run the `amspatch list all` command to obtain the correct name for the new QFE patch:

The name of the file is not necessarily the same as the name of the patch.
8. Under the **QFE Name** column, note the name of the patch.
9. Install the patches in numerical order.
 - To install a new patch on the system, run the `amspatch apply <patchname>` command, where `<patchname>` is the name of the patch.
 - To install all downloaded QFE patches on the system, run the `amspatch apply all` command.
10. When the patch application is complete, open the Element Manager navigation pane, and click **Tools > Software Inventory**.
11. Verify the patch version listed in the **Patch Level** column.
12. Navigate to **System Status > Element Status** and then click **Start**.
13. Confirm the operation.
14. Navigate to **System Status > Alarms** and check for service-impacting alarms.

Installing the Avaya Aura® Media Server patches in High Availability

Before you begin

- Download the most recent Avaya Aura® Media Server QFE patches and store them in the QFE subdirectory. QFE patches are ZIP files, but do not unzip them. The Avaya Aura® Media Server patching utility uses the QFE ZIP files. For a Linux server, the default QFE folder location is `/opt/avaya/app/amsinst/ma/MAS/qfe`.
- Back up Avaya Aura® Media Server before applying patches.

About this task

Install a new QFE patch to apply a change to the Avaya Aura® Media Server system. This procedure forces the backup server to become the active instance when the primary server is stopped.

Review *Avaya Aura® Contact Center Release Notes* and follow the instructions in each Avaya Aura® Media Server patch Readme file.

Procedure

1. Navigate to Element Manager for the backup Avaya Aura® Media Server node you want to patch.
2. In the navigation pane, click **System Status > Element Status**.
3. Click **Stop** and confirm the operation on the following page.
4. Close Element Manager.
5. On the backup server, open a Linux terminal.
6. On the backup server, change to the root user by running the `su -` command.
7. Run the `amspatch list all` command to obtain the correct name for the new QFE patch:
The name of the file is not necessarily the same as the name of the patch.
8. Under the **QFE Name** column, note the name of the patch.
9. Install the patches in numerical order.
 - To install a new patch on the system, run the `amspatch apply <patchname>` command, where `<patchname>` is the name of the patch.
 - To install all downloaded QFE patches on the system, run the `amspatch apply all` command.
10. When the patch application is complete, open the Element Manager navigation pane, and click **Tools > Software Inventory**.
11. Verify the patch version listed in the **Patch Level** column.
12. Navigate to **System Status > Element Status** and then click **Start**.
13. Confirm the operation.
14. Navigate to **System Status > Alarms** and check for service-impacting alarms.
15. Repeat the steps for the primary server.

Part 6: Network Control Center Server migrations and patches

- [Network Control Center server migration](#) on page 299
- [Network Control Center Server patch installation](#) on page 329

Chapter 18: Network Control Center server migration

This chapter describes how to migrate Avaya Aura® Contact Center Release 6.x to a new server running Avaya Aura® Contact Center Network Control Center Release 7.1.x. This chapter also describes how to migrate Network Control Center Release 7.1.x from one server to another.

Existing system	New server
Avaya Aura® Contact Center Network Control Center Release 6.x on Windows Server 2008 R2	Avaya Aura® Contact Center Network Control Center Release 7.1 on Windows Server 2016 or Windows Server 2019
Avaya Aura® Contact Center Network Control Center Release 7.0 on Windows Server 2012 R2	
Avaya Aura® Contact Center Network Control Center Release 7.1.x on Windows Server 2016 or Windows Server 2019	

This chapter describes how to migrate to a Network Control Center Server in a solution with a CS 1000 or an Avaya Aura® Unified Communications platform.

You can use the procedures in this chapter to:

- Migrate data from your existing Network Control Center server to a new server.
- Migrate a Network Control Center server to a new server. For example, to move Network Control Center server software from one server to a new larger and faster server.

A Network Control Center server includes the following software:

- Network Control Center (NCC)
- Contact Center License Manager (LM)
- Contact Center Manager Administration (CCMA)

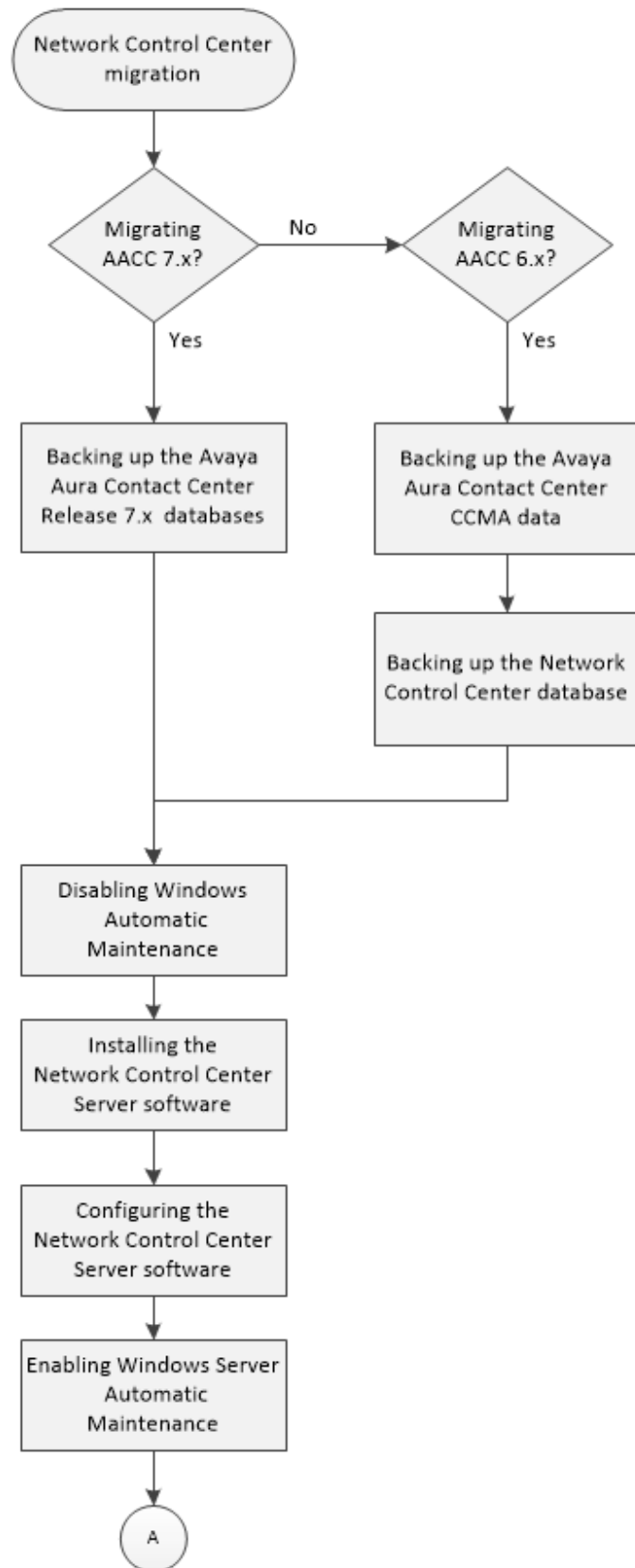
Network Control Center Server migration prerequisites

- Ensure that your hardware meets all requirements as described in *Avaya Aura® Contact Center Overview and Specification*.
- Prepare your new server for software installation. For more information see, [Common server preparation procedures](#) on page 45.

Network Control Center Server migration procedures

About this task

This task flow shows you the sequence of procedures you perform to migrate to an Avaya Aura® Contact Center Release 7.1 Network Control Center Server.

**Figure 14: Network Control Center Server migration procedures**

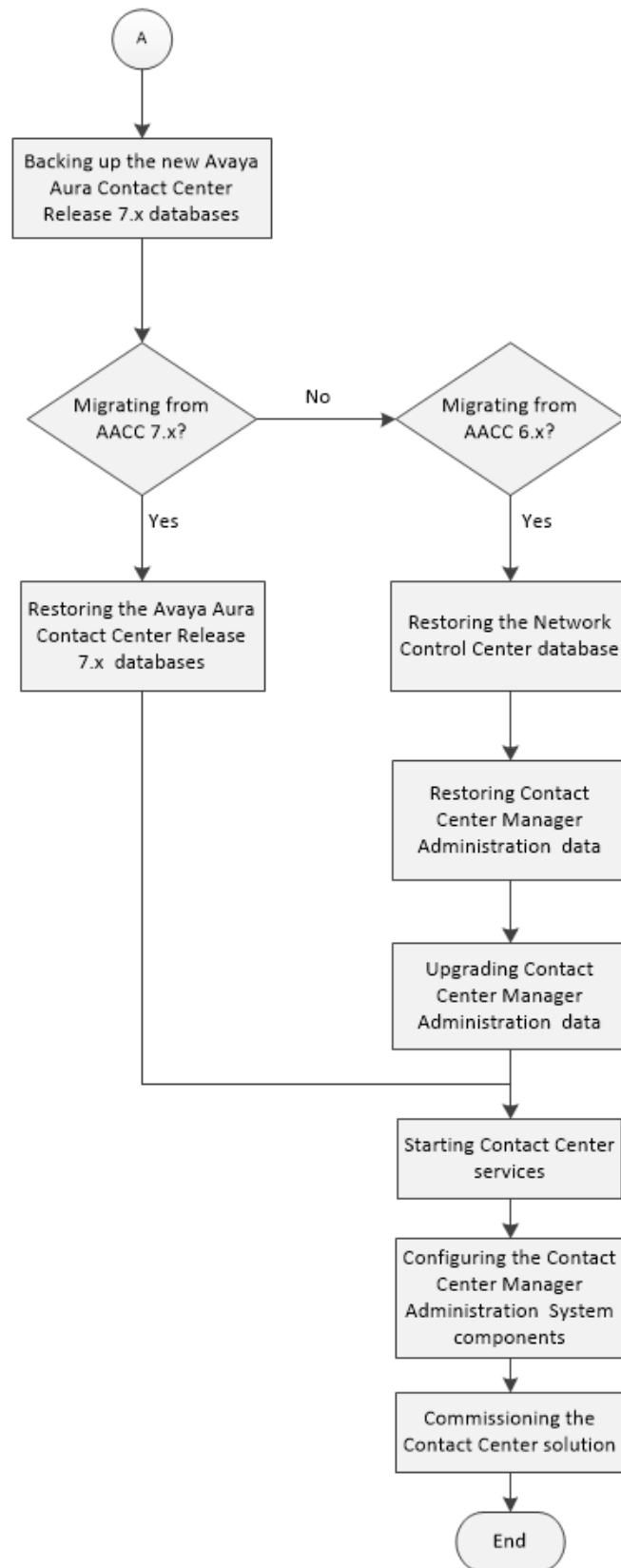


Figure 15: Network Control Center Server migration procedures continued

Backing up the Avaya Aura® Contact Center Release 7.1 databases

About this task

Back up the Avaya Aura® Contact Center Release 7.1 databases so you can restore them on the new server after you install the Avaya Aura® Contact Center Release 7.1 software.

Procedure

1. Log on to the existing Avaya Aura® Contact Center Release 7.1 server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
4. In the right pane, click **Create**.
5. From the **Drive Letter** list, select the network drive on which to store the Voice Contact Server database.
6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.
7. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the user password.
9. Click **Save**.
10. Click **OK**.
11. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
12. In the **Media Type** section, select **Network Location**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.
15. Click **Yes**, to continue with the backup.

Backing up the Avaya Aura® Contact Center CCMA data

Before you begin

- Map a network drive on which to back up your database. The network drive must be in NTFS format.
- Log on to the Contact Center Manager Administration server as an administrator.

About this task

Back up the Contact Center Manager Administration data on the source server Release 6.x to enable migration of the data to the new Contact Center server.

If your Contact Center Manager Administration uses High Availability replication, you must backup the data from the active CCMA.

Procedure

1. On the server with CCMA, choose **Start > All Programs > Avaya > Contact Center > Manager Administration > Configuration**.
2. In the left pane of the **Avaya Configuration** window, expand **Avaya > Applications > Backup & Restore**.
3. In the right pane, click **Backup & Restore**.
4. In the **Contact Center Manager Administration - Backup And Restore** dialog box, click **Backup** tab.
5. Select **Drive**.
6. Type the drive where the backed up database is stored.
7. Click **Next**.
8. In the **Perform Backup** section, select **Run Now**.
9. Click **Next**.
10. In the **Username** box, type a user name with administrative privileges for the server to which you store the backup.
11. In the **Password** box, type a password with administrative privileges for the server to which you store the backup.
12. From the **Domain** list, select the domain of the server to which you store the backup.
13. Click **Finish**.

Backing up the Avaya Aura[®] Contact Center Network Control Center database

About this task

Back up the Avaya Aura[®] Contact Center Network Control Center database so you can restore it on the new server after you install the Avaya Aura[®] Contact Center Network Control Center Server software.

Procedure

1. On the Network Control Center server, click **Start > All Programs > Avaya > Database Maintenance**.

2. In the Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the Backup Locations pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which you want to store the Network Control Center database.
5. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.
9. Click **OK**.
10. In the Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Applications** section, select **CCMS**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.

Disabling Windows Server Automatic Maintenance

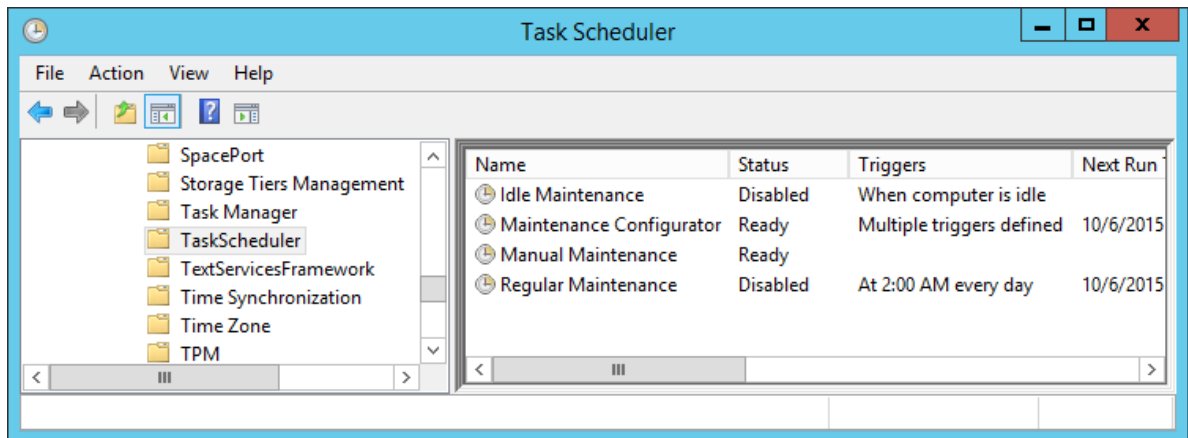
About this task

Disable Windows Server Automatic Maintenance while installing Contact Center software. Windows Server Automatic Maintenance can occasionally interfere with the real-time requirements for Contact Center. You must therefore temporarily disable Automatic Maintenance to install and configure Contact Center software. Re-enable it after deploying Contact Center.

Procedure

1. Log on to the Contact Center server as an administrator.
2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Disable**.

5. In the **Name** column, right-click **Regular Maintenance** and then click **Disable**.



6. From the **File** menu, click **Exit**.

Installing the Network Control Center Server software

Before you begin

- If you install Network Control Center server software with an AML Avaya Communication Server 1000, ensure the PABX is configured. See *Avaya Aura® Contact Center and Avaya Communication Server 1000 Integration*.
- If you install Network Control Center server software with an Avaya Aura® Unified Communications platform, ensure the platform is configured. See *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.
- Download the most recent Network Control Center patches to the server.

About this task

Install the Network Control Center server software to enable your contact center to route contacts to available agents with the correct skills.

Procedure

1. Insert the Contact Center DVD into the DVD drive of your server.
2. If the installation does not automatically start, double-click **Setup.exe**.
3. Click **Accept** to install the Microsoft .NET Framework on the server.

If you are prompted to accept the Microsoft .NET Framework license agreement, click **Accept**. If you are prompted to restart the server, click **Yes** and repeat step 2.

4. Contact Center software installer runs Operating System and hardware checks on the server. If the installer returns a Fail, the software installation cannot proceed until you correct the problem. Review any failures returned by the System Readiness Check and consult *Avaya Aura® Contact Center Overview and Specification* to determine the actions to resolve the issue.

You can ignore warnings if the potential impact to the operation of the contact center is understood and not applicable.

5. The Contact Center software installer platform and server selection screen appears.

The screenshot shows the Avaya Aura Contact Center 7.1 installer window. The title bar is red with the Avaya logo and the text 'Avaya Aura® Contact Center 7.1'. The main content area is white with a red border. It contains two sections: 'Select Voice Platform' and 'Select Server Installation Option'. The 'Select Voice Platform' section has two radio buttons: 'Avaya Aura® - SIP' (selected) and 'Avaya Communication Server 1000 - AML'. To the right of this section is a text box explaining that integrating with a SIP-enabled Avaya Aura Unified Communications platform gives Contact Center access to and control of Avaya Aura phones and includes Contact Center in the solution's dial plans. The 'Select Server Installation Option' section has five radio buttons: 'Voice and Multimedia Contact Server with Avaya Aura® Media Server', 'Voice and Multimedia Contact Server without Avaya Aura® Media Server', 'Voice Contact Server Only', 'Multimedia Contact Server Only', and 'Network Control Center Server Only'. Below this section is a checkbox labeled 'Configure Workspaces for Avaya Aura Contact Center'. To the right of this checkbox is a text box explaining that selecting this checkbox configures and uses Avaya Workspaces in your SIP-enabled contact center solution. At the bottom right of the window is a 'Cancel' button.

6. Select the type of Network Control Center server to install:

In an Avaya Communication Server 1000 (CS1000) based solution, in the **Select Voice Platform** section, select **Avaya Communication Server 1000 - AML**.

In a SIP-enabled solution, in the **Select Voice Platform** section, select **Avaya Aura - SIP**.

7. In the **Select Server Installation Option** section, select **Network Control Center Server Only**.
8. Click **Next**.
9. Under **Journal Database Drive**, select the drive for the database journal.
10. Under **Voice Contact Server Database Drive**, select the drive for the database.
11. In the **Service Packs** section, browse to and select the Service Pack.



12. Click **Install**.
13. The **AVAYA GLOBAL SOFTWARE LICENSE TERMS** window appears.
14. Read the terms of the license.
 - If you accept the terms, click **I ACCEPT THE LICENSE TERMS**. *The installation continues.*
 - If you do not accept the terms, click **I DECLINE THE LICENSE TERMS**. *The installation returns to the Select Destination Drive screen.* Click **Cancel** to stop the install.
 - To print the license terms, click **Print**.
15. The **MICROSOFT SOFTWARE LICENSE TERMS** window appears.
16. Read the terms of the license.
 - If you accept the terms, click **I ACCEPT THE LICENSE TERMS**. *The installation continues.*
 - If you do not accept the terms, click **I DECLINE THE LICENSE TERMS**. *The installation returns to the Select Destination Drive screen.* Click **Cancel** to stop the install.
 - To print the license terms, click **Print**.

17. The **Progress** window appears and displays the installation progress.
18. When the software is installed, you have the following options.
 - To continue configuring the server installation data:
 - a. Select **Launch Avaya Aura Contact Center Ignition Wizard**.
 - b. Click **Configure**. This starts the Avaya Aura® Contact Center Ignition Wizard.
 - To defer configuring the server installation data:
 - a. Clear **Launch Avaya Aura Contact Center Ignition Wizard**.
 - b. On the message box, click **Yes**.
 - c. On the main installer screen, click **Close**.
 - d. Follow the on-screen instructions and shut down the Contact Center server.

You must use the Ignition Wizard to initialize Avaya Aura® Contact Center, otherwise Avaya Aura® Contact Center is not operational. For more information about the Ignition Wizard, see the following procedures.

Configuring the Network Control Center Server software

Before you begin

- If you install Network Control Center server software with an AML Avaya Communication Server 1000, ensure the PABX is configured. See *Avaya Aura® Contact Center and Avaya Communication Server 1000 Integration*.
- If you install Network Control Center server software with an Avaya Aura® Unified Communications platform, ensure the platform is configured. See *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.
- You must configure the required language and locale of the Contact Center server operating system, if it is not a Latin-1 language, before configuring the Contact Center server using the Contact Center Ignition Wizard. For more information about configuring language and locale settings on the Contact Center server, see *Avaya Aura® Contact Center Server Administration*.
- Download the most recent Network Control Center patches to the server.

About this task

Configure the Network Control Center server software to enable your contact center to route contacts to available agents with the correct skills.

Procedure

1. Log on to the Contact Center server using the Administrator account details.
2. On the Contact Center Ignition Wizard screen, click **Next**. If the Contact Center Ignition Wizard is not visible, click the Ignition Wizard shortcut on the desktop.

3. On the **End-User License Agreement** screen, read the license agreement. Optionally, click **Print** to generate a local soft copy (in OpenXPS Document format) of the license agreement.
4. Select **I Accept the Terms of the End-User License Agreement** and click **Next**.
5. On the **Configuration Data** window, type the configuration details for each tab.
6. Select the **Core** tab, and configure the server details.

7. In the **Site Name** box, type the site name for the Contact Center server. The site name must not contain spaces or non-alphabetical characters except hyphen (-) and underscore (_). The first character must be a letter. The site name must be unique and can consist of 6 to 15 characters.
8. In the **System Account Configuration** section, in the **Password** box, type a password for the Contact Center administration account. The password is not checked against the server security policy for minimum password requirements. Avaya recommends that you enter a password that conforms to your corporate password policy.
9. In the **Confirm Password** box, type the password.
10. Select the **Licensing** tab, and configure the licensing details.

The screenshot shows the 'Configuration Data' window for Avaya Contact Center. The 'Licensing' tab is selected. The window contains the following fields and controls:

- License Type:** A drop-down menu with 'Standard KRS' selected.
- License File:**
 - License File Location:** A text input field with a 'Browse' button and a 'Skip' button.
 - System HostID (MAC Address):** A text input field containing '00:50:56:8D:48:8D'.
- License Manager Package:**
 - Package:** A drop-down menu with 'Nodal NCC' selected.
 - Features:** A list box containing 'Universal Networking' with an unchecked checkbox.

At the bottom, there are navigation buttons: '< Back', 'Next >', and 'Cancel'. A 'Click Next to Continue' instruction is also present.

11. From the **License Type** drop-down list, select **Standard KRS**.
12. Click **Browse** to locate and load your license file.
13. From the **Licensing Package** list, select the license type that you have purchased. Select **Nodal NCC** for single-site contact centers. Select **Corporate NCC** for multi-site contact centers.
14. From the list of **Optional Packages**, enable the licensed features that you have purchased.
15. Select the **Security Configuration** tab, and configure the security details in the **Security Store Details** section.

The screenshot shows the 'Configuration Data' window for Avaya Contact Center. The 'Security Configuration' tab is selected. The 'Security Store Details' section contains fields for 'Full Computer Name (FQDN)' (CC7SIP.aaccdomain.com), 'Encryption Algorithm Level' (SHA256), 'Key Size' (2048), 'Security Store Password', and 'Confirm Store Password'. The 'Name of Organizational unit' and 'Name of Organization' fields are empty. The 'City or Locality' and 'State or Province' fields are empty. The 'Two letter country code' field is empty. The 'Subject Alternative Name' section has a 'Type' dropdown set to 'DNS' and a 'Value' field. There are 'Add' and 'Remove' buttons. A 'Create Store' button is at the bottom right. A 'Skip Security Configuration' checkbox is at the bottom left. Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom.

16. If you do not want to enable security, select the **Skip Security Configuration** checkbox and skip to [the next steps](#) on page 315.

! Important:

A warning message appears. If you proceed without enabling security, you cannot fully commission your solution. For example, in SIP-enabled contact centers that use Voice, the SIP CTI link is disabled until you configure Contact Center TLS certificates to communicate securely with Application Enablement Services.

17. In the **Full Computer Name (FQDN)** box, type the full FQDN of the server on which you are creating the security store.

! Important:

The FQDN must be the full machine name of the server that the Security Store resides on. The FQDN name is case-sensitive.

18. In the **Name of Organizational unit** box, type the name of the department or division within the company.
19. In the **Name of Organization** box, type the company name.
20. In the **City or Locality** box, type the name of the city or district in which the contact center is located.

21. In the **State or Province** box, type the state or province in which the contact center is located.
22. In the **Two Letter Country Code** box, type the country code in which the contact center is located.
23. In the **Security Store password** box, type a password for accessing the new security store.
24. In the **Confirm Store password** box, confirm the password for accessing the new security store.

 **Important:**

Ensure you remember this password, because you need it when you log on to Security Manager after install. If you forget the password, you cannot access Security Manager.

25. If you are implementing High Availability in the contact center, generate the security store using Subject Alternative Names (SANs). In the **Subject Alternative Name** section, for each SAN you want to add:
 - a. From the **Type** drop-down list, select DNS.
 - b. In the **Value** field, type the FQDN for the server.
 - c. Click **Add**.

For a High Availability system, add the current server FQDN and the Managed name for the HA pair.

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

The default value for **Encryption Algorithm** is SHA256 and the default value for **Key Size** is 2048.

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

27. Click **Create Store**.
28. You can now use the **Security Configuration** tab to create and save a Certificate Signing Request (CSR) file.

The screenshot shows the 'Avaya Contact Center' window with the 'Configuration Data' tab selected. The 'Security Configuration' sub-tab is active. The main heading is 'Configuration Data' with the AVAYA logo. Below it, a message says 'Enter the required configuration data.' The 'Security Configuration' tab is selected, showing a section titled 'Store created – Generate Identity Security Certificate by signing the Certificate Signing Request provided.' This section includes a 'Certificate Signing Request file' field with a 'Create CSR File' button. Below this is an 'Add' button and a list of 'Imported Trusted Certificate Authority Root Certificate(s)' with a 'Remove' button. There is also a field for 'Imported Identity Security Certificate' with a 'Remove' button. On the right, a 'Status' panel contains instructions: 'Ensure that a removable or network drive is available.', 'Create the Certificate Signing Request file and save it to a removable or network drive.', and 'Alternatively, to defer Security Configuration and continue with the Initiation Wizard.' with a 'Reset' button. At the bottom, there are navigation buttons: '< Back', 'Next >', and 'Cancel'.

29. Click **Create CSR File**.

30. From the **Save In** drop-down list, select a shared location in which to save the CSR file and click **Save**.

You must now send the Certificate Signing Request file to a Certificate Authority and receive a signed certificate and root certificate to import to the security store.

31. Click **Add** to import certificates. In the **Open** dialog box, navigate to the location of a certificate and click **Open**. To remove the imported certificate, select the required certificate from the list and click **Remove**.

You can import either a chained certificate, or separate root and signed certificates. Root certificates appear in the **Imported Trusted Certificate Authority Root Certificate(s)** section. A signed certificate appears in the **Imported Identity Security Certificate** section.

If a chained certificate contains both root and signed certificates, you can add root certificates and signed certificate simultaneously by importing just one chained certificate.

If a chained certificate contains root certificates only, you can use the chained certificate to add all root certificates at a time. To add a signed certificate, click **Add** and navigate to the required signed certificate.

If you have separate root and signed certificates, you must add them one by one by clicking the **Add** button. Always add a signed certificate last.

! Important:

When adding a chained certificate, the system can ask you to enter the password you created for accessing the security store. See [the previous steps](#) on page 313.

32. Click **Next**.
33. Review and verify the summary information, and click **Configure**.
34. After the installation is complete, click **Finish**.
35. If prompted, restart the server.

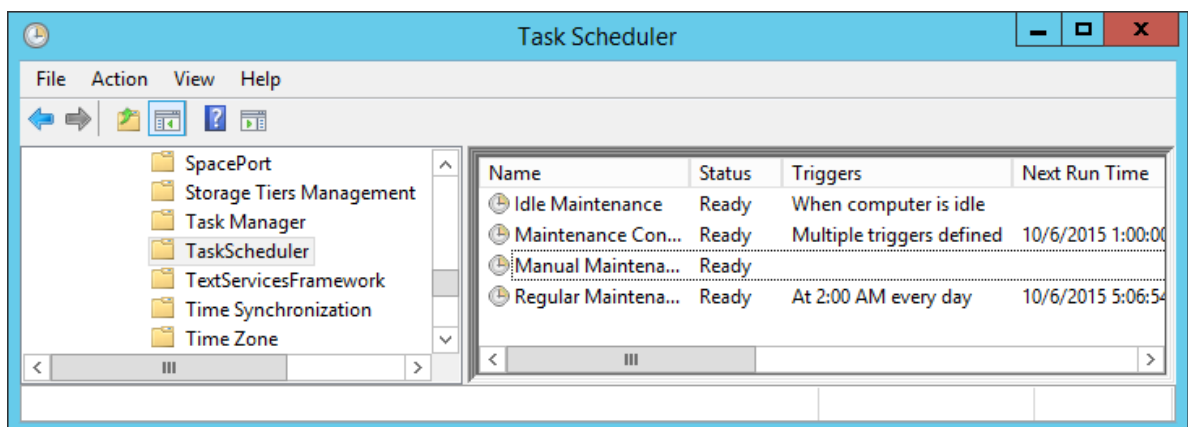
Enabling Windows Server Automatic Maintenance

About this task

Enable Windows Server Automatic Maintenance after deploying Contact Center software.

Procedure

1. Log on to the Contact Center server as an administrator.
2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Enable**.
5. In the **Name** column, right-click **Regular Maintenance** and then click **Enable**.



6. From the **File** menu, click **Exit**.

Backing up the new Avaya Aura® Contact Center Release 7.1 databases

About this task

After running the Ignition Wizard, backup the Avaya Aura® Contact Center Release 7.1 databases.

The backup databases capture the system in a known clean state and these might be required later if issues arise during data migration.

Procedure

1. Log on to the new Avaya Aura® Contact Center Release 7.1 server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
4. In the right pane, click **Create**.
5. From the **Drive Letter** list, select the network drive on which to store the databases.
6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.
7. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the user password.
9. Click **Save**.
10. Click **OK**.
11. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
12. In the **Media Type** section, select **Network Location**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.
15. Click **Yes**, to continue with the backup.

Restoring the Network Control Center Release 7.1 databases

Before you begin

- Back up the old Network Control Center databases.

- On the new server, map a drive to the Network Control Center database backups.

! Important:

When you migrate configuration information from the old server to the new server, do not run the two application servers simultaneously. Both applications are configured the same, so they attempt to access and control the same resources. Continuing to run the old applications in the Contact Center can result in unpredictable behavior.

About this task

Restore the Network Control Center Release 7.1 databases. After you complete this procedure, you must restart your server

! Important:

You must complete this procedure to ensure all databases are restored at the same time.

Procedure

1. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
2. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the Backup Locations pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which you stored the Network Control Center database backup.
5. In the **UNC Path** box, type the location of the Network Control Center databases in the format \\Computer Name\Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.
9. Click **OK**.
10. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Restore**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Application** section, select **CCMS**, **ADMIN**, and **CCMA**.
13. In the **Restore contents** section, select **Data**.
14. From the **Backup Location** list, select the network drive containing the backed up Network Control Center server databases.
15. Click **Restore**.
16. Click **Yes**.
17. Use the **Progress information** field to monitor the progress of the restoration.

18. On the **Database Maintenance** message box, click **OK**.
Wait for the restore to complete.
19. From the **Start** menu, in the Avaya area, click **Server Configuration**.
20. In the Server Configuration dialog box, click **Apply All**.
21. Restart the Network Control Center server.

Restoring the Network Control Center Server database

Before you begin

- Back up the old Network Control Center Server database.
- On the new server, map a drive to the Network Control Center database backup.

About this task

Restore the Network Control Center Server database to migrate the data to the new server.

Procedure

1. Log on to the new Network Control Center server.
2. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
3. In the Database Maintenance dialog box, in the Main Menu pane, click **Backup Locations**.
4. In the Backup Locations pane, click **Create**.
5. From the **Drive Letter** list, select the network drive on which you stored the Network Control Center database backup.
6. In the **UNC Path** box, type the location of the Network Control Center database in the format \\Computer Name\Folder\Backup Location. This must precisely match the location you specified when you backed up the old database.
7. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the user password.
9. Click **Save**.
10. Click **OK**.
11. In the Database Maintenance dialog box, in the Main Menu pane, click **Restore**.
12. In the **Media Type** section, select **Network Location**.
13. In the **Application** section, select **CCMS**.
14. In the **Restore** contents section, select **Data**.

15. From the **Backup Location** list, select the network drive containing the backed up Contact Center Manager Server database.
16. Click **Restore**.

Restoring Contact Center Manager Administration data

Before you begin

- Know the network location (in Universal Naming Convention (UNC) format) of the drive for the backed up data.

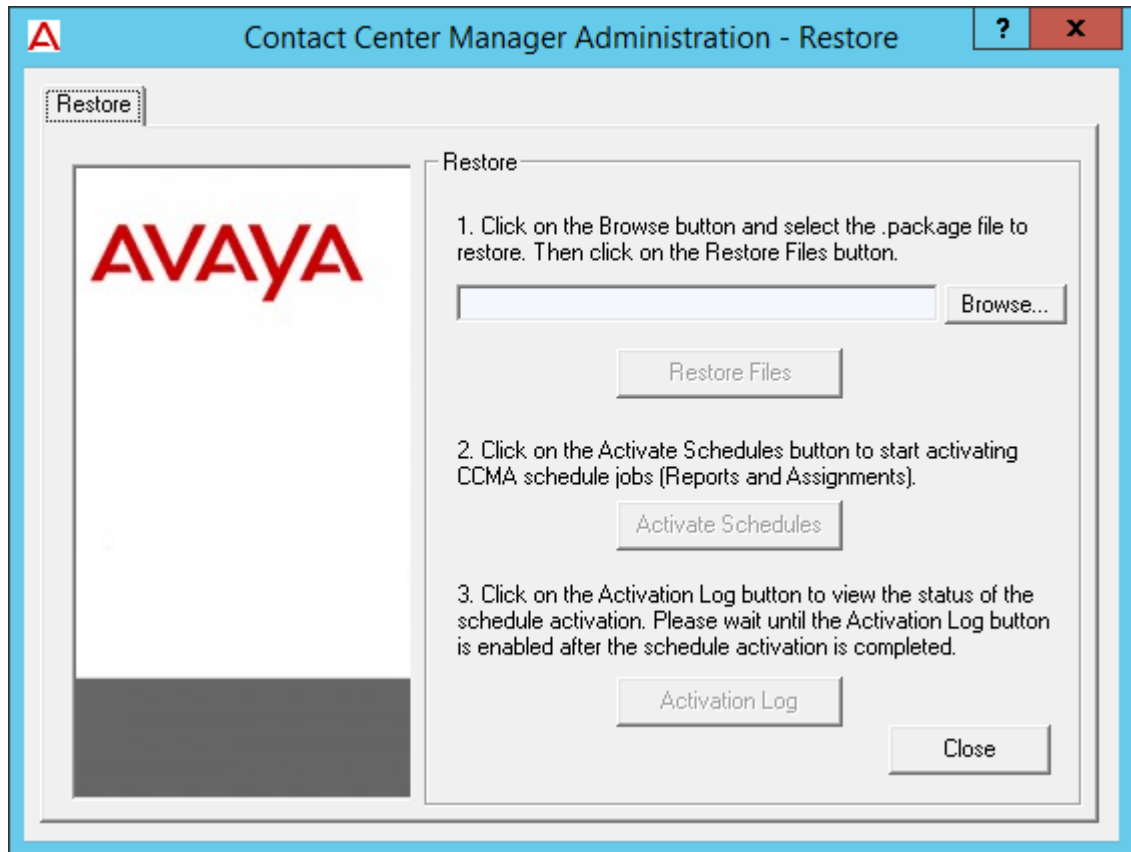
About this task

Restore the Contact Center Manager Administration data to migrate the data to the new server. Use this procedure if you are restoring Avaya Aura® Contact Center Contact Center Manager Administration data. You must restore the CCMA database as part of a matched set; the CCMA data must be restored to the same server as its corresponding databases (for example, CCMS, CCT, or CCMM).

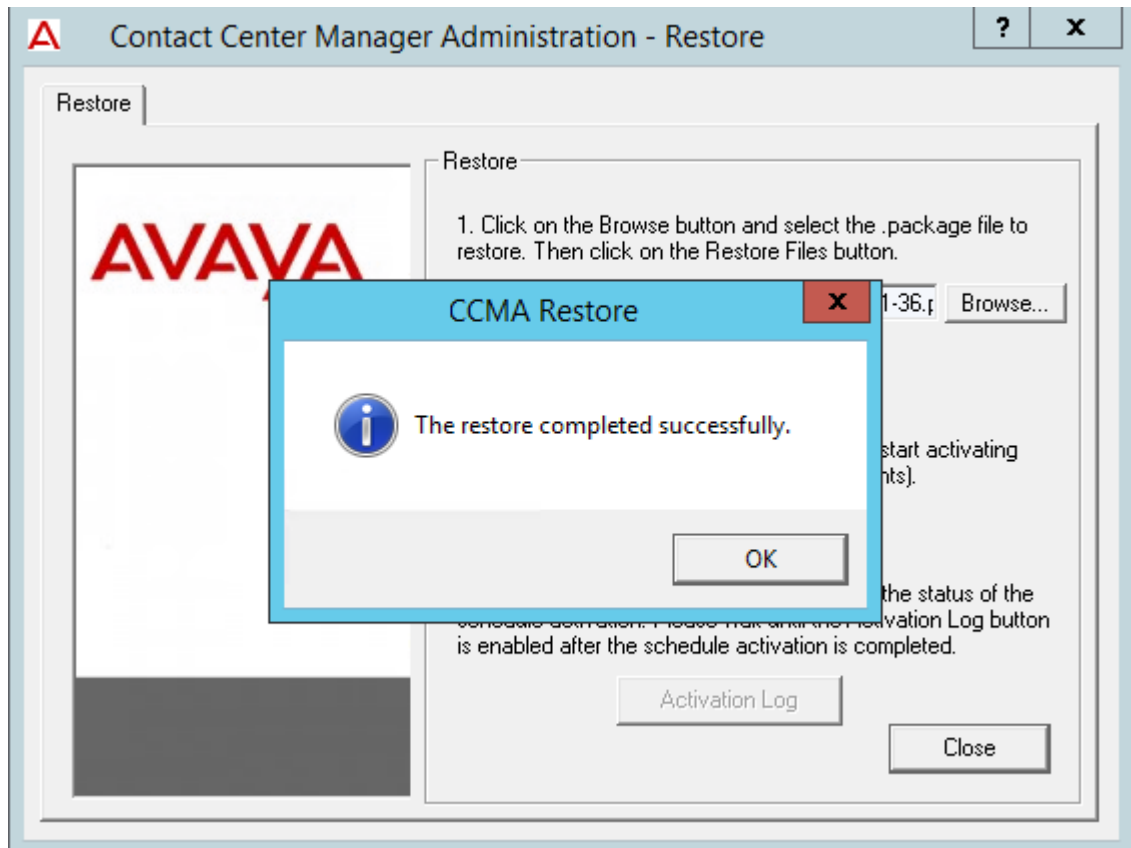
Procedure

1. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.
2. In the left pane of the Avaya Configuration window, expand **Avaya > Applications > Restore**.
3. In the right pane, click **Restore**.
4. On the **Restore** message box, click **OK**.

5. In the **Contact Center Manager Administration - Restore** dialog box, click the **Restore** tab.



6. To select a backup file to restore from, click **Browse**.
 7. In the **Select a backup file** dialog box, select the required .package file.
 8. Click **Open**.
 9. To restore the backup file data onto the administration data server, click **Restore Files**.
- The restore completed successfully message box appears.



10. Click **OK**.

Upgrading the Contact Center Manager Administration data

Before you begin

- Restore the backed up Contact Center Manager Administration (CCMA) data.

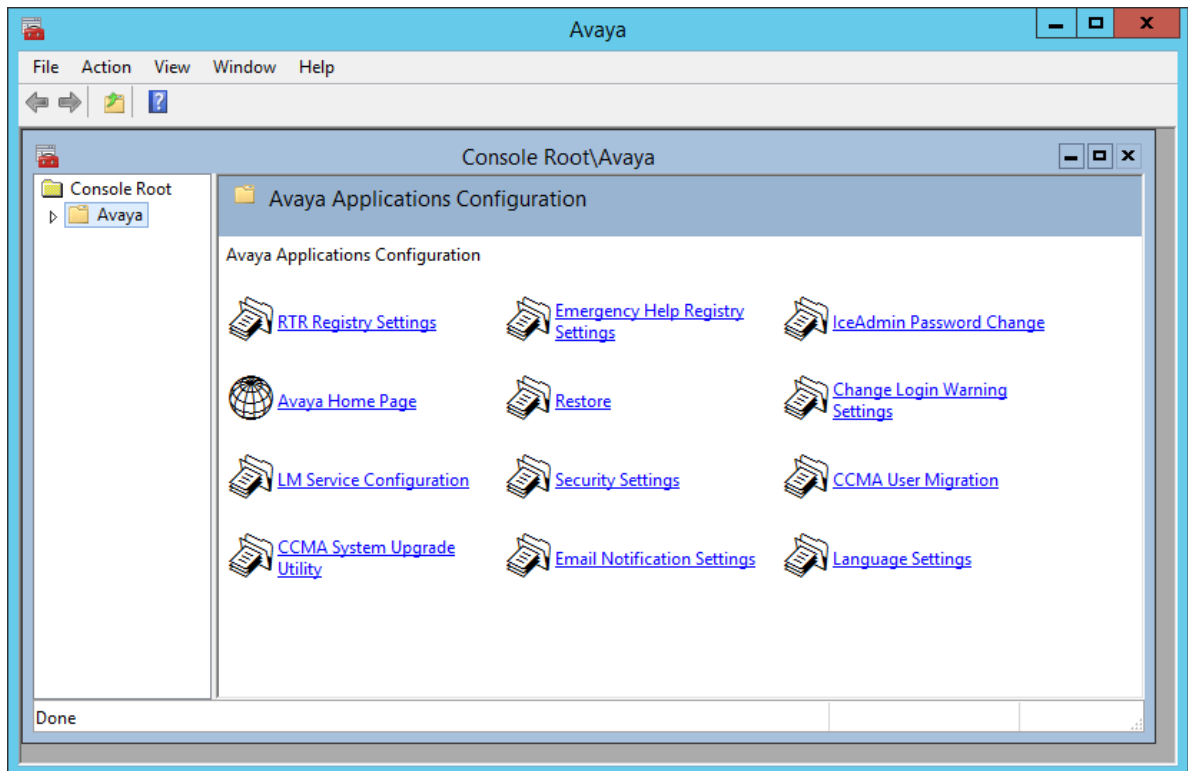
About this task

Upgrade Contact Center Manager Administration (CCMA) data to the Intersystems Caché database format used by Avaya Aura® Contact Center Release 7.1.

Procedure

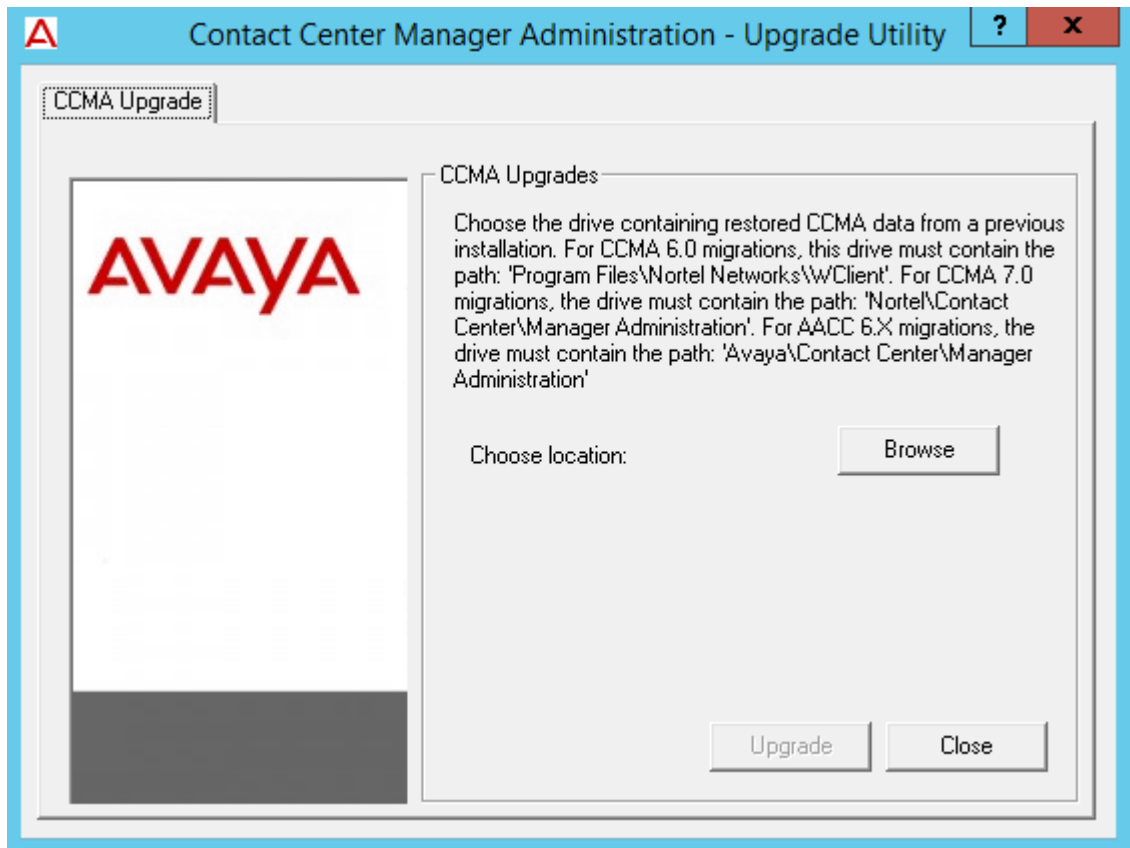
1. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.

2. In the left pane, click **Avaya** > **Applications** > **CCMA System Upgrade Utility**.



3. In the right pane, click **CCMA System Upgrade Utility**.

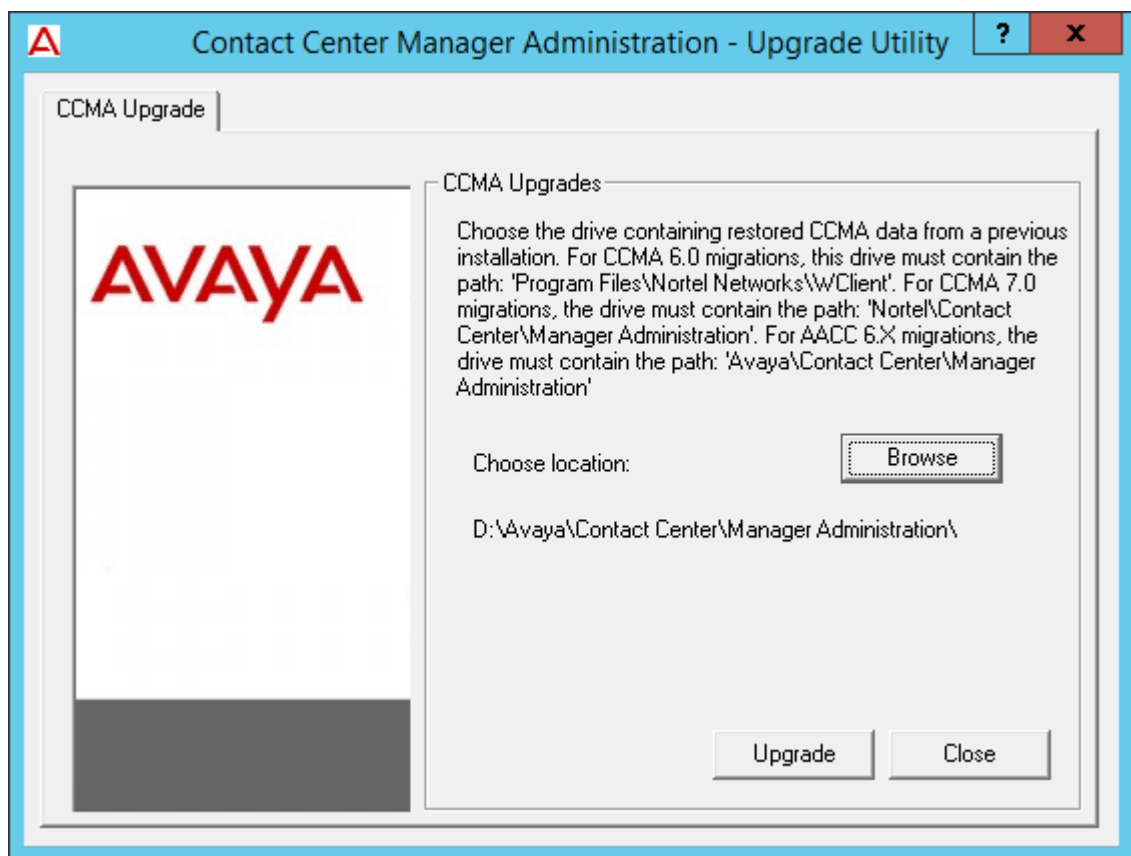
4. Click **Yes** on the confirmation dialog box.



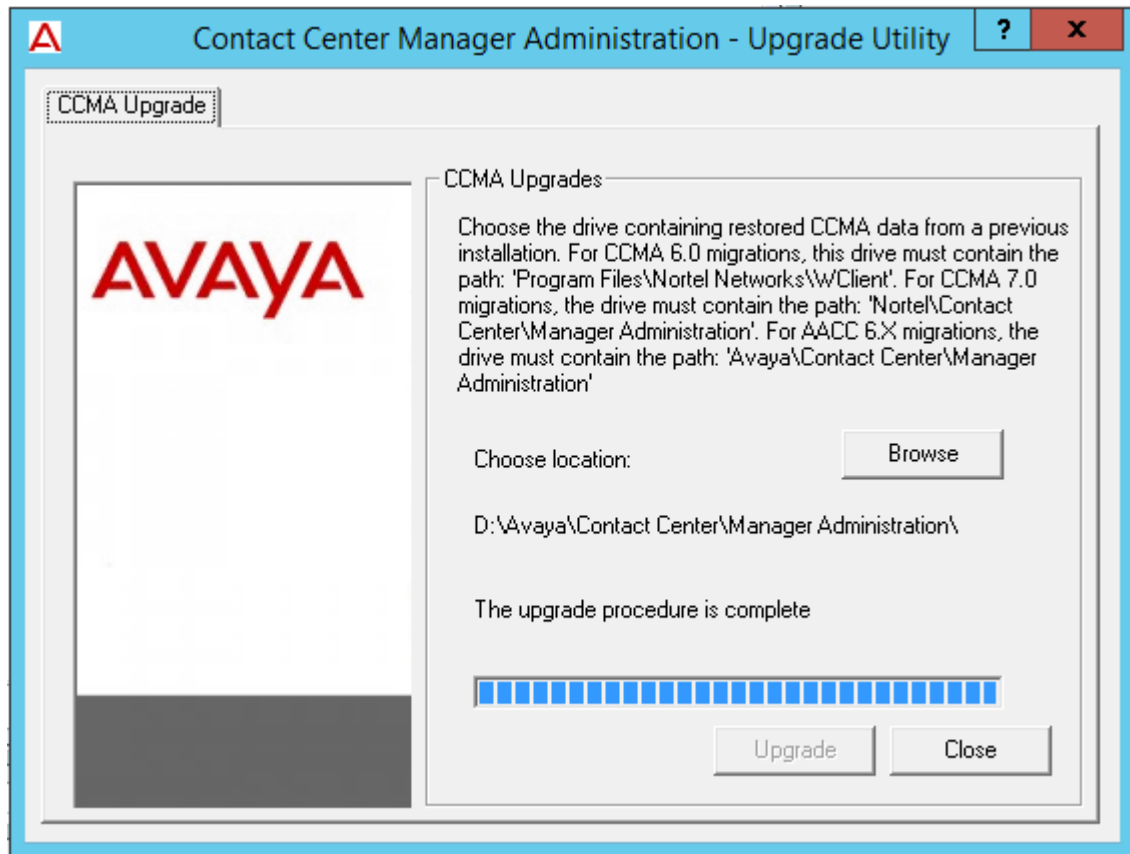
5. On the Upgrade Utility, click **Browse** and follow the instructions on the **CCMA Upgrades** screen to choose a location.

Select only the drive letter as the location of the restored CCMA data. The upgrade utility automatically detects and appends the correct directory structure for the old system data.

Example of upgrading from an Avaya Aura® Contact Center Release 6.4 system:



- Click **Upgrade**.



- Close the Upgrade Utility application. Click **Close**.

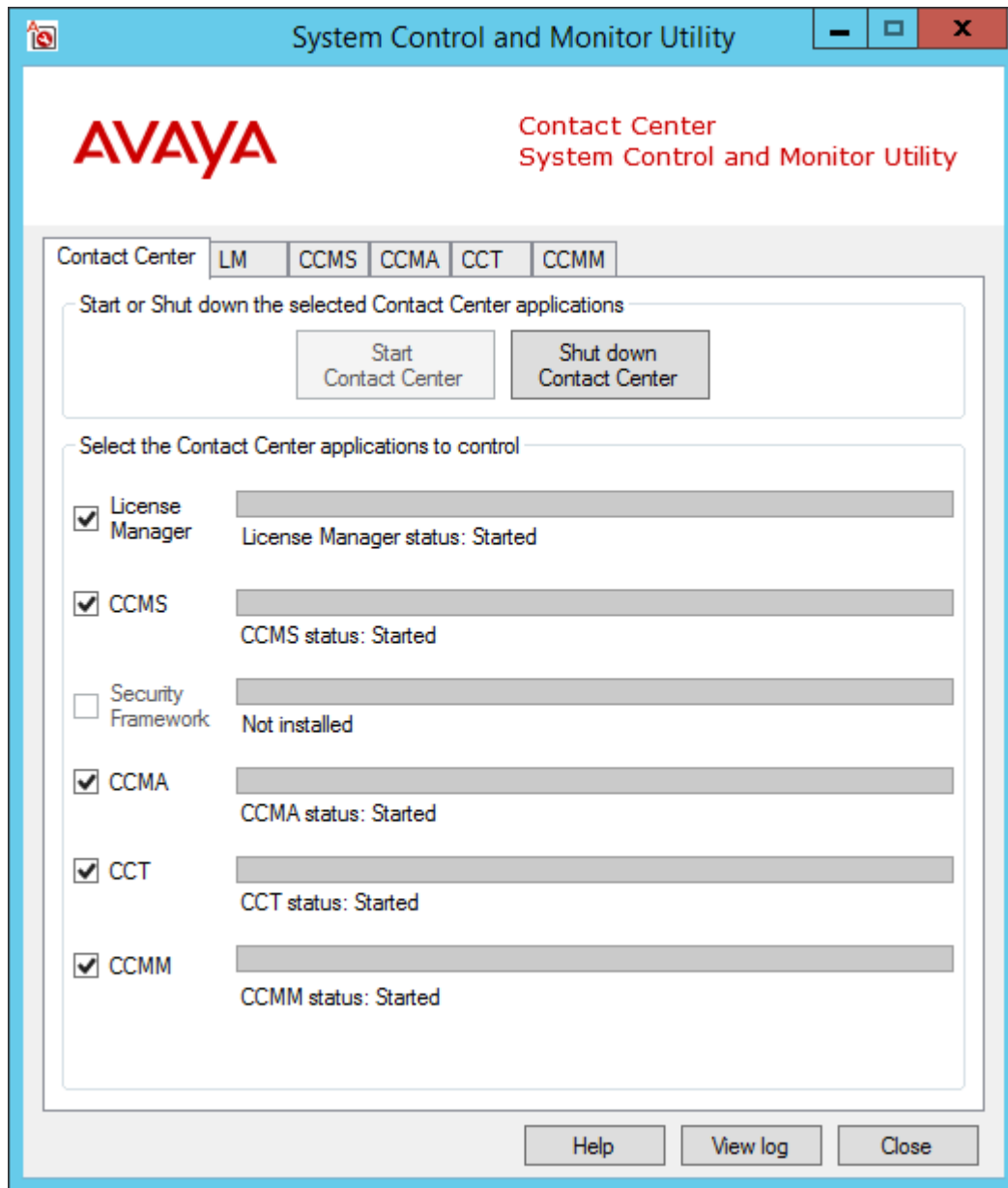
Starting Contact Center services

About this task

Start the Contact Center services to begin re-configuration after migrating or upgrading a system. The database restore and upgrade utilities automatically stop Contact Center services. Start Contact Center services to continue commissioning the solution.

Procedure

- Log on to the Contact Center server.
- From the **Start** menu, in the Avaya area, click **System Control and Monitor Utility**.
- Click the **Contact Center** tab.
- Click **Start Contact Center**.



Wait for Contact Center services to start.

Configuring the Contact Center Manager Administration system components

About this task

Configure the Contact Center Manager Administration (CCMA) system components for the new solution. Ensure that the Contact Center Manager Server (CCMS) settings are correct for the new solution.

To access CCMA and other Contact Center components, you must use the Microsoft Edge browser in Internet Explorer mode.

Procedure

1. In your browser, type the URL of the server and then press **Enter**.
The default URL is `https://<server name>`, where `<server name>` is the host name of the Avaya Aura® Contact Center Release 7.1.x server. If you turned off Web Services security, use `http://<server name>`.
2. On the main login page, in the **User ID** field, type the username.
The default user ID is `webadmin`.
3. In the **Password** box, type the password.
The default password is `webadmin`.
4. Click **Log In**.
5. On the launchpad, click **Configuration**.
6. In the left pane, right-click the CCMS server name and then click **Edit Properties**.
7. Update the Contact Center Manager Server details to match your new solution and then click **Submit**.
8. In the left pane, right-click the CCMS server name and then click **Refresh Server**.
9. On both Contact Center Manager Administration dialogs, click **Yes**.
10. Log off from CCMA.
11. Using the System Control and Monitor Utility (SCMU), restart Avaya Aura® Contact Center services.

Commissioning the Contact Center solution

About this task

Commission the Contact Center solution.

Procedure

1. After migrating your server and restoring the server databases, some of the old configuration settings might not match your new solution. Commission your new server in the new solution. For more information, refer to *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000* or *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications*.
2. Use the procedures in *Avaya Aura® Contact Center Server Administration* to configure your licensed features.

Chapter 19: Network Control Center Server patch installation

This chapter describes how to install patches on Network Control Center Server. Apply patches to resolve product issues.

A Network Control Center Server includes the following server software:

- Network Control Center (NCC)
- Contact Center License Manager (LM)
- Contact Center Manager Administration (CCMA)

Network Control Center Server patch installation prerequisites

- Download the most recent documentation. See [Downloading the most recent documentation](#) on page 45.
- Download and review the latest Avaya Aura® Contact Center Release Notes. The Release Notes contain information about known issues, patches, and workarounds specific to a release and patch line-up of Contact Center. For more information about the Contact Center Release Notes, see the Avaya website (<http://support.avaya.com>).

Disabling Windows Server Automatic Maintenance

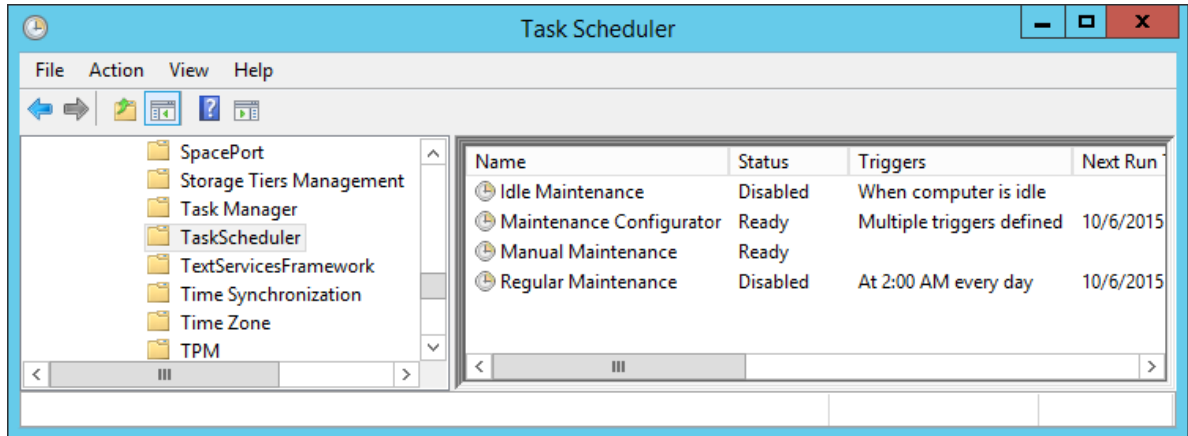
About this task

Disable Windows Server Automatic Maintenance while updating Contact Center software. Windows Server Automatic Maintenance can occasionally interfere with the real-time requirements for Contact Center. You must therefore temporarily disable Automatic Maintenance to update Contact Center software. Re-enable it after the update.

Procedure

1. Log on to the Contact Center server as an administrator.

2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Disable**.
5. In the **Name** column, right-click **Regular Maintenance** and then click **Disable**.



6. From the **File** menu, click **Exit**.

Installing Network Control Center Server Feature Packs and Service Packs

Before you begin

- Download the most recent Contact CenterRelease Pack, Feature Pack and Service Packs.
- Download the most recent Contact Center software patches.
- Back up the Contact Center databases.
- Temporarily stop Microsoft Windows Server Automatic Maintenance while you update Voice and Multimedia Contact Server software.
- Avoid installation from shared locations, because it might lead to installation failure. To ensure successful installation, mount the Release Bundle or install it locally.
- If you deploy in a virtual environment and want to install Avaya Workspaces, you must manually deploy three virtual machines using the Avaya Workspaces Open Virtual Appliance (OVA). See [Deploying the Avaya Workspaces OVA](#) on page 177.

About this task

Install the most recent Network Control Center Feature Pack and Service Packs to take advantage of new features, and to ensure that you have the most current development updates.

Procedure

1. Open the Release Pack, Feature Pack or Service Pack ZIP file.
2. Browse to the Avaya Release Pack Installer directory.
3. Double-click `setup.exe` to launch the Contact Center Release Pack Installer.
4. If you downloaded GA patches along with the Release Pack:
 - a. Select **Yes**.
 - b. Click **Browse**.
 - c. On the Browse for Folder screen, browse to the folder where you downloaded the patches, and click **OK**.
5. On the Contact Center Release Pack Installer screen, click **Next**.
6. On the Avaya Global License Terms screen, click **I ACCEPT THE LICENSE TERMS**.
7. On the MICROSOFT SOFTWARE LICENSE TERMS screen, click **I ACCEPT THE LICENSE TERMS**.
 The Avaya Release Pack Installer shuts down Contact Center and installs the Release Pack, Feature Pack or Service Pack.
8. When the software update completes successfully, click **Restart**.
 Contact Center reboots the server to finalize the installation.

Installing Network Control Center Server software patches

Before you begin

- Download the most recent Contact Center patches.
- Ensure that you have a recent backup of the Contact Center databases. Avaya recommends that you schedule a daily backup of the Contact Center databases at an off peak time. For more information on scheduling backups, see *Maintaining Avaya Aura® Contact Center*.
- Temporarily stop Microsoft Windows Server Automatic Maintenance while you update Network Control Center software.

About this task

Install the most recent Network Control Center software patches to ensure that you have the most current development updates.

Note:

The Network Control Center patches appear as CCMS patches.

Procedure

1. From the **Start** menu, in the Avaya area, click **Update Manager**.

2. Click **Install**.
3. Click **Browse** and navigate to the folder where you downloaded the patch.
4. Click **Scan for Updates**.

The Contact Center Updates section displays the available patches.

5. Select the appropriate patch.
6. Click **Install Selected Updates**.

The Update Manager installs the patch and displays a confirmation message.

7. Click **Close**.
8. Verify that the newly installed patch appears under Installed Updates.

Next steps

Re-enable Microsoft Windows Server Automatic Maintenance.

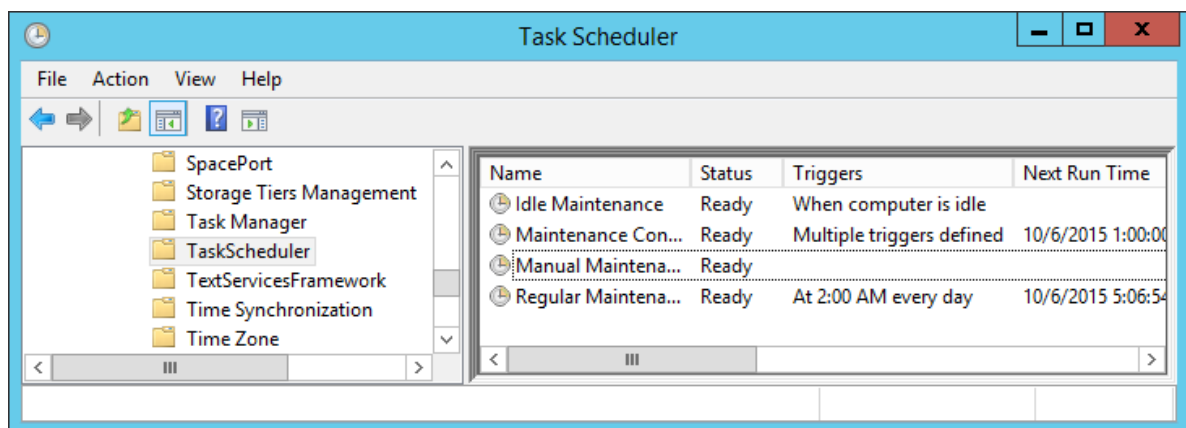
Enabling Windows Server Automatic Maintenance

About this task

Enable Windows Server Automatic Maintenance after updating Contact Center software.

Procedure

1. Log on to the Contact Center server as an administrator.
2. From the **Start** menu, click **Run** and type `Taskschd.msc`.
3. On the Task Scheduler window, in the left pane, click **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
4. In the **Name** column, right-click **Idle Maintenance** and then click **Enable**.
5. In the **Name** column, right-click **Regular Maintenance** and then click **Enable**.



6. From the **File** menu, click **Exit**.

Part 7: AML to SIP migrations

- [AML to SIP Migration](#) on page 335

Chapter 20: AML to SIP Migration

This chapter describes the tasks to complete the migration of the Contact Center servers from an AML-based contact center to a SIP-enabled one. There are many wider considerations when migrating from AML to SIP, including:

- Change of PABX from CS 1000 to Avaya Aura® Communication Manager.
- Change of telephony infrastructure.
- Potential change from Windows workgroup to Windows domain.
- Feature differences between the protocols.
- Voice services migration to Avaya Aura® Media Server.
- Changes to existing CTI applications based on MLSM.

For a complete understanding of the solution migration, download and read the *Avaya Aura® Contact Center CS1000 (AML) to Aura (SIP) Migration Guidelines* application note, available from support.avaya.com.

Supported migrations

You can migrate from the following AML-based contact centers:

- AACC R6.x
- AACC R7.x

Migrating High Availability solutions

If you are migrating from a solution with campus High Availability, you take all backups from the Active servers. You restore backups only to the new active servers, and then commission High Availability on Contact Center.

Prerequisites to completing the AACC migration

Before completing your migration to SIP-enabled Contact Center servers, you must:

- Install and commission your new SIP-enabled PABX.
- Record the sysadmin password on the AML-based system. The database restore on the SIP system restores this password, which you need for commissioning.
- Select the Contact Center server type to which you are migrating:
 - Voice and Multimedia Contact server with Avaya Aura® Media Server.
 - Voice and Multimedia Contact server without Avaya Aura® Media Server.
 - Separate Voice Contact Server and Multimedia Contact Server.

- Install the new Contact Center server(s) with AACC Release 7.x.
- Test the new Contact Center solution with a minimal configuration to ensure that your basic SIP configuration is correct.

Back up the working Contact Center databases and servers so that you can revert to a working system if you encounter issues in the migration.

- Take your AML-based Contact Center offline.
- Back up the databases from your AML-based Contact Center server(s), following the documentation for the Release from which you are migrating.

Turning off Web Services security

About this task

Turn off Web Services security before you restore a CCMM database from a system that did not have security enabled. If you are migrating from an Avaya Aura® Contact Center Release 7.x system that has Web Services security turned on, you can skip this procedure.

Before you begin

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

Procedure

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

Important:

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

2. From the **Start** menu, in the Avaya area, click **Security Manager**.
3. On the Store Access dialog, type the password for the security store, and click **OK**.
4. On the Security Manager screen, select the **Security Configuration** tab.
5. Click **Security Off**.
6. Click **Apply**.
7. On the Security Change Confirmation dialog, click **Confirm**.
8. Click **Log Out**.
9. Restart the Contact Center server.

Next steps

Complete the migration procedures in this book. After the migration, to complete your security configuration, follow the procedures in *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* or *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000*.

Migrating the Voice and Multimedia databases to the SIP-enabled server

Before you begin

- On the new SIP-enabled server, back up the Contact Center databases. You can use this database backup to roll back the migration data and return the new server to a fresh installed state.
- On the new server, map a drive to the old AML Contact Center database backups.

About this task

Migrate the CCMS, CCT, CCMM, and, if applicable, CCMM Offline databases to the new SIP-enabled server(s).

If you have separate Voice Contact Server and Multimedia Contact servers, migrate the CCMS and CCT databases to the Voice Contact Server. Then restore the CCMM and, if applicable, CCMM Offline database to the Multimedia Contact Server. For more information about restoring the Multimedia Contact server database, see [Restoring the Multimedia Contact Server database](#) on page 338.

If each source application backup is in a different backup location, you must map a drive to each of the CCMS, CCT, and CCMM database backup locations.

Procedure

1. Log on to the new SIP-enabled Contact Center server.
2. Click **Start > All Programs > Avaya > Database Maintenance**.
3. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
4. In the **Backup Locations** pane, click **Create**.
5. From the **Drive Letter** list, select the network drive on which you stored the source AML Contact Center database backups.
6. In the **UNC Path** box, type the location of the AML Contact Center databases in the format `\\Computer Name\Folder\Backup Location`.
7. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format `Computer Name\Account Name`.
8. In the **Password** box, type the user password.
9. Click **Save**.
10. If the source backups for each application are in different network locations, repeat steps 4 to 9 to map a drive for each location.
11. In the Main Menu pane, click **Migration**.
12. Select the system from which you are migrating the AML data.
 - If migrating from AACC 6.2 or 6.3, select **Avaya NES 7.0, AACC 6.2 or 6.3**.

- If migrating from AACC 6.4, select **AACC 6.4**.
 - If migrating from AACC 7.x, select **AACC 7.x**.
13. If you are migrating to a Voice and Multimedia contact server, select:
 - CCT
 - CCMS
 - CCMM
 - Offline (if migrating from AACC R6.4 or 7.x)
 14. If you are migrating to a Voice Contact Server, select:
 - CCT
 - CCMS
 15. From the **Migration Location** list, select the network drive containing the AML Contact Center database backups.

You can restore only the databases from a single selected migration location. If this location does not contain one of the database types you selected in steps 13 to 16, the migration fails.
 16. Click **Migrate**.
 17. On the **Are you sure you want to continue?** prompt, click **Yes**.
 18. Use the **Progress information** field to monitor the progress of the migration.
 19. Repeat this procedure if you have multiple backup locations from the AML Contact Center database backups, or if you are migrating to multiple AACC servers.

Next steps

Check Server Configuration to validate that it has the correct configuration for the new SIP-enabled Contact Center server.

Restoring the Multimedia Contact Server database

Before you begin

- Create a new backup of the original Multimedia Contact Server database.
- On the new server, map a drive to the location of the backed up Multimedia Contact Server database.

Important:

When you migrate configuration information from the old server to the new server, do not run the two application servers simultaneously. Both applications are configured the same, so they attempt to access and control the same resources. Continuing to run the old applications in the Contact Center can result in unpredictable behavior.

About this task

Restore the Multimedia Contact Server database to the new server. After the Multimedia Contact Server database is restored, the Contact Center Manager Administration name and email attachment paths are configured for your solution.

Procedure

1. From the **Start** menu, in the Avaya area, click **Database Maintenance**.
2. In the Database Maintenance dialog box, in the Main Menu pane, click **Backup Locations**.
3. In the right pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which you stored the Multimedia Contact Server database backup.
5. In the **UNC Path** box, type the location of the Multimedia Contact Server database in the format \\Computer Name\Folder\Backup Location. This must precisely match the location you specified when you backed up the Database.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** field, type the user password.
8. Click **Save**.
9. Click **OK**.
10. In the Database Maintenance dialog box, in the Main Menu pane, click **Restore**.
11. In the **Media Type** section, select **Network Location**.
12. In the **Application** section, select **CCMM**.
13. In the **Restore contents** section, select **Data**. If you are restoring an AACC Release 6.4 or Release 7.x database, select **Offline** also.
14. From the **Backup Location** list, select the network drive containing the backed up Multimedia Contact Server database.
15. Click **Restore**.
16. Click **Yes**.

Checking the Server Configuration settings on the new SIP-enabled server

Before you begin

- Migrate the CCMS, CCT, and Multimedia databases to the new SIP-enabled server(s).

About this task

Check Server Configuration after migrating the CCMS, CCT, and CCMM databases to the new SIP-enabled server(s). Ensure that the settings in Server Configuration are correct for your new server.

Procedure

1. Click **Start > All Programs > Avaya > Server Configuration**.
2. Select **Local Settings**.
3. Check that the details in Local Settings are correct for the new server.
4. Select **Licensing**.
5. Check that the details in Licensing are correct for the new server.
6. Select **SIP > Network settings**.
7. Check that the details in SIP > Network Settings are correct for the new server.
8. Select **SIP > Local Subscriber**.
9. Check that the details in SIP > Local Subscriber are correct for the new server.

Next steps

Configure Multimedia settings on the new SIP-enabled server.

Configuring Multimedia settings on the new SIP server

Before you begin

- Migrate the Contact Center databases to the new SIP-enabled server(s)
- Update the Contact Center details in Server Configuration

About this task

Configure the Multimedia settings to point to the new SIP-enabled CCMM server.

Procedure

1. Click **Start > All Programs > Avaya > Multimedia Dashboard**.
2. On the CCMM Dashboard, under **Server Availability**, right-click **Contact Center Manager Administrator** and select **Edit**.
3. On the Administrator Login dialog, in the **User Name** box, type `GeneralAdmin`.
4. In the **Password** box, type the password.
The default password is `__ccmm!` on new Contact Center installs.
5. Click **Login**.

6. On the **Administrator Login** dialog, in the **text** box, type the name for the current Contact Center Manager Administration server (CCMA).
7. Click **Save**.
8. On the CCMM Dashboard, under **Server Availability**, right-click **Contact Center Multimedia Server** and select **Edit**.
9. On the **Administrator Login** dialog, in the **User Name** box, type `GeneralAdmin`.
10. In the **Password** box, type the password.
The default password is `__ccmm!` on new Contact Center installs.
11. On the Administrator Login dialog, in the text box, type the name for the current Contact Center Multimedia Server (CCMM).
12. Click **Save**.
13. Click **Update**.
14. Exit the Multimedia Dashboard application.

Next steps

Restore the CCMA databases on the new SIP-enabled server.

Restoring Contact Center Manager Administration data

Before you begin

- Know the network location (in Universal Naming Convention (UNC) format) of the drive for the backed up data.

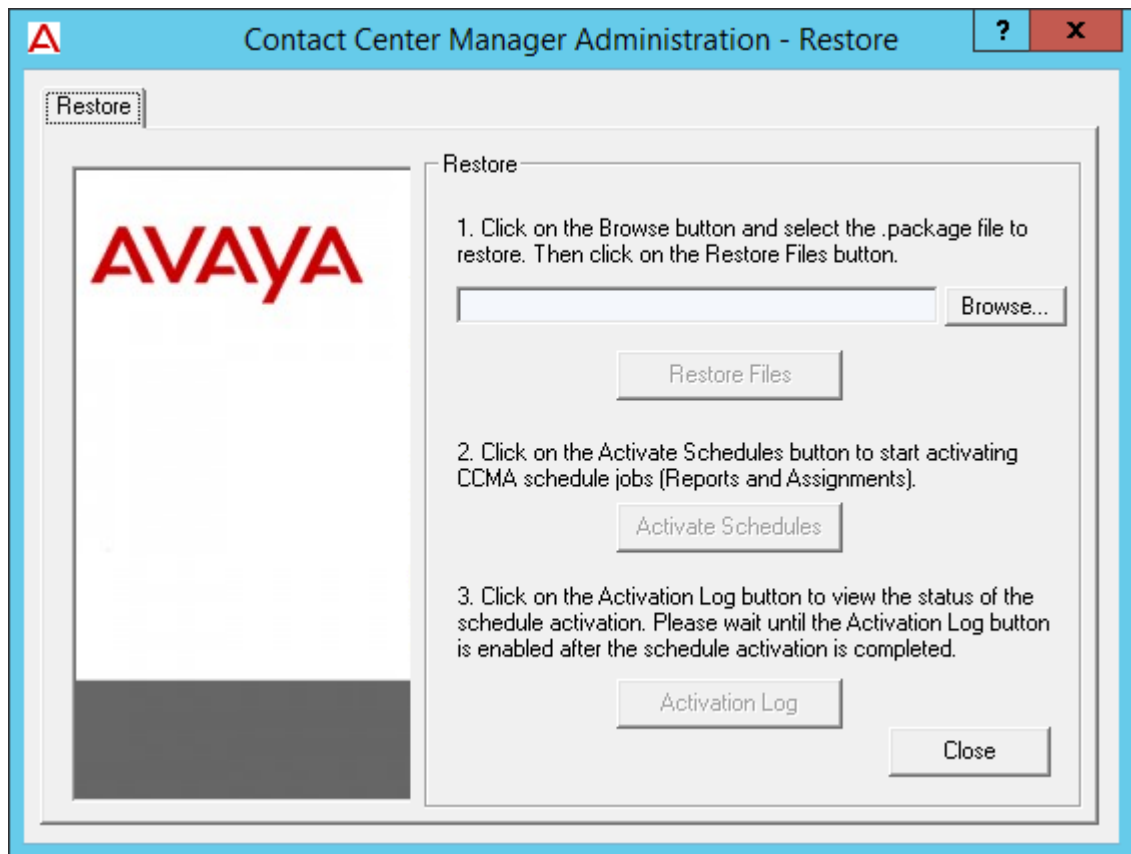
About this task

Restore the Contact Center Manager Administration data to migrate the data to the new server. Use this procedure if you are restoring Avaya Aura® Contact Center Contact Center Manager Administration data. You must restore the CCMA database as part of a matched set; the CCMA data must be restored to the same server as its corresponding databases (for example, CCMS, CCT, or CCMM).

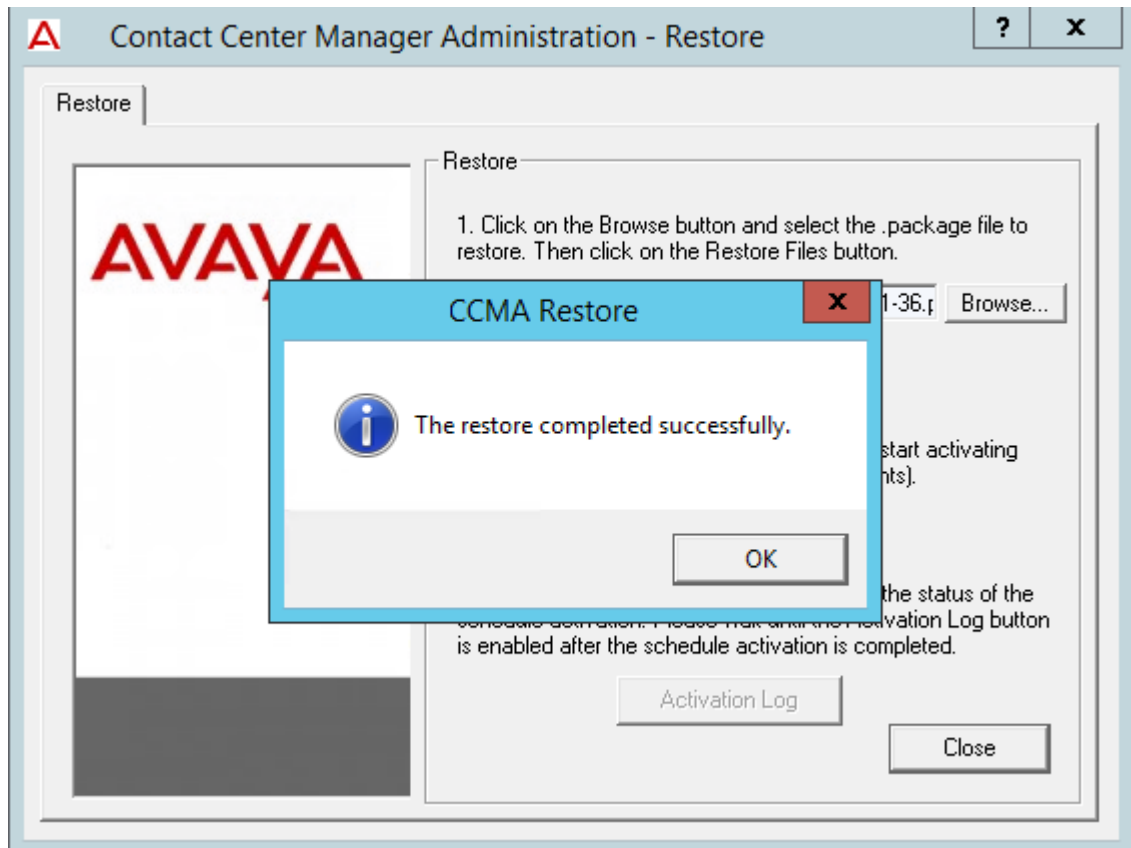
Procedure

1. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.
2. In the left pane of the Avaya Configuration window, expand **Avaya > Applications > Restore**.
3. In the right pane, click **Restore**.
4. On the **Restore** message box, click **OK**.

5. In the **Contact Center Manager Administration - Restore** dialog box, click the **Restore** tab.



6. To select a backup file to restore from, click **Browse**.
 7. In the **Select a backup file** dialog box, select the required .package file.
 8. Click **Open**.
 9. To restore the backup file data onto the administration data server, click **Restore Files**.
- The restore completed successfully message box appears.



10. Click **OK**.

Upgrading the Contact Center Manager Administration data

Before you begin

- Restore the backed up Contact Center Manager Administration (CCMA) data.

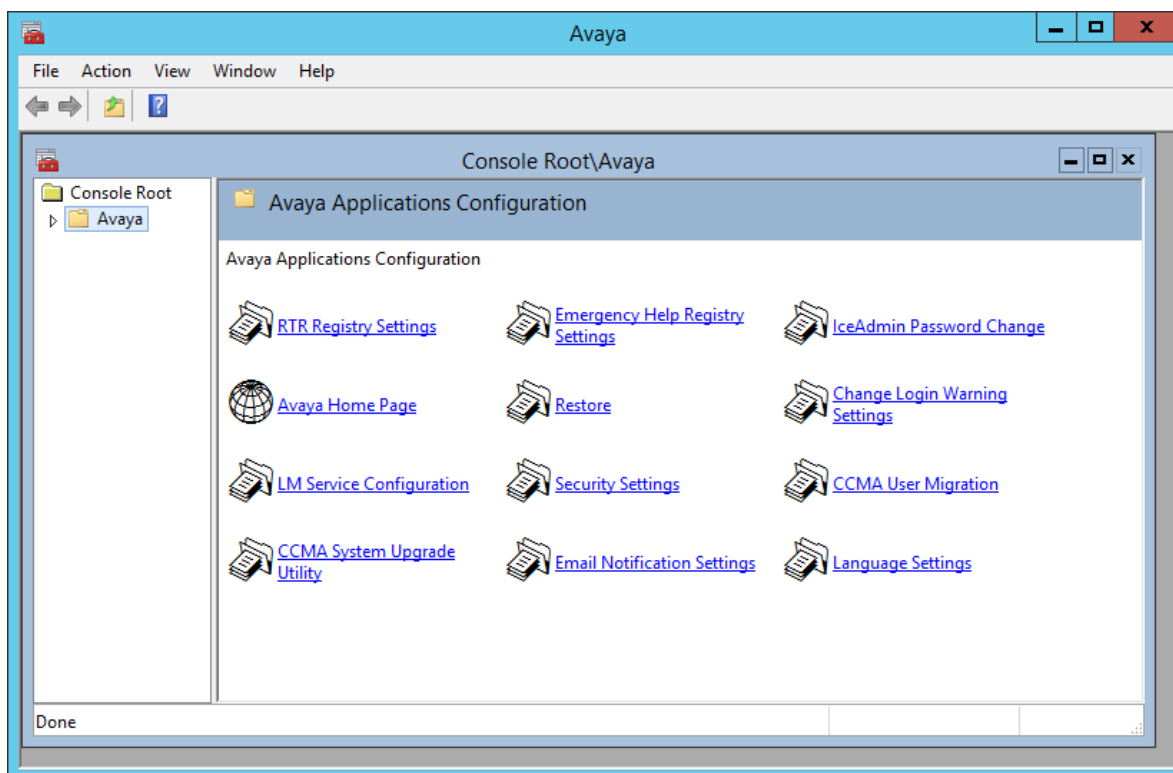
About this task

Upgrade Contact Center Manager Administration (CCMA) data to the Intersystems Caché database format used by Avaya Aura® Contact Center Release 7.1.

Procedure

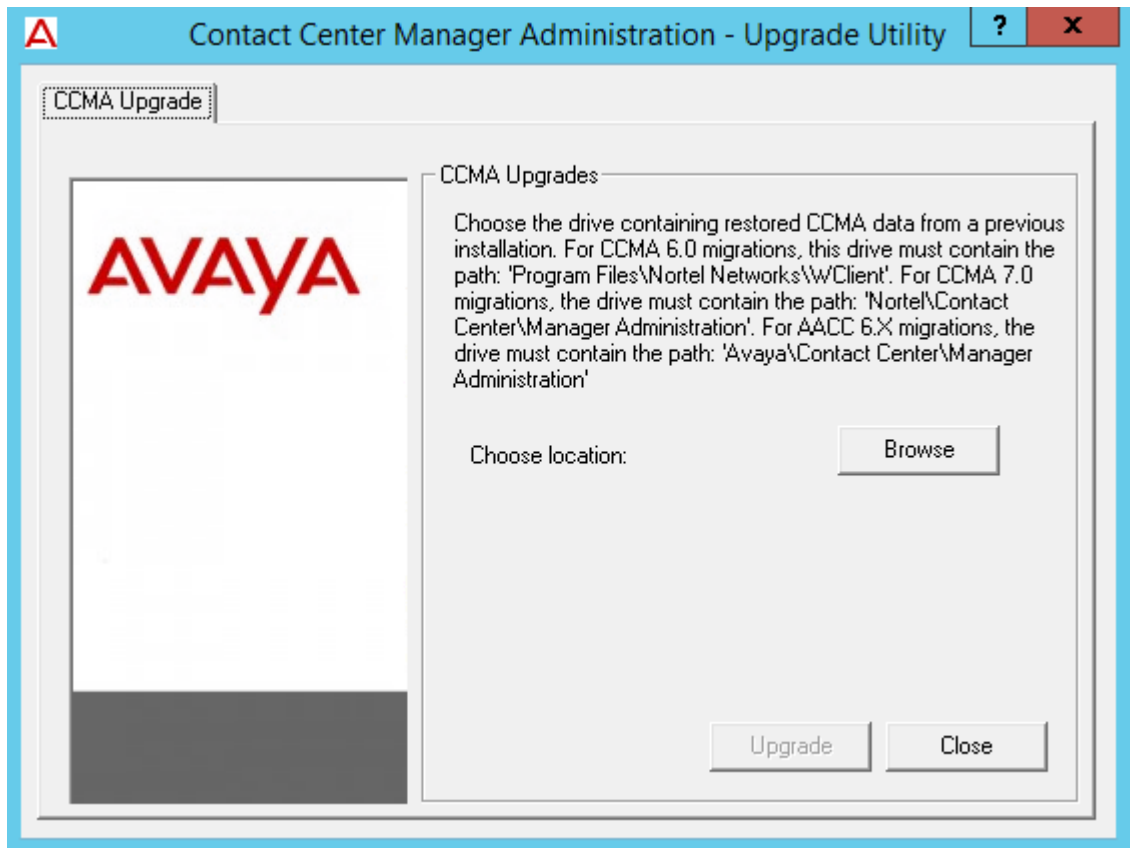
1. From the **Start** menu, in the Avaya area, click **Manager Administration Configuration**.

2. In the left pane, click **Avaya** > **Applications** > **CCMA System Upgrade Utility**.



3. In the right pane, click **CCMA System Upgrade Utility**.

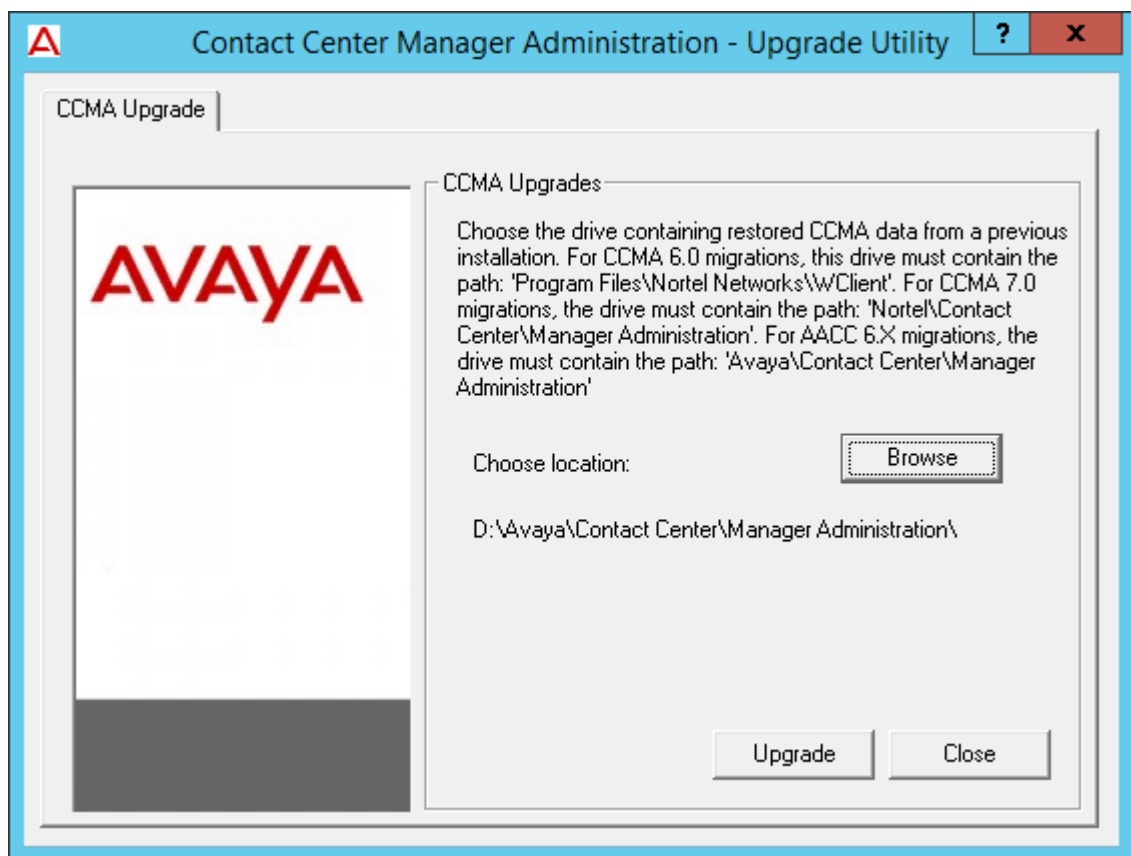
4. Click **Yes** on the confirmation dialog box.



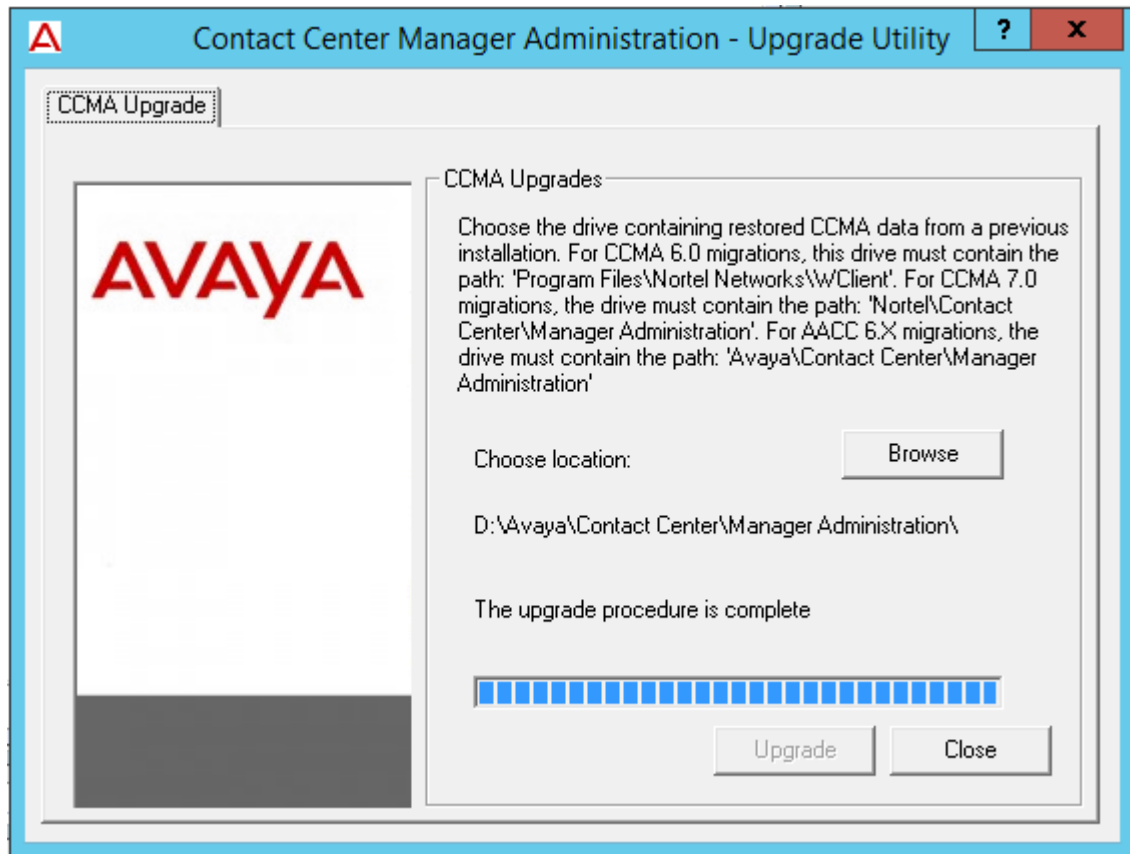
5. On the Upgrade Utility, click **Browse** and follow the instructions on the **CCMA Upgrades** screen to choose a location.

Select only the drive letter as the location of the restored CCMA data. The upgrade utility automatically detects and appends the correct directory structure for the old system data.

Example of upgrading from an Avaya Aura® Contact Center Release 6.4 system:



6. Click **Upgrade**.



7. Close the Upgrade Utility application. Click **Close**.

Completing CCMA and CCMM configuration on the new SIP-enabled server

Before you begin

- Know the sysadmin password from the old AACC system.
- Restore the CCMA databases to the new SIP-enabled server.
- Upgrade the CCMA database.

About this task

Complete the CCMA and CCMM configuration on the new SIP-enabled server. You must configure the switch type as SIP in the Multimedia settings.

Procedure

1. On the new Contact Center server, right click the SMMC System tray on the Windows Task bar and click **Start System**.

When the system has started, the SMMC System tray changes to the Running state.

2. When the system has started, log on to Contact Center Manager Administration with administrative privileges.
3. On the Launchpad, click **Configuration**.
4. For each Contact Center server, right click the server and select **Edit Properties**.

Change the server properties name and IP address to match the new SIP-enabled Contact Center server. You must use the sysadmin password from your old AACC system, because the database restore copied this to the new system.

5. On the Launchpad, click **Multimedia**.
6. In the left pane, select the Contact Center Multimedia to which you want to log on.
7. In the right pane, click **Launch Multimedia Client**.
8. In the CCMM Administration window, select **General Administration**.
9. Select **Server Settings**.
10. For each Server Type, edit the host names to match the new SIP-enabled Contact Center server names.
11. In the left pane, select **E-mail**.
12. Select **General Settings**.
13. Under **Attachment Files**, modify the **Inbound URL**, **Inbound Share**, **Outbound URL**, and **Outbound Share** locations so that they are correct for the new SIP-enabled Contact Center.
14. In the left pane, select **Agent Desktop Configuration**.
15. Select **Common Settings**.
16. Click **Advanced**.
17. From the **Platform** list, select **SIP**.
18. From the **Switch Type** list select **SIP Avaya Aura 6.2FP4 / 7.0**.
19. Click **Save**.
20. Exit the CCMM Administration window.
21. Log off from Contact Center Manager Administration.
22. Restart the Contact Center server.

Next steps

Update the CCMS and CCT configuration data.

Updating the CCMS and CCT configuration data

Before you begin

- Complete the CCMA and CCMM configuration on the new SIP-enabled server.

About this task

Use the CCMA configuration tool to modify user and configuration data to be compatible with SIP Contact Center. You must update the User, CDN, and DNIS data. In particular, modify the following items:

- Agent and supervisor/agent Voice URIs, Call Presentation Classes, and, if relevant, Windows domain and user IDs.
- CDN (Route Point) URIs
- DNIS URIs

Procedure

1. On the new Contact Center server, log on to CCMA with administrative privileges.
2. In the Configuration component of Contact Center Manager Administration, on the menu, choose **Download > Configuration Tool**.
3. On the dialog box, click **Run**.
4. To extract the spreadsheet and its associated files to the default directory, in the **WinZip Self-Extractor** dialog box, click **Unzip**.

A message appears, confirming that you successfully unzipped the spreadsheet and its associated files.

5. To navigate to the directory of your choice, in the **WinZip Self-Extractor** dialog box, click **Browse**.



Important:

The validation template file and the Online Help file must be in the same folder as the spreadsheet. The naming convention for these files is Consolidated_ConfigurationTool.chm for Help files, and Consolidated_Validation.xml for validation files.

6. Open the spreadsheet file `Consolidated_ConfigurationTool.xlsm`.

A Microsoft Excel message prompts whether you want to enable all macros.

7. Click **Enable Macros**.
8. Run the macro **CCM Download** to download data from the Contact Center server.
9. Modify the configuration data with the correct SIP values.

If you need help entering values, place your cursor in the column heading cell. A comment appears with information on the types of values allowed, and whether data is mandatory or optional. For more detailed information, click Configuration Tool Help.

10. Save your changes.
11. On the Configuration Tool spreadsheet toolbar, click **Data Validation**.
12. In the **Data Validation - Configuration Tool** dialog box, in the **Configuration Data** area, select the data to validate. You can validate all of the data you changed or a portion of it.
13. Click **OK**.

The application reads all of the entered data, highlights any incorrectly formatted values, highlights mandatory cells that are missing any values, and displays an error message in any row containing an error.
14. Correct all errors that the validation macro identifies.
15. Run the macro **CCM Upload** to upload the modified data to the Contact Center server.
16. Save and close the spreadsheet.

Next steps

Run the CCMS Workflow Compliance Report and ensure your application flows are consistent with a SIP-enabled Contact Center.

Generating the CCMS Workflow Compliance report

Before you begin

- Update the CCMS and CCT configuration data

About this task

Generate a CCMS Workflow Compliance report to find out if the migrated scripts or application flows contain commands or code constructs that are not compatible with a SIP-enabled Contact Center.

The Workflow Compliance Checker generates a PDF report that guides you in making the necessary changes to scripts and application flows using Avaya Orchestration Designer.

Procedure

1. Browse to `D:\Avaya\Contact Center\Common Components\WorkflowComplianceChecker`.
2. Double-click the `Workflow Application.exe` file to run the Workflow Compliance Checker application.
3. Click **Generate report** to generate and save the report in PDF format.
4. Save the report to `D:\Temp\WCC`.
5. Click **Close**.
6. Open the Workflow Compliance report.

7. Use Avaya Orchestration Designer to update and activate your scripts and applications, following the recommendations in the Workflow Compliance report.

You must complete all the recommendations of the Workflow Compliance report.

Next steps

Refer to the *Avaya Aura® Contact Center CS1000 (AML) to Aura (SIP) Migration Guidelines* application note for further steps to complete the migration of the contact center solution.

Part 8: Common procedures

- [Common procedures for patching](#) on page 353
- [Avaya Workspaces upgrades](#) on page 359
- [Deploying Avaya Workspaces High Availability](#) on page 369

Chapter 21: Common procedures for patching

This chapter provides common procedures related to hot patching. It also describes how to start System Management and Monitoring Component (SMMC) services after a patch installation.

Hot patching for Mission Critical High Availability

Before you begin

- Ensure that you have a standby server license for the server you are hot patching.
- Ensure both existing active and standby servers have the same patch level.

About this task

Microsoft Windows Server does not support the patching of running applications. You must stop a Windows Server application to patch it.

Contact Center is supported on the Microsoft Windows Server operating system. The Contact Center High Availability feature supports hot patching. In a Contact Center that uses the High Availability licensed feature, two sets of Contact Center applications run but only the active set processes contacts. The other set, the standby applications, do not process contacts and therefore can be stopped and patched without shutting down the Contact Center. This process of patching the stopped standby applications is called hot patching.

Contact Center provides service packs and patches. Contact Center releases service packs that deliver multiple product updates, fixes, and some enhancements in a single installable package. In between service pack releases, Contact Center uses patches to deliver individual product updates.

Most Contact Center patches and service packs support hot patching. A small number of Contact Center patches or service packs might not support hot patching, and these updates require a maintenance window. Read the patch or service pack Readme file to determine if the update supports hot patching.

If your Contact Center is licensed for active and standby servers, you can hot patch your software to minimize down time.

Important:

You must ensure that you patch both the active and standby servers to the same patch level.

If you are hot patching a Contact Center Release 7.0 system to AACC Release 7.0 Feature Pack 1 or later, you must reset the standby server minimum TLS version to TLS 1.0 before you perform the manual switch over to the standby server. Agent Desktop Release 7.0 does not work with TLS 1.2. After patching the active server to Feature Pack 1 or later, and updating the Agent Desktop clients, you can set the minimum TLS version back to TLS 1.2 if appropriate for your Contact Center solution. For information on configuring the minimum TLS version, see *Avaya Aura® Contact Center Server Administration*.

When you select a manual switchover, Contact Center warns you if the shadowing latency between the active and standby servers is greater than the 10 second threshold. If you continue with the manual switchover when the latency is over threshold, after the switchover completes you must back up the new active server databases and restore them on the new standby server. This adds time and complexity to the hot patching process. For hot patching, Avaya recommends that you perform the manual switchovers only when the shadowing latency is under threshold.

For Mission Critical High Availability, use the System Management and Monitoring Component (SMMC) system tray to perform switchovers and start and stop the servers. For more information about the SMMC system tray, see *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* and *Avaya Aura® Contact Center Server Administration*.

Procedure

1. Read the patch Readme file to determine if the patch supports hot patching.
2. Use SMMC to stop the standby server system (Server B).
3. Install and apply the patch or service pack to the standby server (Server B). If required, reboot the server after installing the patch or service pack.
4. Use SMMC to start the standby server B. Ensure that you synchronize the data between the servers.
5. If you are hot patching from Contact Center Release 7.0 to Release 7.0 Feature Pack 1 or later, configure the Web Services minimum TLS version on the standby server to TLS 1.0.
6. Run a manual switchover, the current standby Server B becomes an active server.
Server B is now running and processing contacts.
7. Use SMMC to stop Server A.
8. Install and apply the patch or service pack to Server A. If required, reboot the server after installing the patch or service pack.
9. If the shadowing latency was greater than 10 seconds when you performed the manual switchover:
 - a. Backup all the contact center databases on the active server, Server B.
 - b. Restore all the active Server B contact center database backups onto Server A.
 - c. On Server A, confirm the server details are correct in Server Configuration, click Apply All and reboot the server.
10. After Server A starts, confirm that High Availability is correctly configured on standby Server A.

11. Use SMMC to start standby Server A. Ensure that data is synchronized between the servers.
12. Run a manual switchover, the current standby Server A becomes an active server.
Server A is now running and processing contacts.
13. If the shadowing latency was greater than 10 seconds when you performed the manual switchover:
 - a. Backup all the contact center databases on Server A.
 - b. Restore all the active Server A contact center database backups onto Server B.
 - c. On Server B, confirm the server details are correct in Server Configuration, click Apply All and reboot the server.
14. After Server B starts, confirm that High Availability is correctly configured on standby Server B.
15. Use SMMC to start Server B. Ensure that data is synchronized between the servers.
Server A is now the active server and Server B is now the standby server again.
16. If you configured the Web Services minimum TLS version on the standby server to TLS 1.0, you can now change it back to TLS 1.1 or 1.2 depending on the requirements of your Contact Center solution.
17. If your HA solution has a Remote Geographic Node server (RGN) configured as Standby server shadowing data from the campus site Active server, run steps [18](#) on page 355 to [23](#) on page 355, to patch the RGN server.
18. Use SMMC to stop the RGN standby server system (RGN Server).
19. Install and apply the patch or service pack to the RGN server. If required, reboot the server after installing the patch or service pack.
20. Restore the backup of Server A to RGN Server. Note: Restore the backup taken from Active Server A in the step [13](#) on page 355 above.
21. On the RGN server, confirm the server details are correct in Server Configuration, click Apply All and reboot the server.
22. After the RGN server starts, confirm that High Availability is correctly configured on the RGN server.
23. On the RGN Standby Server, use SMMC to start shadowing. Ensure shadowing starts on the RGN server.

Hot patching for hot standby High Availability

Before you begin

- Ensure that you have a standby server license for the server you are hot patching.

- Ensure both existing active and standby servers have the same patch level.

About this task

Microsoft Windows Server does not support the patching of running applications. You must stop the Windows Server application to patch it.

Contact Center is supported on the Microsoft Windows Server operating system. The Contact Center High Availability feature supports hot patching. In a Contact Center that uses the High Availability licensed feature, two sets of Contact Center applications run but only the active set processes contacts. The other set, the standby applications, do not process contacts and therefore can be stopped and patched without shutting down the Contact Center. This process of patching the stopped standby applications is called hot patching.

Contact Center provides service packs and patches. Contact Center releases service packs that deliver multiple product updates, fixes, and some enhancements in a single installable package. Between service pack releases, Contact Center uses patches to deliver individual product updates.

Most Contact Center patches and service packs support hot patching. A small number of Contact Center patches or service packs might not support hot patching and these updates require a maintenance window. Read the patch or service pack Readme file to determine if the update supports hot patching.

If your Contact Center is licensed for active and standby servers, you can patch your software to minimize downtime. You must ensure that you patch both the active and standby servers to the same patch level.

Important:

Both the active and standby server must be updated to the same patch level.

For hot standby High Availability, use the High Availability utility to start and stop shadowing. For more information about the High Availability utility, see *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000* and *Avaya Aura® Contact Center Server Administration*.

You can also use this procedure for hot patching Multimedia Contact Servers.

Procedure

1. Read the patch Readme file to determine if the patch supports hot patching.
2. Stop shadowing on the standby server (Server B).
3. Stop all Contact Center services on the standby server (Server B).
4. Install and apply the patch or service pack to the standby server (Server B). If required, reboot the server after installing the patch or service pack.
5. Start shadowing on the standby server B. Ensure that the data is synchronized between the servers.
6. Run a manual switchover so the current standby Server B becomes an active server.
Server B is now running and processing contacts.
7. Install and apply the patch or service pack to Server A. If required, reboot the server after installing the patch or service pack.

8. Back up all the contact center databases on Server B.
9. Restore all the active Server B contact center database backups onto Server A.
10. Open the High Availability utility on Server A and verify the data.
11. Open Server Configuration on Server A and verify the data.
12. Click **Apply All**.
13. On the Restart Required dialog box, click **Yes**.
14. On the HA system dialog box, click **OK**.
15. Start shadowing on Server A. Ensure that the data is synchronized between the servers.
16. Run a manual switchover so Server A becomes the active server.
17. Back up all the contact center databases on active Server A.
18. Restore all the contact center database backups onto Server B.
19. Open Server Configuration on Server B and verify the data.
20. Click **Apply All**.
21. On the Restart Required dialog box, click **Yes**.
22. On the HA system dialog box, click **OK**.
23. Start shadowing on server B.

Server B is now the standby server and Server A is the active server again.

24. If your High Availability solution has the Remote Geographic Node server (RGN) configured as a standby shadowing data from the active server, perform steps [25](#) on page 357 to [31](#) on page 357.
25. Install and apply the patch or service pack to the RGN server. If required, reboot the server after installing the patch or service pack.
26. Restore the backup onto the RGN server.

Remember to restore the backup from Server A taken in step [17](#) on page 357 above.
27. Open Server Configuration on the RGN server and verify the data.
28. Click **Apply All**.
29. On the Restart Required dialog box, click **Yes**.
30. On the HA system dialog box, click **OK**.
31. Start shadowing on the RGN server using the High Availability utility.

Starting SMMC

About this task

During a patch installation, all System Management and Monitoring Component (SMMC) services and the SMMC System Tray application stop to enable Contact Center files to be patched. After patching the server, if the patch does not require a server reboot, you must start the SMMC applications manually.

Procedure

1. Navigate to **SMMC SystemTray**.
2. On the Windows system tray, right-click the SMMC icon and click **Start SMMC**.

Chapter 22: Avaya Workspaces upgrades

Migrations

When migrating Avaya Aura® Contact Center to a new server or virtual guest, you must install and configure Avaya Workspaces on a new server or virtual guest together with the Avaya Aura® Contact Center Release 7.1.x software.

To deploy Avaya Workspaces on a new server, use the following high-level steps for the initial installation:

1. When deploying in a virtual environment, manually deploy three virtual machines using the Avaya Workspaces OVA. See [Deploying the Avaya Workspaces OVA](#) on page 177.
2. When installing the Avaya Aura® Contact Center DVD software, do the following:
 - a. Select the **Configure Workspaces** check box.
 - b. If you are deploying in a physical environment, select the drive for the Avaya Workspaces database.

Depending on your solution, see one of the following procedures:

- [Installing the Voice and Multimedia Contact Server with Avaya Aura Media Server software for Avaya Aura Unified Communications platform](#) on page 216
 - [Installing the Multimedia Contact Server software](#) on page 179
 - [Installing the Voice and Multimedia Contact Server without Avaya Aura Media Server software for Avaya Aura Unified Communications platform](#) on page 70
3. In the Ignition Wizard, configure the details for the Avaya Workspaces cluster and NTP servers. See [Configuring Avaya Workspaces during the initial installation](#) on page 362.

Upgrades and patch installation

To upgrade Avaya Workspaces, you must select the Avaya Workspaces configuration check box when installing the Avaya Aura® Contact Center Release Pack, Feature Pack, or Service Pack in the Contact Center Release Pack Installer.

In a virtual environment, if upgrading from a previously configured Avaya Workspaces, you must redeploy the Avaya Workspaces cluster using the OVA for the latest release. Shut down the virtual machines created from the OVAs for the previous release.

For an Avaya Workspaces patch installation, you must download the Contact Center Workspaces Patch Installer application. Hot patching is not supported for Avaya Workspaces upgrades. You must upgrade Avaya Workspaces during a scheduled maintenance window.

Use the following steps for upgrading and patching Avaya Workspaces:

1. When deploying in a virtual environment, manually deploy three virtual machines using the Avaya Workspaces OVA. See [Deploying the Avaya Workspaces OVA](#) on page 177.

2. When installing the Avaya Aura® Contact Center Release Pack, Feature Pack, or Service Pack, in the Contact Center Release Pack Installer, select the check box to configure Avaya Workspaces.

Depending on your solution, see one of the following procedures:

- [Installing Voice and Multimedia Contact Server without Avaya Aura Media Server Release Packs, Feature Packs and Service Packs](#) on page 112
 - [Installing Multimedia Contact Server Release Packs, Feature Packs and Service Packs](#) on page 194
 - [Installing Voice and Multimedia Contact Server with Avaya Aura Media Server Release Packs, Feature Packs and Service Packs](#) on page 253
3. In the Contact Center Update Configurator, configure Avaya Workspaces. See [Configuring Avaya Workspaces using the Update Configurator](#) on page 365.
 4. To download and install the Avaya Workspaces patches, do the following:
 - a. Download the Contact Center Workspaces Patch Installer application. See [Downloading Contact Center Workspaces Patch Installer](#) on page 366.
 - b. Install the Avaya Workspaces patches. See [Installing Avaya Workspaces patches](#) on page 367.

Deploying the Avaya Workspaces OVA

Before you begin

Download the Avaya Workspaces OVA from the Avaya Support website at <https://support.avaya.com>.

Note:

If upgrading from a previously configured Avaya Workspaces installation, you must re-deploy the Avaya Workspaces cluster using the OVA, which is shipped with the latest release. Before you start deploying new virtual machines, shut down the virtual machines created from OVAs of the previous release.

About this task

Use this procedure to deploy optional Avaya Workspaces in a virtual environment. Deploy the Avaya Workspaces OVA file onto a VMware ESXi host server using vCenter to create a virtual machine with the Avaya Workspaces software for use in the Contact Center solutions.

For Avaya Aura® Contact Center, you need to deploy three virtual machines from the Avaya Workspaces OVA. There is no restriction for the virtual machine names. For example, you can use the following names: wsk8master, wsk8node1, and wsk8node2. Use this procedure to deploy and configure each of the three virtual machines.

You must also ensure that you correctly configure CPU and memory reservation parameters for the Avaya Workspaces virtual machines. For more information, see *Avaya Aura® Contact Center Overview and Specification*.

Procedure

1. In your vCenter client, select the host server on which to deploy the Avaya Workspaces OVA.
2. Select **File > Deploy OVF Template**.
3. On the **Source** window, click **Browse**.
4. On the **Open** message box, select the Avaya Workspaces OVA file.
5. Click **Open**.
6. On the **Source** window, click **Next**.
7. On the **OVF Template Details** window, verify the details of the Avaya Workspaces OVA template and click **Next**.
8. On the **End User License Agreement** window, read the license agreement, and if acceptable, click **Accept**.
9. Click **Next**.
10. On the **Name and Location** window, type the name of the new Avaya Workspaces virtual machine. This is not the server hostname. This is the name of the VMware virtual machine as it appears in the VMware inventory.
11. Click **Next**.
12. On the **Host and Cluster** window, select the host server or cluster to deploy the Avaya Workspaces OVA. If you selected a cluster, select a **Specific Host** on that cluster.
13. Click **Next** to display the **Storage** window.
14. From the **Select a destination storage for the virtual machine files** list, select a location to store the Avaya Workspaces virtual machine image. Ensure that the storage location you select has sufficient available storage space to store a thick provisioned virtual machine image.
15. Click **Next**.
16. On the **Disk Format** window, select **Thin Provision**.
17. Click **Next**.
18. On the **Ready to Complete** window, verify the deployment settings. If you need to modify any settings, click **Back**.
19. Click **Power on after deployment**.
20. Log on to the Avaya Workspaces virtual machine using the default credentials.
The user name is `root`, and the password is `root01`. You must not change the default credentials at this step. You can create a new password later when configuring Avaya Workspaces in the Ignition Wizard.
21. Enter the `# ifconfig` command to establish the name of your network adapter.

22. To open the network configuration script, enter the `# vi /etc/sysconfig/network-scripts/ifcfg-ens192` command.
Ensure the network adapter name matches your environment.
23. Press the **Insert** key to enter the edit mode.
24. Modify the **IPADDR**, **GATEWAY**, **NETMASK**, and **DNS** fields as required. Ensure the **BOOTPROTO** field is set to *none*.
25. To save the changes, press **Esc** and type `:wq!`. To exit without changes, press **Esc** and type `:q!`.
26. Enter the `# systemctl restart network` command to restart the network service and enable the changes.
27. In **VM Options**, under the **VMWare tools** section, clear the **Synchronize guest time with host** check box.

You must use NTP servers for time synchronization of Contact Center machines and Avaya Workspaces nodes. You can configure time synchronization settings while configuring Avaya Workspaces in the Ignition Wizard for fresh installs or in the Update Configurator when installing at a later stage or upgrading.

Configuring Avaya Workspaces during the initial installation

About this task

Use this procedure to configure Avaya Workspaces during the initial installation of your Contact Center solution. In the Ignition Wizard, use the Workspaces tab to configure the Avaya Workspaces details and the Other settings tab to configure NTP servers for time synchronization.

 **Note:**

Ensure that you enter the Cluster IP Address for the Avaya Workspaces cluster. This is a single IP address that you use to access Avaya Workspaces.

Procedure

1. On the Contact Center Ignition Wizard screen, select the **Workspaces** tab and configure the details.

The screenshot shows the 'Configuration Data' window for 'Avaya Contact Center'. The 'Workspaces' tab is selected. The window contains the following fields and controls:

- Workspaces Section:**
 - IP Addresses:** A list box with an 'Add' button and a 'Remove' button.
 - Password:** A text input field.
 - Confirm Password:** A text input field.
- LDAP Server Section:**
 - IP Address:** A text input field.
 - Port:** A text input field.
 - Protocol:** A dropdown menu.
- Cluster IP Section:**
 - IP Address:** A text input field.

At the bottom, there is a 'Click Next to Continue' instruction and three buttons: '< Back', 'Next >', and 'Cancel'.

2. In the **Workspaces** section, click **Add** next to the **IP Addresses** box to add IP addresses of Avaya Workspaces nodes. Select an address and click **Remove** if you want to remove an IP address.

You must add three IP addresses to proceed the configuration.

! Important:

If you have a physical solution, you must enter IP addresses that are not in use.

3. In the **Workspaces** section, in the **Password** box, enter the root password for the Avaya Workspaces nodes.

The password is checked against the server security policy for minimum password requirements. Avaya recommends using a password that conforms to your corporate password policy.

* Note:

Do not use special symbols: @ # £ & ^.

4. In the **Confirm Password** field, enter the password again.
5. In the **LDAP Server** field, in the **IP Address** box, enter the IP address of the LDAP Server.
6. In the **Port** field, enter the port number of the LDAP protocol.
7. From the **Protocol** list, select a type of encryption:
 - TCP
 - TLS
8. In the **Cluster IP** field, enter the IP Address of the Avaya Workspaces cluster.
9. Select the **Other settings** tab to configure NTP servers for time synchronization.

The screenshot shows the 'Avaya Contact Center' configuration window with the 'Configuration Data' tab selected. The 'Other settings' sub-tab is active. It contains sections for 'NTP Servers' (with 'Add' and 'Remove' buttons), 'SSH session timeout' (set to 10 minutes), and 'Cluster time zone' (showing Windows and Linux time zones). Navigation buttons at the bottom include '< Back', 'Next >', and 'Cancel'.

10. In the **NTP Servers** section, click **Add** to add an IP address of an NTP server.
 You can add up to three IP addresses. To remove the IP address, select the required IP address and click **Remove**.
11. In the **SSH session timeout** box, type the timeout value in minutes.
 The default value is 10 minutes. You can enter the value from 5 to 60 minutes.
12. In the **Cluster time zone** section, from the list, select the time zone of the Linux cluster.
 Avaya recommends using the appropriate time zone of the Windows system. You can view the current Windows time zone on the same screen.

13. Click **Next**.

Next steps

If you want to deploy and configure Avaya Workspaces High Availability, see [Deploying Avaya Workspaces High Availability](#) on page 369.

Configuring Avaya Workspaces using the Update Configurator

About this task

After the Avaya Release Pack Installer reboots the server, the Contact Center Update Configurator opens so that you can configure Avaya Workspaces.

Before you begin

- If upgrading in a virtual environment, remove the Avaya Workspaces cluster drive on the Contact Center server. Typically it is the W:\ drive. From Release 7.1.0.3, this drive is no longer required for virtual deployments of Avaya Workspaces.

Procedure

1. On the Contact Center Update Configurator, select the **Configure Workspaces** tab.
2. Next to the **IP Address** box, click **Add**.

You must enter three IP addresses to proceed the deployment.

Important:

If you have a physical solution, you must enter IP addresses that are not in use.

To remove an IP address, select an address and click **Remove**.

3. In the **Cluster IP** field, enter the IP address of the Avaya Workspaces cluster.
4. In the **Password** box, type the root password for the Avaya Workspaces cluster.

The password is checked against the server security policy for minimum password requirements. Avaya recommends that you enter a password that conforms to your corporate password policy.

Note:

Do not use special symbols: @ # £ & ^.

5. In the **Confirm Password** box, retype the password.
6. **(Optional)** To ensure that passwords match, select the **Show password** check box.
7. In the **LDAP IP Address** box, type the IP address of the LDAP server.
8. In the **Port** field, enter the port number of the LDAP protocol.

9. From the **Protocol** list, select one of the following encryption types:
 - TCP
 - TLS
10. To configure NTP servers for time synchronization, select the **Other settings** tab.
11. To add an IP address of an NTP server, next to the **IP Address** box, click **Add**.

You can add up to three IP addresses.

To remove an IP address, select an address and click **Remove**.
12. In the **SSH session timeout** box, type the timeout value in minutes.

The default value is 10 minutes. You can enter the value from 5 to 60 minutes.
13. From the **Linux cluster time zone** list, select the time zone of the Linux cluster.

Avaya recommends that you use the appropriate time zone of the Windows system. You can view the current Windows time zone on the same screen.
14. Click **Configure**.
15. When the Contact Center Update Configurator completes the configuration process, click **Yes** to restart the server.

Next steps

If you want to deploy and configure Avaya Workspaces High Availability, see [Deploying Avaya Workspaces High Availability](#) on page 369.

Downloading Contact Center Workspaces Patch Installer

About this task

The Contact Center Workspaces Patch Installer application is a .net application used for upgrading the deployed Avaya Workspaces. This application must be launched from the Contact Center server used for the original deployment of the Avaya Workspaces cluster. The application is not installed on Contact Center systems, instead it is embedded within each Avaya Workspaces Patch Bundle.

When launched on the Contact Center system, the application displays:

- the deployment type and version of the current Contact Center software installation
- the name and version of any Avaya Workspaces Patch installed on the system
- the name and version of the Avaya Workspaces Patch that will be installed
- the name and version of the services already installed on the Avaya Workspaces cluster
- the target version of the service which will be updated during Avaya Workspaces Patch installation

The Contact Center Workspaces Patch Installer generates two log files during the patch installation process. One log is for the Contact Center Workspaces Patch

Installer application called WorkspacesPatchInstaller.log. The other log file is for the patch itself called Install_WorkspacesPatch_7.x.x.x_x86, where 7.x.x.x is the release number, for example Install_WorkspacesPatch_7.1.0.2_x86. Both logs are located in folder: C:\Avaya\Logs\Sysops\WorkspacesPatchInstaller.

Use this procedure to download and launch the Contact Center Workspaces Patch Installer application.

Procedure

1. Download the most recent Avaya Workspaces Patch Bundle and the accompanying checksum text file from <http://support.avaya.com>.
2. Using MD5 checksum software, generate a checksum of the downloaded Avaya Workspaces Patch Bundle and verify it matches with the content of the downloaded checksum text file.
3. Log on to the Contact Center server as Administrator.
4. Extract the downloaded Avaya Workspaces Patch Bundle to a local folder.

The **WorkspacesPatchInstaller.exe** file is located in the **WorkspacesPatchInstaller** folder.

Next steps

Launch the Contact Center Workspaces Patch Installer and start installing the Avaya Workspaces patches.

Installing Avaya Workspaces patches

About this task

Use this procedure to install the Avaya Workspaces Patch Bundle.

You must patch Avaya Workspaces during a maintenance window. You can deploy the Avaya Workspaces Patch Bundle in the same maintenance window used for updating and patching Contact Center. Note that Avaya Workspaces is not operational during the maintenance window.

Note:

Contact Center services that reside on the Windows Server 2016 and 2019 systems are not shut down during the Avaya Workspaces patching process. You do not need to restart Contact Center services after the Avaya Workspaces patching process.

Before you begin

- Download the most recent Avaya Workspaces Patch Bundle and the accompanying checksum text file from <https://support.avaya.com>.
- Using MD5 checksum software, generate a checksum of the downloaded Avaya Workspaces Patch Bundle and verify it matches with the content of the downloaded checksum text file.

- The Avaya Workspaces patching process requires a functional Avaya Workspaces cluster to be available. If the Avaya Workspaces deployment is not detected on the Contact Center server, the Contact Center Workspaces Patch Installer application blocks the installation.

Procedure

1. Log on to Contact Center server as an administrator.
2. Run the `kubectl get nodes` command to verify that the Avaya Workspaces cluster is available.

A list of the available Avaya Workspaces nodes is displayed.

3. Extract the downloaded Avaya Workspaces Patch Bundle to a local folder.
4. From the WorkspacesPatchInstaller folder, launch the `WorkspacesPatchInstaller.exe` file.
5. When prompted, enter the username and password of the Avaya Workspaces cluster.
6. Click **OK**.
7. Click **Install**.

The installation process starts. When the installation finishes, the `Installed successfully` message is displayed.

8. Click **Close**.

Chapter 23: Deploying Avaya Workspaces High Availability

Avaya Workspaces supports High Availability for fault tolerant and resilient contact center solutions. You can configure Avaya Workspaces High Availability only on the following Contact Center server types that support both Avaya Workspaces and Mission Critical High Availability:

- Voice and Multimedia Contact Server without Avaya Aura® Media Server
- Multimedia Contact Server Only

You can deploy Avaya Workspaces High Availability only if Mission Critical High Availability is configured.

You can deploy Avaya Workspaces High Availability both on physical and virtual servers, however, the deployment procedures are different for physical and virtual environments. You must first fulfill all prerequisites and then configure Avaya Workspaces High Availability using the Workspaces HA Configurator tool.

If you deploy on a physical server, see [Avaya Workspaces High Availability deployment on a physical server](#) on page 369.

If you deploy on a virtual server, see [Avaya Workspaces High Availability deployment on a virtual server](#) on page 372.

Avaya Workspaces High Availability deployment on a physical server

Enabling Avaya Workspaces High Availability requires a new six-node Workspaces HA cluster to be configured. When you configure Avaya Workspaces High Availability in a physical environment, you must have a new third server — the Workspaces HA supplementary server — to host a part of the Workspaces HA cluster. When Avaya Workspaces High Availability is configured, each physical server (Active, Standby, and Workspaces HA supplementary server) hosts two nodes of the Workspaces HA cluster - one master and one worker. To access Avaya Workspaces, you must use the cluster IP address as a single entry point for the cluster. All IP addresses that you use for the Workspaces HA cluster must belong to the same subnet.

You can deploy the new server on Windows Server 2016 or Windows Server 2019. The Active, Standby, and Workspaces HA supplementary server must have the same operating system. Ensure that the new server meets the requirements for the Workspaces HA supplementary server.

! Important:

Before you upgrade a physical solution with Avaya Workspaces High Availability, you must manually shut down two nodes of the existing Workspaces HA cluster hosted on the Workspaces HA supplementary server. This action prevents the Workspaces cluster IP from pointing to the nodes on the Workspaces HA supplementary server, which can block the Update Configurator operation on the Active server.

When you run the `Workspaces_HA.bat` file on the Workspaces HA supplementary server, it deletes the existing nodes that you shut down and deploys the new nodes.

Configuring Avaya Workspaces High Availability for a physical deployment using the Workspaces HA Configurator tool

About this task

The Workspaces HA Configurator is a new tool for configuration, repair and administration of Avaya Workspaces High Availability. Use this procedure to deploy Avaya Workspaces High Availability for a physical server.

Before you begin

Deploy the new Workspaces HA supplementary server.

*** Note:**

Do not install Avaya Aura® Contact Center on the Workspaces HA supplementary server. The Workspaces HA Configurator performs all necessary Workspaces HA configuration for this server, without requiring Avaya Aura® Contact Center software. Note that the Workspaces HA supplementary server has a different specification than a standalone, Active, or Standby server in an Avaya Workspaces solution. For more information, see *Avaya Aura® Contact Center Overview and Specification*.

Procedure

1. Log in to the Active server.
2. Log in to CCMA:
 - a. On the Launchpad, click **Multimedia**.
 - b. Click **Launch Multimedia Client**.
 - c. In the CCMM Administration, in the left pane, click **Workspaces Configuration**.
 - d. In the **Workspaces Server IP** field, update the virtual Cluster IP address.
 - e. (Optional) In the **Workspaces Server Port** field, update the port number if using a port other than the default.
 - f. In the **Domain Server IP** field, update the IP address of the LDAP server.
 - g. (Optional) In the **Domain Server Port**, update the port number if using a port other than the default.
 - h. In the **Workspaces Admin Username** field, update the name of the administrator account.

- i. Click **Save**.
3. Launch the Workspaces HA Configurator tool.
4. Enter the user password of the existing Workspaces cluster.
5. Enter the IP Addresses for Master 2, Master 3, Worker 2 and Worker 3 into the corresponding fields.

The Workspaces HA Configurator automatically prepopulates the Master 1 and Worker 1 IP Addresses.

When all fields are filled in, the Configure button appears at the bottom of the screen.

6. Click **Configure**.

The Workspaces HA Configurator displays a warning message stating that the configuration process disables the existing Workspaces cluster and removes one of the Workspaces cluster nodes.

7. Click **Yes** to continue configuration.

The Ready to configure... dialog box appears prompting the next steps.

8. On the prompt, on the Active server, navigate to `D:\Avaya\Contact Center\Workspaces\VHDX` and copy the **VHDX** folder both to the Standby server and the Workspaces HA supplementary server.

You can choose any location except for the Workspaces drive.

9. To create two new virtual machines on both the Standby server and the Workspaces HA supplementary server, perform the following steps:
 - a. From the administrative command prompts, run the **Workspaces_HA.bat** file from the just copied VHDX folder.
 - b. Enter `Y` to accept the warning message about removal of existing Workspaces Hyper-V machines.
 - c. Enter the drive letter designated for the Workspaces drive.
Typically it is `W:\`.
 - d. When the InstallShield Wizard screen appears, on the **Welcome** screen, click **Next** to start installing Workspaces High Availability.
 - e. On the **License Agreement** screen, check the checkbox to accept the terms in the license agreement and click **Next**.
 - f. On the **Ready to Install the Program** screen, click **Install** to start the installation.
 - g. When the install process is complete, click **Finish**.
 - h. If prompted, reboot the Standby server and the Workspaces HA supplementary server.

After reboot, a command window launches automatically to complete the configuration.

- i. After script completes the configuration on both the Standby and the Workspaces HA supplementary server, return to the Active server.
10. On the Active server, on the **Ready to configure...** screen of the Workspaces HA Configurator tool, click **Continue**.

The Workspaces HA Configurator starts the configuration process. You can monitor the progress in the Progress Messages board.
11. Once the configuration completes, the Information dialog box is displayed. Click **Ok**.

The Progress Messages board displays that the script execution is successful.
12. Click **Close**.
13. On the Confirmation dialog box, click **Yes**.
14. Log in to Avaya Workspaces as an agent to check if the cluster is operational.

See *Using Avaya Workspaces for AACC and ACCS*.

You can re-run the configuration process if a failure occurs or if the Workspaces HA cluster behaves incorrectly. For more information, see *Troubleshooting Avaya Aura® Contact Center*.

Avaya Workspaces High Availability deployment on a virtual server

Deploying Avaya Workspaces High Availability in a virtual environment requires three additional nodes for the Workspaces HA cluster. You must deploy and configure the new nodes in the same subnet as the existing nodes in the cluster. At the end of the deployment, your Avaya Workspaces cluster is reconfigured to 6 nodes — 3 masters and 3 workers. To access Avaya Workspaces, you must use the cluster IP address as a single entry point for the cluster.

Deploying additional virtual machines for Avaya Workspaces High Availability

Before you begin

- Update your Contact Center with Avaya Workspaces to the latest version. Check the latest version at <https://support.avaya.com>.
- Download the latest Avaya Workspaces OVA from the Avaya Support website at <https://support.avaya.com>.

About this task

Before deploying Avaya Workspaces High Availability you need to deploy three additional virtual machines with the latest version of Avaya Workspaces OVA. It is required for a New Cluster IP address to provide a single entry point for the cluster. Ensure the new virtual machines are in the same subnet as the existing nodes of the Avaya Workspaces cluster.

There is no restriction for the virtual machine names. For example, you can use the following names: wsk8ha1, wsk8ha2, and wsk8ha3.

Use this procedure to deploy and configure each of the three virtual machines.

 **Important:**

Use this procedure for virtual solutions only. If you deploy on a physical machine, ignore this procedure.

Procedure

1. In your vCenter client, select the host server on which to deploy the Avaya Workspaces OVA.
2. Select **File > Deploy OVF Template**.
3. On the **Source** window, click **Browse**.
4. On the **Open** message box, select the Avaya Workspaces OVA file.
5. Click **Open**.
6. On the **Source** window, click **Next**.
7. On the **OVF Template Details** window, verify the details of the Avaya Workspaces OVA template and click **Next**.
8. On the **End User License Agreement** window, read the license agreement, and if acceptable, click **Accept**.
9. Click **Next**.
10. On the **Name and Location** window, type the name of the new Avaya Workspaces virtual machine. This is not the server host name, this is the name of the VMware virtual machine as it appears in the VMware inventory.
11. Click **Next**.
12. On the **Host and Cluster** window, select the host server or cluster on which to deploy the Avaya Workspaces OVA. If you selected a cluster, select a **Specific Host** on that cluster.
13. Click **Next** to display the **Storage** window.
14. From the **Select a destination storage for the virtual machine files** list, select a location to store the Avaya Workspaces virtual machine image. Ensure that the storage location you select has sufficient available storage space to store a thick provisioned virtual machine image.
15. Click **Next**.
16. On the **Disk Format** window, select **Thin Provision**.
17. Click **Next**.
18. On the **Ready to Complete** window, verify the deployment settings. If you need to modify any of the settings, click **Back**.
19. Click **Power on after deployment**.

20. Log into the Avaya Workspaces virtual machine using the default credentials.
The user name is `root` and the password is `root01`.
21. Enter the `# ifconfig` command to establish the name of your network adapter.
22. To open the network configuration script, enter the `# vi /etc/sysconfig/network-scripts/ifcfg-ens192` command. Ensure the network adapter name matches your environment.
23. Press the **Insert** key to enter the edit mode.
24. Modify the **IPADDR**, **GATEWAY**, **NETMASK** and **DNS** fields as required. Ensure the **BOOTPROTO** field is set to *none*.
25. To save the changes, press **Esc** and type `:wq!`. To exit without changes, press **Esc** and type `:q!`.
26. Enter the `# systemctl restart network` command to restart the network service and enable the changes.
27. Ensure that the time of the Avaya Workspaces virtual machine is aligned with the time of the Contact Center server. Follow the VMWare instructions (KB 1189) to align time synchronization of the Avaya Workspaces virtual machine and the Contact Center server.

Configuring Avaya Workspaces High Availability for a virtual deployment using the Workspaces HA Configuration tool

About this task

Workspaces HA Configuration is a new tool for configuration, repair and administration of Avaya Workspaces High Availability. Use this procedure to configure Avaya Workspaces High Availability for a virtual server.

Before you begin

Deploy 3 additional virtual machines for the Avaya Workspaces cluster. See [Deploying additional virtual machines for Avaya Workspaces High Availability](#) on page 372.

Procedure

1. Log in to the Active server.
2. Log in to CCMA:
 - a. On the Launchpad, click **Multimedia**.
 - b. Click **Launch Multimedia Client**.
 - c. In the CCMM Administration, in the left pane, click **Workspaces Configuration**.
 - d. In the **Workspaces Server IP** field, update the virtual Cluster IP address.
 - e. (Optional) In the **Workspaces Server Port** field, update the port number if using a port other than the default.
 - f. In the **Domain Server IP** field, update the IP address of the LDAP server.

- g. (Optional) In the **Domain Server Port**, update the port number if using a port other than the default.
- h. In the **Workspaces Admin Username** field, update the name of the administrator account.
- i. Click **Save**.

3. Launch the Workspaces HA Configurator tool.
4. Enter the user password of the existing Workspaces cluster.
5. Enter the IP Addresses for all Master and Worker nodes.

When all fields are filled in, the Configure button appears at the bottom of the screen.

6. Click **Configure**.

The Ready to configure... dialog box appears.

7. Follow the instructions displayed.

8. Click **Continue**.

The Workspaces HA Configurator starts the configuration process. You can monitor the progress in the Progress Messages board.

9. Once the configuration completes, the Information dialog box is displayed. Click **Ok**.

The Progress Messages board displays that the script execution is successful.

10. Click **Close**.

11. On the Confirmation dialog box, click **Yes**.

12. Log in to Avaya Workspaces as an agent to check if the cluster is operational.

See *Using Avaya Workspaces for AACC and ACCS*.

You can re-run the configuration process if a failure occurs or if the Workspaces HA cluster behaves incorrectly. For more information, see *Troubleshooting Avaya Aura® Contact Center*.

Index

A

AACC firewall considerations	43
about MBT migration	32
add	
Linux user group and user	267 , 282
server to domain	50
adding media servers in CCMA	274 , 289
ADMIN, CCT, CCMS, and CCMA	
restoring databases	151
ADMIN, CCT, CCMS, CCMA and CCMM	
restoring databases	231
Agent desktop	
upgrades	43
antivirus	54
Automatic Maintenance	
disabling 69 , 112 , 127 , 165 , 176 , 193 , 215 , 252 , 305 , 329	
enabling 92 , 114 , 149 , 168 , 188 , 196 , 228 , 257 , 315 , 332	
Avaya Aura Media Server	
patch installation	256 , 295
Avaya Aura Media Server configuration	271 , 288
Avaya Aura Media Server Hyper-V migration	292
Avaya Aura Media Server installing patches	296
Avaya Aura Media Server migration	259
Avaya Aura Media Server patches	259
Avaya Aura Media Server patching	294
Avaya Aura Media Server software installation	
add Linux user group and user	267 , 282
install Linux server	264 , 280
installation procedure (Linux)	267 , 283
Avaya Aura Media Server upgrades	259
Avaya support website	17
Avaya Workspaces	359 , 362 , 365 , 369 , 370 , 372 , 374
Avaya Workspaces OVA	177 , 360

B

backing up	
Database Integration Service	62 , 122 , 205
backing up Avaya Aura Communication Control Toolkit	
.....	68 , 127 , 214
backing up Avaya Aura Contact Center Manager	
Administration	65 , 124 , 212 , 303
backing up Avaya Aura Contact Center Manager Server	
.....	67 , 126 , 213
backing up Avaya Aura Contact Center Multimedia	68 , 214
backing up existing Avaya Aura Media Server data	208
backing up Multimedia Contact Server	175
backing up Network Control Center	304
backing up Voice and Multimedia Contact Server	
databases	66 , 209
backing up Voice Contact Server databases	
.....	63 , 122 , 125 , 175 , 207 , 303

backup locations	31
------------------------	--------------------

C

CCMS, CCT, and CCMA, ADMIN	
restoring databases	151
CCMS, CCT, CCMA, ADMIN, and CCMM	
restoring databases	231
Communication Control Toolkit backups	68 , 127 , 214
configuration	362 , 370 , 374
configuration data	
updating	349
Configuration Tool spreadsheet	
after migration	349
configuring Avaya Aura Media Server data	271 , 288
configuring settings	
Multimedia Complement for Elite migration	108 , 248
connection	
contact center subnet	50
Contact Center Manager Administration backups	
.....	65 , 124 , 212 , 303
Contact Center Manager Administration data restoration	
.....	98 , 154 , 236 , 319 , 341
Contact Center Manager Server backups	67 , 126 , 213
Contact Center Multimedia backups	68 , 214
Contact Center software installation	
server preparation	45
Contact Center Workspaces Patch Installer	366

D

data management	
multimedia	107 , 191 , 247
database encryption	42
Database Integration Service backup	62 , 122 , 205
Database Integration Service configuration	
restoring	94 , 150 , 230
deployment	177 , 360 , 365 , 369 , 372
disable	
unused network adapters	52
disable Admin Approval Mode	
Windows Server administrators	52
documentation	45
download	
recent server patches	51

E

Element Manager	232 , 270 , 287
Element Manager account	269 , 284
enable	
Microsoft Remote Desktop connection	52

expansion [35](#), [36](#)

F

firewall considerations
 AACC [43](#)

H

high availability [353](#), [355](#)
High Availability [369](#), [370](#), [372](#), [374](#)
hot patching [353](#), [355](#)
hot standby HA [355](#)

I

installation
 Linux server [264](#), [280](#)
 service packs [49](#)
installing Avaya Aura Media Server patches [256](#), [295](#), [296](#)
installing patches
 AAMS [256](#), [295](#)
 Avaya Aura Media Server [256](#), [295](#)
iptables [269](#), [284](#)

L

locations for backups [31](#)

M

MBT migration general information [32](#)
media server adding in CCMA [274](#), [289](#)
media server removing from CCMA [275](#), [290](#)
Microsoft Windows Server 2016 [48](#)
Microsoft Windows Server 2019 [48](#)
migrating Multimedia Contact Server [171](#)
migrating Network Control Center server [299](#)
migrating security certificates [41](#)
migrating Voice and Multimedia Contact Server [56](#), [199](#)
migrating Voice Contact Server [117](#)
migrating with standby [34](#)
migration [24](#)
migration Co-resident Avaya Aura Media Server [292](#)
migrations supported [26](#)
Mission Critical [353](#)
Multimedia Complement for Elite migration
 configuring settings [108](#), [248](#)
Multimedia Contact Server backups [175](#)
Multimedia Contact Server database [189](#), [338](#)
Multimedia Contact Server migration [171](#)
Multimedia Contact Server patching [193](#)
Multimedia Contact Server software installation
 installation procedure [179](#)
multimedia database
 restoring [151](#), [231](#)

N

NCC [309](#)
Network Control Center backups [304](#)
Network Control Center database Restore [318](#)
Network Control Center server migration [299](#)
Network Control Center Server migration [299](#)
Network Control Center Server patching [329](#)
NTP [269](#), [284](#)

P

patching [359](#)
patching Avaya Aura Media Server [294](#)
patching Avaya Workspaces [367](#)
patching Multimedia Contact Server [193](#)
patching Network Control Center Server [329](#)
patching Voice and Multimedia Contact Server [111](#), [251](#)
patching Voice Contact Server [165](#)
physical deployment [369](#)
physical environment [370](#)

R

RCW reports
 convert [109](#), [163](#), [249](#)
related documentation [12](#)
removal
 server software [292](#)
removing media servers from CCMA [275](#), [290](#)
restoring
 server databases [151](#), [231](#)
restoring Avaya Aura Media Server data [233](#), [271](#)
restoring Avaya Media Server data [242](#), [285](#)
restoring Contact Center Manager Administration data
 [98](#), [154](#), [236](#), [319](#), [341](#)
restoring database [95](#), [96](#), [152](#), [235](#)
Restoring database [318](#)

S

same server standby migrations [34](#)
security [54](#)
server
 restoring database [151](#), [231](#)
server preparation [45](#)
 adding a server to a domain [50](#)
 disabling unused network adapters [52](#)
 download recent patches to the server [51](#)
 enable Microsoft Remote Desktop connection [52](#)
 installing the most recent supported operating
 system service packs [49](#)
server software uninstallation
 remove Avaya Aura Media Server software [292](#)
shared location
 CSR export [53](#)

SMMC startup	358
software installation	
disable Admin Approval Mode	52
standby migrations	34
starting SMMC	358
support	17
supported migrations	26

T

turning off web services security	93 , 189 , 229 , 336
---	--

U

updating	
configuration data	349
upgrade	24
upgrades and migrations	
Media Server	38 , 259
upgrading	359

V

videos	16
virtual deployment	372
virtual environment	374
Voice and Multimedia Contact Server backups	66 , 209
Voice and Multimedia Contact Server database	95 , 96 , 235
Voice and Multimedia Contact Server migration	56 , 199
Voice and Multimedia Contact Server patching	111 , 251
Voice and Multimedia Contact Server software	
installation procedure	82 , 216
Voice and Multimedia Contact Server with Avaya Aura	
Media Server migration	200
Voice and Multimedia Contact Server without Avaya Aura	
Media Server migration	57
Voice and Multimedia Contact Server without Avaya Aura	
Media Server software	
installation procedure	70
Voice Contact Server	118
Voice Contact Server backups	63 , 122 , 125 , 175 , 207 , 303
Voice Contact Server database	152
Voice Contact Server migration	117 , 118
Voice Contact Server patching	165
Voice Contact Server software	
installation procedure	128 , 139

W

web services security turning off	93 , 189 , 229 , 336
Windows Server	
disable UAC	52
Windows Server 2016 UI	48
Windows Server 2019 UI	48