Avaya Interaction Center

Installation Planning and Prerequisites

Release 7.3.x
Issue 5
July 2021

© 2021 Avaya Inc

All Rights Reserved.

Notice

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

Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, 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. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"**Hosted Service**" means 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, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in Section M(i)1 or 2 as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "**Software**" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-

alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "**Designated Processor**" means a single stand-alone computing device. "**Server**" means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. "**Instance**" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("**VM**") or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link "Heritage Nortel Products," or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components, to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA

PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

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

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying 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, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

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).

Downloading Documentation

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

Contact Avaya Support

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

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 Inc.

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

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

Contents

Chapter 1: Introduction 11
Purpose 11
Intended audience 11
Document changes since last issue 14
Related resources 15
Documentation 15
Training 16
Viewing Avaya Mentor videos 16
Support 17

Chapter 2: About Interaction Center 19
Internationalization and localization support 19
Supported languages 20
Limitations on support for Traditional Chinese 20
Limitations on support for Thai 21
Limitations on localization and internationalization support withCitrix 21
Interaction Center Release Notes 21
Interaction Center documentation 21
Interaction Center components 22
Interaction Center core servers 22
Interaction Center Design & Administration Tools 23
Agent interfaces 24
Avaya Computer Telephony for IC 25
Web Management 25
Avaya Email Management 26
Avaya Business Advocate for Interaction Center 26
Avaya Content Analyzer 27
Interaction Center Client Software Development Kit 27
Interaction Center for Siebel 29
Avaya Operational Analyst 29
Product interoperability 30
Unsupported features 30
Security for Interaction Center accounts 31
Interaction Center implementation roles 31
Performance factors 36
Interaction Center components 36
Volume of contacts 37
Number of concurrent users 37
Virus scan software 38
Network topology and configuration guidelines 38

Network security 39
Interaction Center communication protocol 39
WAN and LAN connections 39
Remote agents for Avaya Agent 40
Multiple network interface cards 43
Firewall guidelines for Avaya Agent 44
Network and Firewall requirements for Avaya Agent Web Client 45
Support for NAT and firewalls 45
Database guidelines 46
Interaction Center databases 46
Interaction Center database performance guidelines 47
Database table limitations 48
Prerequisites for OA Database Directory Structure 48
Time zone handling 49
Methods for time zone handling 49
Time zone methods used by Interaction Center components 50
Time zone requirements for Web Scheduled Callback 50
Interaction Center server guidelines 50
Server naming guidelines 51
Server partitioning guidelines 52
Web License Manager guidelines 53
Co-location of client applications with servers 53
Time synchronization for servers 54
Server failure considerations 55
Interaction Center core server guidelines 55
Voice channel server guidelines 60
Chat channel server guidelines 61
Email channel server guidelines 62
Business Advocate server guidelines 63
Web Scheduled Callback guidelines 66
Port utilization 66
Ephemeral ports in Interaction Center and OA 67
Limits implied by the ephemeral port range 67
Traditional configuration of the ephemeral port range 68
Firewalling the ephemeral port range 68
Changing the ephemeral port range 69
OA server guidelines 72
Event Collector server guidelines 73
Event Collector Bridge guidelines 75
Event Collector server failover guidelines 76
OA reporting problems caused by incorrect serverdeployment 76
Two Event Collector servers monitor the same agent domains 77

Chapter 4: Interaction Center single sitedeployment scenarios....79
Adapting deployment scenarios....79
Adding more servers and domains....80
Adding more Tomcat servers for the Client SDK or Web Services....80
Including additional servers in a deployment....80
Co-locating servers on one computer....81
Deploying servers on multi-processor computers....81
Items not shown in the deployment scenarios....82
Scenario 1: Single site, voice only....82
Scenario 1: Deployment overview....82
Scenario 1: Interaction Center domain overview....83
Scenario 1: Partitioning of servers....84
Scenario 1: Failover strategy....85
Scenario 2: Business Advocate for single site, voice only....88
Scenario 2: Deployment overview....88
Scenario 2: Interaction Center domain overview....89
Scenario 2: Partitioning of Business Advocate servers....90
Scenario 2: Failover strategy....91
Scenario 3: Business Advocate for single site, highvolume voice....92
Scenario 3: Deployment overview....92
Scenario 3: Interaction Center domain overview....93
Scenario 3: Partitioning of Business Advocate servers....94
Scenario 3: Failover strategy....95
Scenario 4: Single site, multi-channel....96
Scenario 4: Deployment overview....96
Scenario 4: Interaction Center domain overview....97
Scenario 4: Partitioning of servers....99
Scenario 4: Failover strategy....100
Scenario 5: Single site, multi-channel with high volumevoice....104
Scenario 5: Deployment overview....104
Scenario 5: Interaction Center domain overview....105
Scenario 5: Partitioning of servers....106
Scenario 5: Failover strategy....108
Scenario 6: Business Advocate for single site,multi-channel....112
Scenario 6: Deployment overview....113
Scenario 6: Interaction Center domain overview....113
Scenario 6: Partitioning of Business Advocate servers....115
Scenario 6: Failover strategy....116
Scenario 7: Single site, chat and email only....117
Scenario 7: Deployment overview....117
Scenario 7: Interaction Center domain overview....118
Scenario 7: Partitioning of servers....119
Scenario 7: Failover strategy....120

Scenario 8: Two sites, voice only 124
Scenario 8: Deployment overview....124
Scenario 8: Interaction Center domain overview 125
Scenario 8: Site overview 125
Scenario 8: Partitioning of Interaction Center servers 126
Scenario 8: Failover strategy....128
Scenario 9: Two sites, multi-channel 133
Scenario 9: Deployment overview....134
Scenario 9: Interaction Center domain overview 135
Scenario 9: Site overview 135
Scenario 9: Partitioning of servers 136
Scenario 9: Failover strategy....138
Scenario 10: Single instance Business Advocate for twosites, multi-channel 145
Scenario 10: Deployment overview....146
Scenario 10: Interaction Center domain overview 147
Scenario 10: Site overview 148
Scenario 10: Partitioning of Business Advocate servers 148
Scenario 10: Failover strategy for Business Advocate domains 151
Scenario 11: Multi-instance Business Advocate for twosites, multi-channel....152
Scenario 11: Deployment overview....153
Scenario 11: Interaction Center domain overview....154
Scenario 11: Site overview....155
Scenario 11: Partitioning of Business Advocate servers 155
Scenario 11: Failover strategy for Business Advocate domains....158
Scenario 13: Two sites, multi-channel, data center 160
Scenario 13: Deployment overview....161
Scenario 13: Interaction Center domain overview 162
Scenario 13: Site overview 162
Scenario 13: Partitioning of servers....162
Scenario 13: Failover strategy....165
Scenario 14: Business Advocate for two sites,multi-channel, data center 170
Scenario 14: Deployment overview....171
Scenario 14: Interaction Center domain overview 172
Scenario 14: Site overview 173
Scenario 14: Partitioning of servers....173
Scenario 14: Failover strategy....176

Chapter 6: Avaya Agent Web Client serverdeployment scenarios....177
Avaya Agent Web Client deployment guidelines 178
Agent configuration guidelines....179
Overview of deployment scenarios 180
Basic deployment....180
Overview of a basic deployment 180

Overview of network structure for a basic deployment 181
Load balancing deployment 182
Overview of a Load balancing deployment 182
Benefits of a Load balancing deployment 182
Overview of network structure for a load balancing deployment 183
Implementing Load Balancing with AAWC or SDK Clients 183
Summary 184
Multi-site deployment 187
Overview of multi-site deployment 187
Benefits of a multi-site deployment 187
Overview of network structure for a multi-site deployment 188
Hardware requirements for deploying Interaction Center 189
Hardware guidelines for Interaction Center servers 190
Hardware requirements 191
Server distribution 191
Server failover 191
Server speed 191
Server configuration impact 191
Disk space for Interaction Center servers 192
Disk space for server log files 192
Validation of Hardware configuration 192
IBM Logical Partition (LPAR) technology 192
Hardware requirements for Design & Administration Tools 193
Hardware requirements for IC servers 194
Required hardware for Avaya Agent WebConnector / SDK 195
Required hardware for agent workstations 195
Required hardware for the Avaya Agent interface 196
Required hardware for the Avaya Agent Web Client interface 197
Required hardware for IV Chat 197

Chapter 8: Interaction Center licensing 199
Prerequisites for license files 199
Identifying a physical address 200
Identifying a physical address for license files 200
Identifying a physical address in Windows 201
Identifying a physical address on Oracle Solaris 201
Identifying a physical address on AIX 201
Requesting a license file 202
Updating a license file 203
Requesting a replacement license file 204
Identifying HostID 205
Troubleshooting IC License Server 206

About Interaction Center databases 210
Mixed operating system combinations....210
Exceptions to supported database management systems....210
Requirements for database login 211
Installing database servers....211
Installing database client software....212
Location for database clients 213
Requirements for database clients....213
Configuring binary sort order for Web Management 214
Microsoft SQL Server....214
Installing SQL Server 2008....215
Installing SQL Server 2012 and SQL Server 2014 216
Recommended configuration for SQL Server 218
SQL server AlwaysOn Availability Groups 218
Oracle 220
Required version mode for Oracle Client 221
Required patches for an Oracle database....221
Installing Oracle Server....221
Installing Oracle Client....225
IBM DB2....225
Supported versions of DB2 226
Required version mode for IBM DB2 Client....226
Location of IBM DB2 Server 226
Configuring IBM DB2 server for Interaction Center 226
Installing IBM DB2 Client 228
Configuring IBM DB2 client for Interaction Center 228
Troubleshooting DB2 SQL1131N DARI error for IBM DB 9.5 on AIX6.1....229

Chapter 10: Supported Telephony switchesand software....231
Exceptions for Telephony software and switches....231
Avaya Aura® Communication Manager products 231
Supported components 232
Requirements for Avaya Aura® Communication Managerproducts....233
Downloading the Avaya Aura® Application Enablement Services -CVLAN client....234

Chapter 11: Supported Web servers 235
Components that require a Web server 235
Microsoft Internet Information Server....235
Security patches and hot fixes for Microsoft IIS 236
Configuring MIME types for Microsoft IIS....236
IIS Roles....236
Oracle iPlanet Web Server....237
Supported versions of Oracle iPlanet Web server 7.0.13 237

Oracle iPlanet 7 Web Server configuration parameters 237
IBM HTTP Server 238
Supported version of IBM HTTP server 239
Restriction on the deployment of IBM HTTP Server 239
IBM HTTP Server configuration parameters 239
Configuring Tomcat for Interaction Center Client SDKserver and Web Services server (Optional) 240
Installation location for Tomcat 240
Default web application contexts 240
Setting up load balancing or failover 241
Using Jakarta Tomcat Connector to configure a stand-alone HTTPserver 241

Chapter 12: Supported email servers 243
Configuring SMTP and POP3 / IMAP4 servers 244
Configuring security certificates for TLS 246

Chapter 13: Business Advocate 247
Exceptions to platform support for Business Advocate 247
Configuring Windows for Business Advocate 248
Business Advocate implementation modes 248
Implementing Business Advocate in Workgroup mode 248
Implementing Business Advocate in Active Directory mode 249
Configuring Business Advocate (BA) on the Windows Server 2019 250
Installing the Managing Message Queuing (MSMQ) service 251
Configuring Windows for Thai (optional) 251
Creating a user to configure the BA tool 252
Configuring SQL Server for Business Advocate 253
Creating a database for Business Advocate 253
Configuring the SQL Server client 253
Configuring a user to run Business Advocate services 253
Configuring SQL Server for Thai (optional) 254
Configuring Oracle for Business Advocate 254
Location of Oracle components for Business Advocate 255
Creating tablespaces for the Business Advocate database 255
Creating Oracle users for Business Advocate 257
Installing the Oracle Client 258

Chapter 14: Network configuration 259
Enabling TCP/IP networking 259
Verifying DNS resolution 259
Verifying DNS resolution in Windows 260
Verifying DNS resolution on Oracle Solaris and AIX 261
Troubleshooting an unresolved DNS entry 262

Chapter 15: Supported operating systems 263

Regional settings 263
Microsoft Windows Server 263
Prerequisites for Windows Server 264
Microsoft Windows based desktop operating system 265
Setting up Microsoft Windows 8.1 265
Setting up Microsoft Windows 7 266
Setting up Microsoft Windows Vista 266
Setting up Microsoft Windows XP Professional 267
Setting up Microsoft Internet Explorer 267
Security for Unix platforms 270
Oracle Solaris 270
Browser requirements for Oracle Solaris 271
Disk space requirements for Oracle Solaris 271
Configuration requirements for Oracle Solaris 271
User accounts for Oracle Solaris 273
IBM AIX 274
Browser requirements for AIX 275
Disk space requirements for AIX 275
Installing required locales 275
Configuration requirements for AIX 276
User accounts for AIX 277
Citrix 278
Deploying of Interaction Center components in a Citrixenvironment 278
Location of Interaction Center components 279
Multiple configurations of agent desktop applications 279
Interaction Center components supported in Citrix 280
Interaction Center support for publishing applications in Citrix 280
Limitations on support for Citrix 280
Licensing for Interaction Center in Citrix 281
Citrix Web interface 281
Citrix client interface 281
Limitations of integration with Citrix 283

Chapter 16: Required software components 285
About the supported versions 286
Exceptions to supported operating systems 286
Required software for Interaction Center servers 287
Required software for Interaction Center databases 289
Required Interaction Center databases 289
Optional Interaction Center databases 289
Prerequisites for the databases 290
Required software for Telephony 291
Telephony servers 291

Prerequisites for Telephony servers 292
Required software for Web Management 293
Web Management servers 294
Prerequisites for Web Management servers 295
Required software for Email Management and ContentAnalyzer 296
Email Management servers and Content Analyzer servers 297
Prerequisites for Email Management servers and ContentAnalyzer servers 298
Required software for Business Advocate 299
Business Advocate servers 300
Prerequisites for Business Advocate servers 301
Required software for the Interaction Center Client SDK 305
Required software for Interaction Center for Siebel 305
Required software for Design & Administration Tools 306
Required software for agent applications 307
Prerequisites for Avaya Agent 308
Requirements for Avaya Agent Web Client 309
Prerequisites for agent desktop applications on Citrix 310
Upgrading Daylight Saving Time (DST) patches 311
Adobe Acrobat Reader 313
Compilers for Interaction Center Server SDK 314
Compilers for Interaction Center SDK Sample Clients 315

Chapter 18: Server virtualization support 317
VMWare support 318
VMware vSphere Host considerations 319
VMware Interaction Center Guest Operating Systems 321
Overview of commissioning Interaction Center with VMware 321
Performance monitoring and management 323
VMware Snapshot considerations 324
Time synchronization considerations 325
VMware Horizon View 325
About VMware vSphere vMotion 327
Configuring Hosts for vMotion and Migrating Powered-On VirtualMachines 328
Migrating with vMotion 329
Avaya Interaction Center Deployment for VMotion 330
Troubleshooting VMware 330
Microsoft Hypervisor support 331
Microsoft Hypervisor Host considerations 332
Using Hypervisor for Interaction Center Guest Operating Systems 332
Overview of commissioning Interaction Center with MicrosoftHypervisor 333
Microsoft Hypervisor Checkpoint considerations 335
Memory management in Microsoft Hyper-V 2012 336

Appendix A: AES administration 339
Avaya Aura® Application Enablement Servicesadministration 340
AES Configuration for IC 7.3.x 340
Telephony Server support with AES GRHA 342
Advantages of AES GRHA 342
Appendix B: Switch administration 343
Avaya Aura® Communication Manager administration 343
Configuration for IC 7.3.x 344
Best Services Routing (BSR) option 344
Timed ACW 345
Call vectoring adjunct routing request 345
Configuring AES server software 353
Configuring redundant CTI links 353
Configuring the switch in an ACD environment 355
Suppressing logout event when CMS moves agents across skills 355
Service Observing 356
Call Coverage 357
Universal Call ID 359
Index 361

Chapter 1: Introduction

Purpose

The purpose of this guide is to provide detailed information about the planning and third-party software required to deploy an Avaya Interaction Center, Release 7.3.x system.

Deployment of an Interaction Center system is a complex task that requires careful planning. Before you can install and configure your Interaction Center system, review the information in this manual to ensure that your system includes all necessary prerequisites.

This manual includes the following information to help you plan, install and configure an Interaction Center system:

- Deployment planning information, including sample deployment scenarios.
- Minimum system requirements to install and run Interaction Center on the supported Windows operating systems.
- Minimum system requirements to install and run Interaction Center servers on the supported Oracle Solaris operating systems.
- Minimum system requirements to install and run Interaction Center servers on the supported AIX operating systems.

  Note:
  IBM AIX and IBM DB2 are only supported on Interaction Center Release 7.3, 7.3.1, and 7.3.2. For more information see the Unsupported features on page 30. All the information related to IBM AIX and IBM DB2 is only applicable to Interaction Center Release 7.3, 7.3.1, and 7.3.2.
- Network configuration requirements for Interaction Center.
- Supported hardware and software platforms for required third-party applications.
- Information on how to install and configure third-party applications required by Interaction Center.

Intended audience

This guide is for the administrators and customers using Avaya Interaction Center.

Document changes since last issue

We have modified the following sections in this document since the last issue:

- Installing SQL Server 2008 on page 215
- Installing SQL Server 2012 and SQL Server 2014 on page 216
- Configuring Hosts for vMotion and Migrating Powered-On Virtual Machines on page 328
- Unsupported features on page 30
- Support for Citrix XenApp 7.5
- Server virtualization support on page 317

Related resources

Documentation

See the following related documents at http://support.avaya.com.

Title	Use this document to:	Audience
OA Planning and Prerequisites	The purpose of this guide is to provide detailed information about the setup and configuration of the servers on which you install Avaya Operational Analyst.	People who make contact center reporting planning and buying decisions for the customer Database administrators System administrators System implementation team
OA Installation and Configuration	The purpose for this guide is to provide detailed instructions for installing and upgrading Avaya Operational Analyst.	Avaya Global Services personnel Business partners Customers who install their own Avaya OA software

Finding documents on the Avaya Support website

Use this procedure to find product documentation on the Avaya Support website.

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com.
2. At the top of the screen, enter your username and password and click **Login**.
3. Click **Documents**.
4. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
5. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
6. Use the **Content Type** filter on the left to select the type of document you are looking for, or click Select All to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.

7. Click **Enter**.

Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. In the **Search** field, enter the course code, and click **Go to search** for the course.

Course Code	Course Title
ATC01175WEN	IC and OA Overview
ATC01176IEN	Interaction Center Administration and Configuration
AUCC100010695	IC-Siebel Integration
ATC100011017	IC-Siebel Integration, Installation and Troubleshooting
AUCC100010728	The Basics of Operational Analyst Part 1
AUCC100010729	The Basics of Operational Analyst Part 2

Viewing Avaya Mentor videos

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

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 http://support.avaya.com and perform one of the following actions:
  - In Search, type Avaya Mentor Videos to see a list of the available videos.
  - In Search, type the product name. On the Search Results page, select Video in the Content Type column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

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

Chapter 2: About Interaction Center

Avaya Interaction Center (Interaction Center) is a multimedia contact center solution that provides a blended channel management solution for voice, Web, and email contacts.

Interaction Center combines server and client applications to help enterprises to manage information. Interaction Center provides a single view of the customer, a single set of business rules and workflows, and a single agent interface across all media.

Interaction Center can perform the following:

- Manage high volumes of customer contacts.
- Support a broad range of communication channels.
- Deliver consistent and integrated customer service.
- Capture, manage, and derive business value from all relevant customer information.

This section provides an overview of Interaction Center. This section includes the following topics:

- Internationalization and localization support on page 19
- Interaction Center Release Notes on page 21
- Interaction Center documentation on page 21
- Interaction Center components on page 22
- Avaya Operational Analyst on page 29
- Unsupported features on page 30
- Security for Interaction Center accounts on page 31
- Interaction Center implementation roles on page 31

Internationalization and localization support

This section describes the languages for which Interaction Center provides internationalization and localization support, and any limitations on that support. This section includes the following topics:

- Supported languages on page 20
- Limitations on support for Traditional Chinese on page 20
- Limitations on support for Thai on page 21

- Limitations on localization and internationalization support with Citrix on page 21

Supported languages

Internationalization and localization support includes localized interfaces and localized online help systems for agent desktop applications. Interaction Center supports the following languages with the localization release of Interaction Center:

- English
- German
- French
- Italian
- Spanish
- Portuguese
- Japanese
- Korean
- Simplified Chinese
- Thai
- Traditional Chinese
- Russian

Limitations on support for Traditional Chinese

Interaction Center supports Traditional Chinese only on Windows Server with a supported Oracle database.

Interaction Center does not include support for Traditional Chinese internationalization and localization in the following components:

- Avaya Content Analyzer
- Business Advocate
- Interaction Center for Siebel Integration
- IC Script Debugger
- Spell Checker

Limitations on support for Thai

Interaction Center supports Thai only on Windows and Oracle Solaris operating systems. Interaction Center does not support Thai on AIX.

Interaction Center does not include support for Thai internationalization and localization in the following components:

- Document searches in Web Self-Service
- Spell checking
- Content Analyzer
- Thai B. E. (Buddhist Era) date format
- Thai word wrap in the website

Limitations on localization and internationalization support with Citrix

Citrix is responsible for all localization and internationalization support within the Citrix MetaFrame environment.

Interaction Center Release Notes

You must carefully read the *Avaya Interaction Center* 7.3.x *Release Notes* file before you plan your Interaction Center deployment, or install and configure your Interaction Center system.

The Release Notes is available on the Avaya Support website at http://support.avaya.com.

Interaction Center documentation

The Interaction Center Release 7.3.x documentation is available on the Avaya Support website at http://www.avaya.com/support.

Interaction Center components

You can deploy Interaction Center in a variety of configurations. A typical configuration includes several Interaction Center components.

This section includes the following topics:

- Interaction Center core servers on page 22
- Interaction Center Design & Administration Tools on page 23
- Agent interfaces on page 24
- Avaya Computer Telephony for IC on page 25
- Web Management on page 25
- Avaya Email Management on page 26
- Avaya Business Advocate for Interaction Center on page 26
- Avaya Content Analyzer on page 27
- Interaction Center Client Software Development Kit on page 27
- Interaction Center for Siebel on page 29

Interaction Center core servers

The Interaction Center core servers are the core of the Interaction Center architecture. These servers manage communication between internal and external components, and control the routing of contacts.

The Interaction Center core servers manage communication between the following components:

- Telephony equipment, such as ACDs, PBXs, and IVRs
- Internet applications, such as Web, Email, and VOIP applications
- Databases
- Interaction Center administrative tools
- Interaction Center client applications

Interaction Center Design & Administration Tools

The Interaction Center Design & Administration tools include:

- IC Manager on page 23
- Avaya Workflow Designer on page 23
- Avaya Database Designer on page 24

IC Manager

IC Manager is an administrative application that monitors, manages, and configures Interaction Center. With IC Manager, contact center supervisors and system administrators can:

- Add, delete, and modify information for agents, servers, and devices
- Start, stop, and configure Interaction Center servers
- Monitor server, agent, and device activities

Avaya Workflow Designer

Avaya Workflow Designer is a customization tool for workflows. Workflow Designer includes sample workflows and pre-defined blocks. You can use Workflow Designer to design, create, and compile:

- Routing workflows that control the routing of contacts through all media channels, and manage the related data during the initial stages of a contact
- Blending workflows that implement business rules to define how agents handle contacts across multiple media
- Email analysis workflows that analyze and process inbound and outbound email contacts
- Agent scripts that can be stored and run in the application
- Business Advocate workflows that qualify contacts for Business Advocate routing

You can also use Workflow Designer to create and compile custom flows to meet the specific needs of your enterprise and your contact center.

Avaya Database Designer

Avaya Database Designer is a customization tool that helps you customize Avaya applications and configure Interaction Center databases. With Database Designer, you can:

- Set database connections
- Configure databases and database connections for Interaction Center and Business Advocate
- Create data sources for servers to access the database
- Upload the application interface, help files, data model, and IC Scripts to the database when you implement Avaya Agent or Avaya Agent Web Client.

Agent interfaces

This section includes the following topics that describe the primary agent interfaces:

- Avaya Agent on page 24
- Avaya Agent Web Client on page 24

Avaya Agent

Avaya Agent is an agent desktop application that integrates multiple media channels and agent applications. With Avaya Agent, an agent can:

- Handle inbound contacts from customers and others in multiple media, such as voice, email, and chat
- Handle outbound voice contacts to customers and others
- Access and review information about a customer from the Interaction Center database

Avaya Agent Web Client

Avaya Agent Web Client provides a browser based application interface for the agents in your contact center. Agents do not need the Avaya Agent Web Client software installed on their desktops.

The Avaya Agent Web Client interface provides a functionality that is similar to the Avaya Agent interface. Agents access the interface by connecting to the Avaya Agent Web Client server through a Web browser.

Avaya Agent Web Client supports agent tasks and supervisor tasks. A supervisor can monitor chat sessions in Avaya Agent Web Client. You cannot log in to both Avaya Agent Web Client and Avaya Agent applications simultaneously from the same computer.

Avaya Computer Telephony for IC

Avaya Computer Telephony for IC (Telephony) is a computer telephony integration solution that seamlessly links computers, telephones, voice, and data to provide intelligent call qualification and routing in conjunction with voice and data collection. This solution has an open, scalable architecture that integrates with the most popular PBXs, ACDs, and IVRs to maximize the investment of a company in the telephony infrastructure.

Web Management

Avaya Web Management (Web Management) is a Web-based marketing, sales, and service application that personalizes and manages Web transactions across the enterprise. Web Management includes integrated functionality for:

- Web self-service
- Live customer interaction through chat contacts
- Email functionality in your customer website

Web Management provides access to these features through multiple Web channels, including Web chat, Web-driven customer callback, and real-time, browser-based collaboration and navigation. By providing customers with direct Web-based service, Web Management can:

- Increase buy-to-browse ratios
- Let your customers handle multiple tasks during a single Web visit
- Reduce the costs associated with telephone-based service, because customers can get more done on the Web

Web Self-Service is a component of Web Management that includes a Frequently Asked Questions (FAQ) database. Agents and customers can search this database using the HTML interface for Web Self-Service.

Avaya Email Management

Avaya Email Management (Email Management) is an application that helps contact centers effectively manage the increasing volume of customer email with intelligent email routing and automated response capabilities.

Email Management uses rules-based email management technology to analyze incoming messages and compose personalized answers that can be automatically sent to a customer or queued for review by an agent. Email Management uses data from the IC database and from external sources to help develop highly personalized responses.

The Web Self-Service FAQ database can also store suggested responses for agents handling email contacts. The Interaction Center email analysis workflow can be configured to automatically search the Web Self-Service FAQ database for suggested responses using specific keywords found in the customer email or using the email topic as determined by Avaya Content Analyzer. Avaya Content Analyzer is an optional component. These suggested responses are delivered to agents with the customer emails to enhance email processing efficiency.

Avaya Business Advocate for Interaction Center

Avaya Business Advocate is part of the standard Interaction Center offer. An enterprise can benefit from the predicted soft ACD technologies without requiring additional license requirements.

Business Advocate is an application that manages email, Web chat, and voice contacts. Business Advocate understands the needs of each service that you offer to your customers. Business Advocate allocates agent resources to those services to meet the service levels set by you and expected by your customers.

The patented predictive technology in Business Advocate:

- Optimizes resource allocation and contact routing decisions
- Implements Universal Queue for routing
- Uses a location enhanced set of distributed routing algorithms
- Provides optimized, configuration-less routing across different sites for all media

Business Advocate provides fully integrated multimedia, multi-site management of all your contacts.

With Business Advocate, you can increase and decrease your agent resource pool. Business Advocate monitors contacts, service classes, and agents in real time. Business Advocate uses the information from the real-time monitoring to apply your agent resources where the agents are most needed.

Avaya Content Analyzer

Avaya Content Analyzer (Content Analyzer) is an optional Interaction Center component that performs content analysis on incoming and outgoing email. Content Analyzer applies complex, natural language algorithms to the content of email contacts, and derives a statistically-based match between the intention of that text and a list of pre-applied topics.

With Content Analyzer, you can automatically:

- Identify the language that a customer uses in an email contact
- Route email contacts to agents based on topic and agent skills
- Screen out an email to which the contact center does not want to respond
- Suggest responses for agents to use when an agent responds to an email contact
- Respond to email contacts automatically without agent intervention

Content Analyzer can analyze and classify text only in the following languages:

- English
- Chinese
- French
- German
- Italian
- Japanese
- Korean
- Portuguese
- Spanish

Content Analyzer can identify additional languages in the text of an email contact, although Content Analyzer cannot analyze those languages. For more information, see *IC Administration Guide: Servers & Domains*.

Interaction Center Client Software Development Kit

The Avaya Interaction Center Client Software Development Kit (Client SDK) is a client-side toolkit that you can use to:

- Develop a custom agent desktop application with access to Interaction Center core functionality
- Allow existing custom agent desktop applications to access the Interaction Center core functionality

- Allow a third-party agent framework or application to work with Interaction Center
- Integrate a custom application or custom code on clients or on servers

A custom agent desktop application developed with the Client SDK can:

- Save valuable screen space. The agent desktop does not need to display an Interaction Center agent application.
- Minimize functionality to only those features required for a specific implementation. The custom application does not have to include features that are not required for an agent in the contact center.

The Client SDK includes the following features:

Client API: This client-side API includes an application-level protocol that hides communication and session management and provides interfaces that are meaningful to custom applications. Avaya designed the Client API to support future Interaction Center enhancements.

Supported technologies: The Client SDK:

- Includes .NET and Java libraries for custom application development.
- Works with NAT, firewalls, and proxy servers.

Security: The Client SDK supports the following security:

- Secure Socket Layer (SSL) for synchronous communication.
- Advanced Encryption Standard (AES) for asynchronous communication.

Supported integrations: The Client SDK supports server-side and client-side integrations with an Interaction Center core system.

Supported scalability: The Client SDK provides the following support for scalability:

- Up to 500 agents per Client SDK server

Support for internationalization: The Client SDK provides internationalization support for custom applications in languages other than US English. For more information, see *IC Client SDK Programmer Guide*.

Interaction Center for Siebel

Avaya IC for Siebel includes the following types of integrations:

Integration type	Definition
Native	Thin-client Siebel provides the entire desktop user interface for an Interaction Center for Siebel integration. Avaya IC provides voice and email work item routing and data collection reporting that occurs in the background.
Hybrid	In an Interaction Center for Siebel integration, the desktop user interface consists of a Siebel call center internet browser window and an Avaya Agent task bar window. The integration of Avaya IC with Siebel allows you to use the customer management features in the Siebel software and the features in Avaya IC that automate the processing of customer contacts. All channels, including voice, email, and chat are supported in Hybrid type of integration.

The Interaction Center for Siebel integration combines Interaction Center with the Siebel application. Interaction Center for Siebel provides the customer management features of the supported versions of Siebel with the contact management and routing features of Interaction Center.

With Siebel integration, the agents in your contact center can provide a unique and customized interaction with each customer. Each agent:

- Receives work items that are appropriate for the set of skills of that agent.
- Performs contact work in multiple media channels.
- Accesses any historical data about work previously performed for a specific customer.

In Interaction Center for Siebel, all agent interactions occur through the Siebel Communications Toolbar.

For more information about planning and prerequisites for Interaction Center for Siebel, see *Avaya IC for Siebel Integration*

Avaya Operational Analyst

Avaya Operational Analyst (OA) is a required component of Interaction Center. OA performs operational reporting for a multimedia contact center, growing from single channel analysis, to full interaction, multi-channel analysis with a common data model and user interfaces across these systems.

IC 7.3 integrates and works with OA 7.3.

OA provides reporting tools that show you summary and detail information about the contact activity at your contact center.

With OA, you can:

- Create and maintain customized reports that help managers to monitor contact center, marketing, and service activities.
- Build PowerPlay data cubes, then view the summary information in the cube and drill through to more detailed information in the CCQ database, and IC Repository database.
- Use business reporting features to distinguish and detail contacts leading to sales, fulfillment requests, or customer service requests.

For more information about OA and its prerequisites, see OA *Installation Planning and Prerequisites*.

Product interoperability

For information about interoperability, see the *Avaya IC and OA 7.3.x Overview and Specification guide*. For the latest and most accurate compatibility information, go to:

http://support.avaya.com/CompatibilityMatrix/Index.aspx

Avaya Interaction Center and Operational Analyst Overview and Specification Guide contains information for the following:

- Supported OA 7.3.x releases
- Supported Server Operating Systems
- Supported Desktop Operating Systems
- Supported Databases
- Supported Java Runtime Environment and Java Development Kit
- Supported Web Browsers
  - Browsers supported on End-Customer Chat Escalations
  - Browsers supported for IC client application and Email Template Administration and Website applications in IC

Unsupported features

Interaction Center does not support the following features starting with Interaction Center 7.3.x:

- List Management: Interaction Center 7.3.x does not support the List management application.

- Same Time Feature: The Same Time feature from Web agent is no longer supported.

Security for Interaction Center accounts

Interaction Center has security features for agent and administrator accounts and passwords. The security features include configurable parameters for Interaction Center accounts, such as:

- Maximum log-in attempts before an account is disabled.
- Rules for password change intervals.
- Rules for password validity, such as minimum and maximum number of alphabetic and numeric characters.
- Records of the creation and changes to all login accounts.
- Password is encrypted and then shared on network for logging to website, RLManager, Avaya Agent Web Client and SDK.

These security features help defend the Interaction Center system against unauthorized users and malicious use.

Note:

Use Interaction Center security features in conjunction with the other contact center security measures.

For more information about how to configure the security parameters, see *IC Administration Guide*.

Interaction Center implementation roles

Implementing an Interaction Center system requires knowledgeable resources. The number of resources you need depends on your environment, and the complexity of the installation.

An implementation team can include representatives from Avaya, an Avaya Business Partner, and the customer. Members of an implementation team can perform more than one role.

The complexity of your Interaction Center installation depends on many factors, such as:

- The number of many media channels in your Interaction Center system.
- The third-party systems you need to integrate with your Interaction Center system.
- The business processes you want to implement in your Interaction Center system.

The following table lists the different roles that Interaction Center projects may require. This table does not include the roles that OA may require. For information about the requirements of OA, see OA *Installation Planning and Prerequisites*.

Role	Responsibility
Project manager	Coordinates developer tasks, manages the project plan, and provides status to management and project sponsors.
Architect	Designs the physical and logical system architecture. Provides designs for complex integrations and logic. Assists other developers with designs and issues. Designs the physical and logical server architecture.
Network administrator	Establishes user network accounts. Monitors the network using network operating system tools or network hardware tools to ensure adequate performance and to diagnose network related issues.
Software developer	Uses the optional Client SDK to create an agent application that leverages the Interaction Center framework. Must be proficient with either Java or .NET development environment.
Application and workflow designer	Determines requirements for application and workflow customizations. Works with the Project Manager to determine estimates for requirement implementation.
Database administrator	Works with the database operating system tools. Installs the database server and required client components. Establishes required database accounts. Tunes the database for optimal performance. Ensures security and database integrity. Ensures standards for data normalization and data attributes. Diagnoses database connectivity and performance issues.
Data modeler	Uses Database Designer to modify database tables and data definitions to meet customer requirements. Assists interface designers by adding table fields, table sets, browsers, and table relations to activate customer required functionality.
Interface designer	Uses XML to modify the layout of the interface for Avaya Agent. For Avaya Agent Web Client, use XML, JSP, and JavaScript to modify the layout of the interface.
Business logic developer	Uses scripting language to ensure that business logic and IC Scripts perform to requirements. Business logic includes checking and verifying program flow, logic, and data entered by users.
Media routing workflow developer	Uses Workflow Designer to modify or create routing workflows for media contacts, including voice contacts, email contacts, and chat contacts. Tests flows with the Workflow servers to make sure they perform correctly and meet performance needs.

Role	Responsibility
Prompter workflow developer	Uses Workflow Designer to modify or create prompting flows as required by the needs of your contact center. Prompter flows can assist agents with typical tasks and provide the scripts for agents to follow during contacts with customers.
Integration test analyst	Designs and runs tests that exercise the developed system. Verifies that the configuration and customization do not cause the Interaction Center system to fail. Uses tools such as WinRunner to automate testing processes.
System test analyst	Designs and runs tests that exercise the developed system in accordance with the business processes of your contact center. Can use tools such as WinRunner to automate testing processes.
Server and Workstation software specialist	Installs software on servers and client computers. Configures the software to operate to the specifications for failover and redundancy. Creates installation procedures or workstation images to enable rapid deployment of agent workstations.
Project librarian	Establishes source code management system and implements rules for developers to check out and check in their source code. Merges changes from multiple developers, if required. Creates software builds for integration tests, system tests, and production environments.
Data migration specialist	Analyzes existing data in legacy systems and creates programs or manual procedures to populate data fields in the new system.
Telephony specialist	Uses Telephony tools to establish agent accounts. Creates or modifies telephony vectors or similar components to help communication with the Interaction Center Telephony server. Configures the Interaction Center Telephony server for optimal performance.
Email specialist	Uses email server tools to establish mail boxes and accounts required for the Interaction Center system. Configures and uses existing email tools to optimize flow of email data. Configures or creates Content Analyzer rules for auto response and auto reply functionality.
Web specialist	Customizes customer-facing Web pages to insert links for Avaya Web Management. Enables, configures, and customizes Web options and Web pages to meet the requirements of your contact center.
Reporting specialist	Uses OA to create or customize reports to meet the needs of the contact center.
Business Advocate specialist	Understands, implements, and tunes routing and configuration in Business Advocate for maximum performance.

Chapter 3: Guidelines for an Interaction Center deployment

Before you deploy and configure Interaction Center, you must plan the components in the system and how the components will be distributed across different computers. Planning an Interaction Center system requires that you understand the needs of the contact center, and that you understand how Interaction Center components work together and with other systems on the network.

If your Interaction Center system includes integration with Siebel, see *Avaya IC for Siebel Integration* for guidelines and planning information.

CAUTION:
Do not install Interaction Center on computers that also host software that filters or controls network access. These types of software can cause Interaction Center to fail or seriously impact performance. For example, pornography filters or software firewalls can affect network access in several ways. They can cause a slowdown in network access, cause applications that open a large number of sockets to fail, or rewrite packets.

This section includes the following topics:

- Performance factors on page 36
- Network topology and configuration guidelines on page 38
- Database guidelines on page 46
- Time zone handling on page 49
- Interaction Center server guidelines on page 50
- Ephemeral ports in Interaction Center and OA on page 67
- OA server guidelines on page 72
- OA reporting problems caused by incorrect server deployment on page 76

Tip:
The information in this chapter is general and cannot anticipate the needs of all contact centers. You can consult an Interaction Center specialist to create a deployment strategy that meets the needs of your contact center.

Performance factors

When you plan the deployment of your Interaction Center environment, review the answers to the following questions:

- Which Interaction Center components does the contact center require?
- How high do you expect the volume of contacts to be for each component?
- How many concurrently connected users do you expect the system to handle?

The answers to these questions help you to decide the type and number of hardware components you need for the Interaction Center system, and the best way to distribute the servers among the hardware components.

This section does not provide you with answers to these questions. The answers are different for every Interaction Center system, because the needs of every contact center are different. This section discusses the issues to consider when you answer these questions for a contact center. This section includes the following topics:

- Interaction Center components on page 36
- Volume of contacts on page 37
- Number of concurrent users on page 37

Interaction Center components

The number of computers you need to deploy depends on the components and the contact rate for an Interaction Center system. For example, a basic Interaction Center system requires:

- At least one server for each media.
- One computer to host the Design & Administration Tools.
- One computer to host the databases and relational database management system.
- One computer to host the OA components.
- One client computer for each concurrently active agent.
- One server to host the Web Connector server.
- One server to host the SDK server.

Interaction Center requires additional computers if the system includes more than one site or additional components, such as Business Advocate.

For more information about the recommended number of computers for an Interaction Center system, see the following deployment scenarios:

- Interaction Center single site deployment scenarios on page 79

- Interaction Center multi-site deployment scenarios on page 123.

Volume of contacts

Determine the volume of contacts that the contact center handles during peak periods of activity when you determine the following:

Processing power required for the computers that host Interaction Center servers: For example, if your contact center has a high contact delivery rate, ensure that the Interaction Center media servers, which support the contact qualifications and delivery, such as the Telephony server and Workflow server, have sufficient processing power.

Multiple servers to divide the responsibilities for the delivery of contacts: For example, the Workflow server processes the majority of the contacts and business rules. The Workflow server can handle tasks, such as media routing, agent blending, prompting, letter generation, and generic business logic. Distribute these responsibilities across multiple Workflow servers to maximize performance and response from the Workflow server and reduce the impact of one Workflow server on the other Workflow servers in an Interaction Center system.

Response time required for contacts in each media: For example, response time is critical for telephony services. Streamline the contact qualification and routing to ensure that telephony services respond in a timely manner during peak periods. Partition the load horizontally by increasing the number of servers. Configure each Workflow server to access only the database that contains the tables required by the workflows. Develop workflows that perform only a single database operation before the workflows make a routing decision.

Number of concurrent users

Consider the number of agents and other Interaction Center users who are typically logged in concurrently during peak periods of activity. The load in an IC system can be directly related to the number of concurrent users. The larger the user population, the more computational resources required.

To avoid performance issues, distribute the responsibilities for the Interaction Center users among multiple servers on different computers.

Some servers have limitations on the number of concurrent users. For more information see *Avaya Interaction Center and Operational Analyst Overview and Specification Guide*.

Virus scan software

Virus scanning software can affect the performance of Interaction Center. Ensure virus scanning is configured to scan program files only (that is, executables, DLLs, and so on), not all files. If virus scanning is configured to scan all files, IC performance may be unacceptable due to frequent scanning of log files and data files.

You must configure the virus scanning software as follows:

- Scan only program and executable files, not all files.
- On the DBMS system, exclude the database files, as recommended by the DBMS vendor, like data files and log files.
- Exclude the directory %PABASE%\data from virus scanning.
- Exclude the directory %AVAYA_IC73_HOME%\logs from virus scanning.
- Exclude the directory %AVAYA_IC73_HOME%\etc from virus scanning.
- Exclude the directory %PABASE%\reports\cognos from virus scanning.
- Exclude the directory %Avaya_IC73_HOME%\etc from virus scanning on every agent machine.
- Exclude the Cognos files from scanning (for example, *.imr files).
- Configure the full system scan to run when overall system activity is low.

Network topology and configuration guidelines

Network topology and configuration have a direct impact on the performance of Interaction Center client-server communications.

Tip:
Consult network specialists to determine the optimal network configuration.

This section includes general guidelines for network topology and configuration that typically result in good performance and reliability for Interaction Center. This section includes the following topics:

- Network security on page 39
- Interaction Center communication protocol on page 39
- WAN and LAN connections on page 39
- Remote agents for Avaya Agent on page 40
- Multiple network interface cards on page 43

- Firewall guidelines for Avaya Agent on page 44
- Network and Firewall requirements for Avaya Agent Web Client on page 45
- Support for NAT and firewalls on page 45

Network security

Make sure that the network provides a minimum of the following security for all computers that host Interaction Center servers and applications:

- Secure physical location.
- Properly administered user IDs and permissions.
- Protection from network-based attacks.
- Regular review of program logs.

Interaction Center communication protocol

Interaction Center components use TCP/IP to communicate across the network. See the documentation for your network to determine the best configuration to support this communication protocol.

Note:

Interaction Center only supports IPv4 IP address. Ensure that all systems where Interaction Center is installed are configured with IPv4 IP addresses.

WAN and LAN connections

In general, LAN connectivity has higher bandwidth, lower delay, and is more stable than WAN connectivity.

If your Interaction Center system includes multiple sites that are connected by WANs, Interaction Center requires reliable WAN connections for proper operation and performance.

Interaction Center requires that backup services be configured on the same LAN. Configuring backup services helps to avoid the increased latency and limited bandwidth when failover occurs across on a WAN.

Remote agents for Avaya Agent

If the Interaction Center system includes remote agents, the agents must have a VPN that meets the requirements of Interaction Center and the network must have sufficient bandwidth for each agent. Remote agents can be voice enabled with an IP Telephony solution such as Avaya IP Agent. For example, an Interaction Center system with remote agents could include all Interaction Center servers and the RDBMS located at a data center and the remote agents located at satellite sites.

This section includes the following topics:

- Connections for remote agents on page 40.
- Bandwidth for remote agents on page 41.
- Bandwidth requirement and latency limitation for multiple channels / servers on page 42

Connections for remote agents

CAUTION:
If the Virtual Private Network (VPN) that provides the connection does not assign a unique IP address to each remote agent, agents who log in with the same IP address after the first agent may not be able to communicate with certain Interaction Center servers, such as the Telephony server.

If the Interaction Center system includes agents who log in from remote sites, Interaction Center requires the following:

- Every agent must have a high-speed connection with a VPN client.
- The VPN client must establish a virtual device with a unique IP address for that agent.
- The VPN client must place the device, whether virtual or not, and the associated unique IP address as the first item in the list of devices that is presented to Interaction Center after login, as the IP address of the first device is included in the Interaction Center session ID for that agent.

Bandwidth for remote agents

To properly work in a remote agent environment, the underlying network topology must provide adequate bandwidth and latency. The required operational bandwidth in this table is based on the agent population and the incoming contact rate for each channel that an agent may handle. If the Interaction Center system also includes customization of the EDU, this variable can also change the bandwidth requirement. To estimate the required bandwidth, use the data in the following table and calculation.

Channel	Kilobits per contact
Chat	800
Email (10K message)	800
Voice (Avaya Agent)	480
Voice (Avaya Agent Web Client)	380

For example:

E * (B *2 + 480 kbps) + E * (A*P)/3600

V * 480 kbps/3600

C * (M * S + 480 kbps)/3600

Where:

- E = number of email contacts per hour
- B = average size of email body
- A = average size of email attachment
- P = percentage of email contact with attachments
- V = number of voice contacts per hour
- C = number of chat contacts per hour
- M = number of chat messages between customer and agent
- S = average size of chat message
- kbps = kilobits per second

Multiply the value calculated for the channel by the number of agents for an estimate of your bandwidth requirements.

Important:
This value is only an estimate. You must consult Avaya Professional Services for proper sizing based on the specific needs for the contact center.

Email contact bandwidth: For email contacts, the number of kilobits per contact depends on the average size of the email message and reply, frequency, and size of attachments.

Chat contact bandwidth: For chat contacts, the number of kilobits per contact depends on the number of messages exchanged within a single contact as well as the size of each message.

Latency: The latency between the Avaya Agent client and the data center must not exceed 150ms average round trip packet time as measured with a “ping” of 1024-byte data size. Anything greater results in degraded client response time.

Impact of agent login: The login of an agent can generate a significant volume of traffic. When an agent logs in for the first time, 3-MB of data is downloaded to the desktop. The bulk of this traffic consists of IC Scripts for Avaya Agent. Customizations might increase the number of IC Scripts downloaded. Following the initial login, the IC Scripts are cached on the local computer. For all subsequent logins, only changed IC Scripts and the VESP Implementation Repository (vesp.imp) are downloaded to the agent desktop, which can amount to 500KB. The size of the vesp.imp is directly related to the number of servers in the system with an average of 1KB per server.

Bandwidth requirement and latency limitation for multiple channels / servers

Avaya IC 7.3.x has been tested for the following bandwidth requirement and latency limitation for better performance.

Email

- Bandwidth requirement between Email / Poller Servers and Data Servers with attachments (approximate size 1-MB) is 100-Mbps or more with low round trip latency not exceeding 10 milliseconds
- Due to high bandwidth requirement between Dataserver and DB server, it is always recommended to have the DB Server and Dataserver co-located

Voice

- Bandwidth requirement between TS and AES is approximately 10-Mbps and round trip latency not exceeding 30 milliseconds.
- Bandwidth requirement between HttpVox and Web Server (IC Connector) is approximately 10-Mbps and round trip latency not exceeding 20 milliseconds.
- Bandwidth requirement between SIPTS and SES is approximately 10-Mbps and round trip latency not exceeding 30 milliseconds.

Chat

- Bandwidth requirements between ICM Server and Attribute servers are minimal and hence it can run over WAN with 5-Mbps link and approximately 100 milliseconds round trip latency

Multiple network interface cards

You need to plan the assignment of your Network Interface Cards (NICs) if the servers in your Interaction Center configuration include a supported Windows operating system.

CAUTION:
If you do not configure the correct NIC for Interaction Center, your system may have problems with NIC driver conflicts, Windows operating system errors, and Interaction Center errors.

When you plan the deployment of your Interaction Center system, determine the following guidelines:

First physical NIC: WebLM supports all the NICs that are available on the computer. The license file could have the MAC address associated with any of the NICs available on the server. WebLM accepts the license file if either of the MAC addresses on the server match the MAC address in the license file. However, you must use the first physical NIC on the computer.

- The NIC is closest to the central processor and is connected to the LAN or WAN.
- The system default NIC in the registry of a Windows computer.

To verify the location and the physical address of the first physical NIC on the computer that hosts the Web License Manager, see Identifying a physical address for license files on page 200.

Note:
Exercise caution when you add a NIC to the computer that hosts Web License Manager, or if you replace a NIC on that computer. Interaction Center license files are defined with the physical address of the NIC. If the physical address changes, the Web License Manager and the Interaction Center system cannot function.

ORB server and multiple NICs: If an ORB server runs on a computer with multiple NICs, you must configure Interaction Center with the IP address for the first network interface card on the computer. The ORB server cannot run on any other NIC.

Webconnector (AAWC)/SDK server and multiple NICs: If the Webconnector (AAWC)/SDK server runs on a computer with multiple NICs, you must configure Interaction Center with the IP address for the first network interface card on the computer. The Webconnector (AAWC)/SDK server cannot run on any other NIC.

Multiple NICs on Web chat computer: If the computer that hosts Web Chat has multiple NICs, assign a different DNS to each NIC.

For example, the computer that hosts Web Chat usually has two interfaces: one for external access from the internet, and one for internal access from the intranet. If both NICs have the same DNS, an agent connection for a Web Chat can result in the SSL connection hair pinning through the external firewall.

Communication Manager switches and software: If your Interaction Center system includes a Telephony server that communicates with the Communication Manager switch and software:

If the Telephony server connects to an AE Services computer, the computer that hosts the Telephony Server does not require a secondary NIC. You can use the public network for communication between the Telephony server and the Communication Manager switch and software.

Telephony licensing keys: Telephony licensing keys are written to the registry of the computer that hosts the Telephony server. If you change the IP address of the primary NIC or change the primary NIC on that computer, the licensing will be void and the Telephony server will not function properly.

Firewall guidelines for Avaya Agent

To provide security for the network, Interaction Center assumes that the customer website for Web Management is located in the DMZ of the network, between the following two firewalls:

- Firewall between the website computer and the internal network where the Interaction Center servers are deployed.
- Firewall between the website computer and the internet.

The firewall is a hardware and software component of the network infrastructure. Firewalls can:

- Block certain network traffic in each direction.
- Perform IP address translation in both directions.
- Unexpectedly break connections.

The firewall policy and design have a direct impact on the deployment and performance of Interaction Center components, such as Web Management servers.

DNS domains: In your network, servers outside the firewall may be in a different DNS domain from servers inside the firewall. Typically, DNS domains outside the firewall cannot resolve the names of DNS domains inside the firewall.

Deployment of Interaction Center components outside firewall: Customers require direct access to the Web Management website to search the Web Self-Service database, or initiate chat contacts with agents in your contact center. Customers can also initiate email contacts from the website. To ensure that customers do not have direct access to your network, deploy the website outside the firewall.

Communication through the firewall: Web Management and Email Management components on the website must communicate with components inside the firewall. This communication might require additional configuration of the operating system on computers that host these components. For example, you might need to add IP addresses to the Hosts table of the operating system on each computer.

Network and Firewall requirements for Avaya Agent Web Client

For Avaya Agent Web Application deployments, the agent desktop, HTTP server and application server must be on the same network. The Avaya Agent Web Client does not work across the public internet that might include proxy or network address translation (NAT) devices. Interaction Center 7.3.x does not support network address translation for agent desktops. Remote agent desktops must be connected to the network hosting the application server using a VPN.

If there is a firewall between the agent computers that run Avaya Agent Web Client and the computer that hosts WebConnector, you must open two configurable ports. The two ports are required because Avaya Agent Web Client receives data in real-time rather than by polling. The first port allows incoming HTTP traffic to the server, and the second port permits the server to notify the client of events. If there is a proxy server, Avaya Agent Web Client can use the proxy server, however, the IP address of the Avaya Agent Web Client must be identifiable and reachable from the computer that hosts WebConnector.

Support for NAT and firewalls

Interaction Center 7.3.x does not support access through Network Address Translation (NAT) devices.

For example, Interaction Center 7.3.x does not support:

- Deployment of the ICM server or Web server between a NAT and a firewall.
- Network address translation for agent desktops. Remote agent desktops must be connected to the network hosting the application server through a VPN.
- VoIP chat if the customer has a private IP address with NAT.

Database guidelines

Interaction Center servers and client applications depend upon the databases to access, store, and retrieve vital data, including information about customers, contacts, employees, and configuration. OA uses data stored in the IC Repository database.

This section describes the databases that the components of Interaction Center use and provides some basic guidelines for their implementation and configuration. This section includes the following topics:

- Interaction Center databases on page 46.
- Interaction Center database performance guidelines on page 47.
- Database table limitations on page 48.

Interaction Center databases

The following table shows the databases that Interaction Center uses. An Interaction Center system might not include all of these databases, as some databases are only used by specific components of Interaction Center.

Database	Description
IC Repository	Stores system level information, including the Employee table with agent information. All Interaction Center systems require this database.
CCQ	Stores application level information for Interaction Center agent applications, such as Avaya Agent, Web Management, and Email Management. All Interaction Center systems require this database.
Business Advocate System Store	Stores administration information, such as system parameters, initialization parameters, location of MSMQ queues, location of servers, and the roles of the Resource Manager servers. This database also stores process definition, run time process, and historical data. Each Logical Resource Manager has a dedicated system store. Only Interaction Center systems that include Business Advocate require this database.

Database	Description
Business Advocate Resource Store	Stores operation information, such as qualifiers, service classes, and agent records and the associated capability sets and profiles. All Resource Manager servers share one Resource store. Only Interaction Center systems that include Business Advocate require this database.
Siebel	Stores information for Interaction Center for Siebel. Only Interaction Center systems that include Interaction Center for Siebel require this database.
OA Real-time database	Stores information required by OA. For more information, see OA *Installation and Configuration*. All Interaction Center systems with OA require this database.
OA Historical database	Stores information required by OA. For more information, see OA *Installation and Configuration*. All Interaction Center systems with OA require this database.

Interaction Center database performance guidelines

Interaction Center components access the databases through a connection pool provided by the Data server. The performance of the Interaction Center clients and servers depends on:

- Access to the databases to store and retrieve information.
- Availability of the databases.
- Ability of the databases to process SQL calls effectively from the application software servers and reporting tools.

The following guidelines for your database server result in good performance and reliability:

Dedicated database computer: Host your database on a dedicated computer. This dedicated location ensures that you can tune your database server to maximize database operations, and improves the reliability and performance of the database. A poorly performing database server adversely affects Interaction Center performance.

Data server location: Do not install the Data server on the computer that hosts your database server.

Effect of contact volume on Data server: Determine the contact volume in your contact center when you deploy your Data server. In a high volume contact center, you can deploy secondary Data servers on the same computers as data-intensive Interaction Center servers.

Location of database files: Install the following database files on the computer that hosts the Data server:

- Database client software
- Database networking libraries

Client to connection ratio: Allocate a 10 to 1 client to connection ratio for the Data server.

Database sizing for contact records: Assume that each contact record occupies a minimum of 5 KB to 10-KB of disk space when you size the database.

Database server tuning: Contact your database software vendor for recommendations on tuning a server for a “decision support” type application, with the number of concurrent users and database size appropriate for your application and contact volumes.

Connection pool: Consider the size of the connection pool when you calculate the amount of memory required in megabytes (MBs). For example, to calculate the amount of memory for Oracle databases, multiply the connection pool size by 3.

Database table limitations

The Interaction Center Data servers for SQL Server support a maximum of 255 columns in a select query. Do not create tables with more than 255 columns in SQL Server databases.

Prerequisites for OA Database Directory Structure

The following are the prerequisites for OA database directory structure:

- If user is creating table spaces at the location *c:\oadb_dbs\<dbname>*, then same directory structure must be present on secondary SQL host.
  User has to create *c:\oadb_dbs\<dbname>* directory on secondary SQL host before adding the database *<dbname>* in availability group from the primary SQL host.
- Sync both the logins created for repository and OA database user to secondary node before installing AOA.
  1. In SQL Server Management Studio, connect to Database Engine using the Availability Listener.
  2. Execute attached `SyncLogins.sql` script. This script creates two stored procedures in the master database. The procedures are named as `sp_hexadecimal` and `sp_help_revlogin`.
  3. Execute `EXEC sp_help_revlogin`.
  4. Select the create login commands for the OA and Repository database users.
  5. Perform manual failover. The secondary node becomes a primary node.

6. Execute the commands on the primary node.

Time zone handling

This section describes the ways that different Interaction Center components handle and record dates and times. This section includes the following topics:

- Methods for time zone handling on page 49
- Time zone methods used by Interaction Center components on page 50
- Time zone requirements for Web Scheduled Callback on page 50

Methods for time zone handling

The Interaction Center components can use the following methods to handle and record dates and times:

Host/local: The Interaction Center component records the date and time in the local time zone, as configured on the host computer.

Local: The Interaction Center component records the date and time in the local time zone.

RDBMS: The Interaction Center component records the date and time in the time zone that the Interaction Center databases use.

Translated to UTC: The Interaction Center component records and stores the date and time in the Coordinated Universal Time (UTC) format. However, when Interaction Center displays the date and time of the event or contact to a user, the date and time is translated into the local time zone of the user.

UTC: The Interaction Center component records the date and time in the UTC format.

Time zone methods used by Interaction Center components

The following table shows the ways that each type of Interaction Center component handles time zones:

Origin of time zone	Interaction Center Servers	IC Manager	Agent desktop applications
ADL file	Host/local	Host/local	Host/local
Database	UTC	UTC	UTC
Dates	UTC	Translated to UTC	Translated to UTC

Time zone requirements for Web Scheduled Callback

Web Scheduled Callback is a time-bound feature. For Web Scheduled Callback to work correctly, all Avaya IC servers and the database must be in the same time zone.

Important:
If the time on the computers that host Avaya IC servers and the database is not synchronized, a time lag may occur between the scheduled time for the callback and the exact time that a Web Scheduled Callback request is delivered to an agent.

Interaction Center server guidelines

This section includes the general guidelines you must follow when you plan your Interaction Center system. You must follow the following guidelines when you decide how many of each type of servers the system requires, which computers will host the servers, and where to locate those computers on the network. This section includes the following topics:

- Server naming guidelines on page 51
- Server partitioning guidelines on page 52
- Web License Manager guidelines on page 53
- Co-location of client applications with servers on page 53
- Time synchronization for servers on page 54
- Server failure considerations on page 55

- Interaction Center core server guidelines on page 55
- Voice channel server guidelines on page 60
- Chat channel server guidelines on page 61
- Email channel server guidelines on page 62
- Business Advocate server guidelines on page 63
- Web Scheduled Callback guidelines on page 66

For more information about server failover guidelines and about individual servers, see *IC Administration Guide*.

Server naming guidelines

In some cases, the Workflow server fails to connect with a server that uses the server type as the name of the server. For example, the failure occurs if an ADU server is named "ADU" or a Web Advocate Adaptor server is named "WAA".

To ensure optimal functioning of your Interaction Center system, use the following naming conventions for your Interaction Center servers:

- Always use a unique server name of up to 32 characters long with no spaces.
- Name your Data servers Data_<*databasetype*>_<*domain*>. For example, **Data_Oracle_Default**.
- In a single site environment, name all other servers <*servername*>_<*domainname*>. For example: **ADU_User1**.
- In a multi-site environment, name all other servers <*servername*>_<*sitename*>_<*domainname*>. For example: **ADU_London_User1**.
- Do *not* set the server name to be the same as the server type, or Interaction Center may encounter errors during operation. For example, use **TS_Voice1** as the name of your Telephony server, not just **TS**.

Important:
Do not use the name **localVDU** or **localADU** for EDU or ADU servers. These are used when the servers are taken off-line to prevent communication with other EDU and ADU servers.

Server partitioning guidelines

The correct partitioning of an Interaction Center system is vital to achieve an optimal level of performance and security. Interaction Center servers use two types of partitioning: physical and logical.

This section describes the issues you must consider when you decide how to partition an Interaction Center system. These issues do not stand alone. Consider these issues with all of the other guidelines in this chapter. This section includes the following topics:

- Physical partitioning on page 52
- Logical partitioning on page 52

Physical partitioning

The deployment method of the Interaction Center servers on physical servers in your system defines the physical partitioning of your Interaction Center system. The physical partitioning performs the following functions for Interaction Center:

- Determines the connectivity between servers.
- Defines how hardware and network failures impact the servers.

You can deploy computers that host Interaction Center servers in a single site on one LAN, or across multiple sites on multiple LANs that are interconnected by WANs.

Logical partitioning

The grouping method of the Interaction Center servers in Interaction Center domains defines the logical partitioning of an Interaction Center system. The Interaction Center domains determine the preferred communication paths and how failover functions.

When you set up the domains for an Interaction Center system, you define the following communication paths:

- Between the Interaction Center servers.
- Between the Interaction Center servers and the Interaction Center client applications.

Important:
Each Interaction Center domain should only contain one server of that type. Certain specific circumstances include exceptions to this rule. For example, the Default domain can include one or more ORB server. For more information about the recommended logical partitioning of servers, see Interaction Center single site deployment scenarios on page 79 and Interaction Center multi-site deployment scenarios on page 123.

Use a common naming convention for your domains to ensure that you can easily identify where a component is deployed. In a multi-site deployment, you should use the following naming convention: *<site>_<service>*, where service represents the media channel or function of the servers in the domain. For example, in an Interaction Center system with a site in Boston, you could name a domain for the voice channel: Boston_VoiceA.

For more information about logical partitioning and how to use Interaction Center domains, see *IC Administration Guide*.

Web License Manager guidelines

Note the following guidelines for the Web License Manager when you plan and deploy licensing for Interaction Center. The following guidelines can help to optimize the performance of an Interaction Center system:

Location of Web License Manager: Install at least one Web License Manager at each site.

If you install a WebLM at each site, WAN segmentation should not prevent an Interaction Center server or client from getting the appropriate licenses. In the deployment scenarios with redundancy, the core servers at each site host a WebLM. This configuration only reduces the total number of computers.

For single CPU machines and VMs, co-locating IC License Server with WebLM causes IC License Server to use a lot of CPU cycles. Hence, in such cases, you must deploy WebLM on a separate machine.

Note:

IC 7.3.x does not support segmented licensing.

Co-location of client applications with servers

Do not install agent desktop applications or the Design & Administration Tools on a computer that hosts Interaction Center servers or OA servers.

Installing client applications on servers impacts the amount of available computer resources, such as CPU and memory. This results in decreased performance and scalability of the servers.

You must host agent desktop applications or Design & Administration Tools on computers that do not impact server performance.

Time synchronization for servers

All servers require time synchronization. This requirement ensures that Interaction Center and OA maintain consistent time. If time is not synchronized, your reports may not be consistent. The clocks on all the servers must also be synchronized to track issues in log files.

To achieve time synchronization if you do not have an existing infrastructure, install NTP (Network Time Protocol) software on all computers that host Interaction Center servers and OA servers. You can use a commercial time synchronization application that includes the ability to provide gradual clock corrections over time, such as Windows Time Service. Interaction Center may fail with time-out errors if you change the system clock in large increments, for example, more than two to three seconds per minute.

CAUTION:
Do not use batch scripts that periodically set the time. These scripts and tools are not accurate enough for the OA databases.

The following table describes the time synchronization utilities that you can use for each operating system supported by Interaction Center and OA:

Operating system	Time synchronization utility
Windows	Third-party NTP utility. Avaya has successfully tested Tardis 2000 v1.4 with OA, and the time adjustment increments in milliseconds, as set out below. You can obtain a copy of Tardis shareware from the HC Mingham-Smith website.
Oracle Solaris	Third-party NTP utility. Avaya has successfully tested the Oracle Solaris `ntpd` process.
AIX	Third-party NTP utility. Avaya has successfully tested the AIX `ntpd` process.

Tardis can make major time changes at unpredictable times, instead of gradual adjustments. These major changes can cause some service requests to time out. For example, the ORB server and ORB NT service may not start automatically when you restart the computer.

To avoid this timeout problem with Tardis, set the time adjustment increments in milliseconds, as follows:

1. From the Windows Control Panel, open Tardis.
2. Adjust the following settings:
   - Maximum correction allowed set in a range from the minimum of 50 milliseconds to a maximum of 500 milliseconds.
   - How often the time is set to Every Minute.

For more information, see the Online Help provided with Tardis.

Server failure considerations

Whenever possible, design an Interaction Center system to ensure that the failure of a single server does not impact all agents. Note the following limitations when you design an Interaction Center system:

Process redundancy limitations: Web Management (WebACD) and Email Management support process redundancy. If the Functional WebACD server fails, Avaya IC can route contacts for email and chat media channels with another WebACD server. However, WebACD server does not support multiple redundancies. There can be only two WebACD servers in the entire Avaya IC system. However, you can have multiple email servers in the Avaya IC system.

Interaction Center core server guidelines

Note the following guidelines for the Interaction Center core servers when you plan and deploy those servers. These guidelines can help to optimize the performance of an Interaction Center system.

This section includes the following topics:

- ADU server guidelines on page 55
- Data server guidelines on page 56
- Directory server and Alarm server guidelines on page 56
- ORB server guidelines on page 57
- Notification server guidelines on page 57
- Report server guidelines on page 58
- Workflow server guidelines on page 58

ADU server guidelines

ADU servers support Interaction Center accounts for agents and administrators. Consider the following guidelines when you plan the deployment of ADU servers:

ADU server limitations: An ADU server can handle events from approximately 500 agents. Include a minimum of two ADU servers at each site.

ADU server failover: Do not configure agent domains to failover to an ADU server that is:

- Not monitored by an Event Collector server at the same site

- Monitored by an Event Collector server at a different site

ADU persistence: If the Interaction Center system requires ADU persistence, follow the guidelines for EDU persistence in EDU server guidelines on page 56.

Data server guidelines

Note the following guidelines when you determine where to locate the Data servers in an Interaction Center system:

Data server location: Do not install the Data server on the computer that hosts your database server.

Network location for Data server: Locate computers that host a Data server topologically close to the computer that hosts the Interaction Center databases on a high-speed backbone. Interaction Center generates the bulk of database access traffic between the Data servers and the database server. This configuration minimizes network bandwidth.

Data server and DUStore server location: When on the same LAN as the database, install a Data server on every computer that hosts a DUStore server. Configure the DUStore server to use this Data server. Also host a backup Data server on another computer. This configuration minimizes network traffic and minimizes failure modes.

Data server and Report server location: When on the same LAN as the database, install a Data server on every computer that hosts a Report server. Configure the Report server to use this Data server. Also, host a backup Data server on another computer. This configuration minimizes network traffic and minimizes failure modes.

For more information about databases and the Data servers, see Database guidelines on page 46.

Directory server and Alarm server guidelines

In a multi-site deployment, when Interaction Center is deployed across a WAN, install a Directory server and Alarm server on every LAN.

These servers are critical for the operation of the other Interaction Center servers. If you have a Directory server and Alarm server on every LAN, a site can still function even if the WAN goes down.

EDU server guidelines

Note the following guidelines when you set up an EDU server for an Interaction Center system:

Multiple EDU servers: Install a separate EDU server for every media channel domain. Different media channels have different requirements for configuring the EDU server to ensure optimal processing.

Email EDU server configuration: Configure the EDU server that processes email contacts as described in the following table:

Configuration parameter	Description
Enable EDU persistence	EDU persistence writes EDU information to the DUStore server based on the checkpoint interval setting and limits the EDU Server memory usage. If there is a failure in your system, Interaction Center can then reconstruct the emails in queue.
Checkpoint every five minutes	The Checkpoint feature ensures that Interaction Center persists changes to an EDU at the end of the checkpoint interval. This setting also minimizes the number of email EDUs in a queue that are lost if the EDU server fails.

EDU limitations: The EDU has a limitation if the contact center includes some Interaction Center agents and some agents who do not work in Interaction Center. Interaction Center cannot track an EDU outside the Interaction Center system.

For example, if an Interaction Center agent transfers a contact out of Interaction Center to a non-Interaction Center agent, then Interaction Center terminates the EDU for that contact. Interaction Center considers the contact to be retired. If an agent transfers the contact back to an Interaction Center agent, Interaction Center assigns a second EDU to the contact.

As a result, the same contact has two EDUs. This limitation can create problems with tracking and reporting for that contact.

ORB server guidelines

All computers that host Interaction Center servers require an ORB server. If a computer does not include an ORB server, you cannot start Interaction Center servers on that computer.

You must install an ORB server:

- On every computer that hosts Interaction Center servers except the ICM server and CIRS server.
- For every network interface on a multi-homed computer with which an Interaction Center server needs to communicate.

For guidelines on how to install and configure Interaction Center on a computer with multiple network cards, see Multiple network interface cards on page 43.

Notification server guidelines

Ensure that the Notification server has access to an SMTP email server to send alert messages.

Report server guidelines

Location of Report servers: Install a Report server on every computer that hosts an EDU server. This configuration minimizes failure modes and network traffic.

Report servers, Data servers, and Workflow servers: The Report server is a heavy user of the Data server. Ensure that the Report servers in the Interaction Center system do not share a Data server with a Workflow server that performs routing.

Workflow server guidelines

Consider the following guidelines when you set up a Workflow server for an Interaction Center system:

Location of Workflow servers: To mitigate the impact of a failure due to customized workflows, keep Workflow servers logically separate. For example, create a Workflow server for each media and host those servers with other servers that are specific to the same media.

Customization of workflows: Workflow servers typically have many external interfaces, such as interfaces to the database and Prompter. Because the Workflow server is scriptable and extensible, Avaya cannot test all possible customizations and usages as part of the out-of-the-box product.

Customized workflows can be less reliable than the sample workflows and can impact the performance of other servers. Thoroughly test all customized workflows, including possible failure scenarios.

Load partitioning: Deploy several Workflow servers to provide general load partitioning for contacts, and to limit the types of workflows run by each Workflow server. If you limit the types of workflows, you minimize the possibility that a workflow may impact the performance of other Interaction Center system functions.

Your Interaction Center system should include separate Workflow servers for the following:

- Each Blender server in your Interaction Center system
- Each media channel in your Interaction Center system
- Each agent workgroup that uses Prompter
- Other utility functions run by the Workflow server, such as periodic tasks

You can configure a Workflow server for each computer that hosts media-specific servers. For example, create a Workflow server for each computer that hosts a Telephony server.

Coupling between Blender server, Workflow server, and ADU server: A tight coupling between the Blender server, Workflow server, and ADU server is critical for agent login and for agent channel assignment.

If you install redundant servers, or the contact center requires higher availability of agents, include the following in your deployment:

- Install at least two sets of Blender server, Workflow server, and ADU server on every LAN in the Interaction Center system that includes agent desktop applications.
- Configure each set of servers to failover to the other set of servers.

Split the agent population on the LAN between the two sets of servers. Each agent group should use one set of servers and use the second set as a backup. This set of servers is critical for agent login and agent channel assignment. If you split your agents across two sets of servers, a single server (or computer) failure cannot disable your contact center. One group of agents can continue uninterrupted operation while the other group restores connections through failover.

Note:

Some deployments do not include an ADU server in a user domain. Those deployments include the Blender server and Workflow server in the user domain, and the ADU server in a media domain. Those deployments also ensure that the failover is configured correctly for the user domains and the failover domains. For more information about how to configure the failover, see Interaction Center single site deployment scenarios on page 79 and Interaction Center multi-site deployment scenarios on page 123.

Workflow server and Business Advocate: Configure at least one Workflow server on the same computer as every Telephony Services Adaptor server and Web Advocate Adaptor server. This Workflow server handles the qualification and exceptions of all the contacts for that server. If the Telephony Services Adaptor server or Web Advocate Adaptor server handles a high volume of contacts, assign multiple Workflow servers to that server. The Telephony Services Adaptor server or Web Advocate Adaptor server can distribute contacts evenly between the assigned Workflow servers.

Workflow server and email qualification: To improve email processing throughput, run email qualification workflows on a different Workflow server than the email analysis workflows. Email analysis should always occur on a dedicated computer in the Email domain.

Depending upon the volume of incoming email contacts, email qualification can occur on:

- The same Workflow server as chat qualification for a contact center with a low to medium volume of email and chat contacts.
- A dedicated Workflow server for a contact center with a medium to high volume of email and chat contacts.

Voice channel server guidelines

Consider the following guidelines for the Interaction Center servers that are specific to the voice channel when you plan and deploy those servers. These guidelines can help to optimize the performance of an Interaction Center system.

This section includes the following topics:

- Telephony server guidelines on page 60
- Telephony Queue Statistics server guidelines on page 60
- DUStore server for voice guidelines on page 61

Telephony server guidelines

For optimal network performance locate your Telephony server in the same LAN as the associated telephony switch (Avaya Aura® Communication Manager) and AES. This location provides Interaction Center telephony services with high-speed access to telephony devices, such as telephony switches or IVRs.

Telephony Queue Statistics server guidelines

Consider the following guidelines when you plan the deployment of Telephony Queue Statistics (TSQS) servers:

Potential queue limitations: If there are more than 500 queues defined on the system, the TSQS server may timeout in a failover situation.

Configuration requirements for multiple TSQS servers: Do not configure more than one TSQS server with the same Site and ACD Name. If you configure redundant TSQS servers with the same Site and ACD name, both servers attempt to create and update the ADU for the queue. This simultaneous update can result in:

- Incorrect and duplicate data in OA reports
- Problems with creation of multiple ADUs
- Failure of both TSQS servers

Backup TSQS servers: If the Interaction Center system requires a backup TSQS server, configure:

- The backup TSQS server NOT to start automatically
- The backup Telephony server for the queue as the first server in the TS Set list for the Voice Device in IC Manager

DUStore server for voice guidelines

If you enable EDU persistence in the EDU server that handles voice contacts, the DUStore server must be in the same domain as the EDU server for voice contacts. If the DUStore server and EDU server are not in the same domain, the Interaction Center system cannot route voice contacts properly.

Chat channel server guidelines

Consider the following guidelines for the Interaction Center servers that are specific to the chat channel when you plan and deploy those servers. These guidelines can help to optimize the performance of an Interaction Center system.

This section includes the following topics:

- Attribute server guidelines on page 61
- DUStore server for chat guidelines on page 61
- ICM server and CIRS server guidelines on page 62
- Web Management servers guidelines on page 62

Attribute server guidelines

Install an Attribute server in the DMZ on the computer that hosts your Interaction Center website if your Interaction Center system records DataWake information. You must also configure ICMBridge for Attribute server.

An Attribute server inside the firewall can record DataWake information. However, if you install an Attribute server on the website computer, you can reduce network traffic across the firewall.

DUStore server for chat guidelines

If you enable EDU persistence in the EDU server that handles chat contacts, the DUStore server must be in the same domain as the EDU server for chat contacts. If the DUStore server and EDU server are not in the same domain, the Interaction Center system cannot properly route chat contacts.

ICM server and CIRS server guidelines

If you expect a high volume of customer interaction and chat contacts on the Web Management website, you can add more than one ICM server to increase the number of supported chat contacts and permit greater scalability.

If the Interaction Center system includes more than one ICM server:

- Configure a CIRS server to provide load balancing for the ICM servers.
- Host each ICM server on a separate computer.

Web Management servers guidelines

Provide Web Management servers with high-speed access to Web and email servers.

Email channel server guidelines

Consider the following guidelines for the Interaction Center servers that are specific to the email channel when you plan and deploy those servers. These guidelines can help to optimize the performance of an Interaction Center system.

This section includes the following topics:

- IC Email/Poller server guidelines on page 62
- DUStore server for email guidelines on page 62
- Email EDU server guidelines on page 63

IC Email/Poller server guidelines

Provide the IC Email/Poller servers with high-speed access to external email server such as Microsoft Exchange or Lotus Domino server implementing SMTP protocol for outbound emails and POP3 / IMAP4 for inbound emails. Email server uses SMTP for outbound emails whereas poller server uses POP3/IMAP4 for downloading inbound emails. Poller server can also connect to POP3/IMAP4 compliant servers over SSL.

DUStore server for email guidelines

Include the following in the deployment of any Interaction Center system that includes the email channel to minimize network traffic, provide load balancing, and minimize failure modes:

- Configure a secondary DUStore server for the email EDU server only
- Locate the secondary DUStore server on the same computer as the email EDU server
- Configure the email EDU server to use this DUStore server

- In case of a failure of the DUStore server, install and configure a backup DUStore server

Email EDU server guidelines

Verify that the persistence parameter is set to "on" for the email EDU server.

Business Advocate server guidelines

This section includes general guidelines to consider when you plan an Interaction Center system that includes Business Advocate. Consider these guidelines when you decide how many of each type of server the system requires, which computers host the servers, and where to locate those computers on the network.

This section includes the following topics:

- Logical Resource Manager guidelines on page 63
- Resource Manager server guidelines on page 64
- Business Advocate databases guidelines on page 64
- Telephony Services Adaptor server guidelines on page 64
- Web Advocate Adaptor server guidelines on page 65
- Workflows for Business Advocate guidelines on page 66

For more information about guidelines that affect Business Advocate, see Event Collector Bridge guidelines on page 75.

Logical Resource Manager guidelines

Consider the following guidelines for each Logical Resource Manager in an Interaction Center system:

ADU server location: Install a dedicated ADU server for each Logical Resource Manager. Host this ADU server on the same computer as the Resource Manager server for the Logical Resource Manager.

This ADU server keeps the Business Advocate statistics for that Logical Resource Manager. Create a redundant ADU server in case of ADU failure.

ADU server domain: Create a separate Interaction Center domain for this ADU server. Do not place this ADU server in the same domain as the Resource Manager servers in the Logical Resource Manager.

Resource Manager server guidelines

Consider the following guidelines for each Resource Manager server in an Interaction Center system:

Resource Manager server domain: Create a separate domain for each Resource Manager server in a Logical Resource Manager. Do not include more than one Resource Manager server in an Interaction Center domain.

Operating system: The Resource Manager server requires a Windows Server operating system. You can host other Interaction Center servers on supported Oracle Solaris or AIX operating systems.

Resource Manager location: Host each Resource Manager server, whether primary or standby, on a separate Windows Server. Do not host more than one Resource Manager server on the same computer.

Resource Manager failover: Resource Manager servers support working in pairs, with one active Resource Manager server and one standby Resource Manager server. The standby Resource Manager server becomes the active Resource Manager server if the active server fails. Configure a standby Resource Manager server for a high availability deployment.

Business Advocate databases guidelines

For an Interaction Center system that uses DB2 for Interaction Center databases, install an Oracle database or SQL Server database to host the Business Advocate database stores.

Telephony Services Adaptor server guidelines

Consider the following guidelines for each Telephony Services Adaptor server in an Interaction Center system:

Telephony Services Adaptor server and Telephony server: Business Advocate requires a tight coupling between the Telephony Services Adaptor server and the Telephony server. These two servers handle voice contacts from a single CTI link on a switch.

Host the Telephony Services Adaptor server on the same computer as the associated Telephony Server. Include both these servers in the same Interaction Center domain.

For redundancy, host pairs of Telephony Services Adaptor server and Telephony server on two separate computers. The total number of agents on both pairs must not exceed the maximum number of agents supported for one CTI link.

Telephony Services Adaptor server and ADU server: A Telephony Services Adaptor server always uses the same ADU server as the Telephony server.

Telephony Services Adaptor server and CTI link: Install a Telephony Services Adaptor server for each CTI link that processes incoming voice contacts. All incoming voice contacts to be routed by Business Advocate require a Telephony Services Adaptor server.

Telephony Services Adaptor server and switch: Install at least one pair of Telephony Services Adaptor server and Telephony server per switch. Each switch must have at least one CTI link controlled by a Telephony Services Adaptor server and Telephony server pair. Even if the switch does not accept incoming voice contacts, a Telephony Services Adaptor server and Telephony server pair is required to transfer voice contacts.

Telephony Server Adaptor server and failover: The Telephony Server Adaptor server does not use the domain mechanism for failover. If the Telephony server or the Telephony Server Adaptor server fails, voice contact routing in Business Advocate fails over to one of the following:

- A backup pair of Telephony server and Telephony Server Adaptor server
- The switch

Web Advocate Adaptor server guidelines

Consider the following guidelines for each Web Advocate Adaptor server in an Interaction Center system:

Web Advocate Adaptor server and WebACD server: Business Advocate requires a tight coupling between the Web Advocate Adaptor server and functional WebACD server. These two servers handle all chat contacts and email contacts in an Interaction Center system.

Install Web ADU servers on same physical network as that of WAA server to avoid network glitch issues across WANs.

Web Advocate Adaptor server location: Install a Web Advocate Adaptor server on any computer that has WebACD server, as WebACD is redundant. Include both these servers in the same Interaction Center domain.

Note:

It is recommended to have redundant WACD servers on the same physical network.
VMware's Fault Tolerance feature is used to achieve High Availability for Web Advocate Adapter server. Hence, the Web Advocate Adaptor server deployed on Fault Tolerance enabled VM machines ensure uninterrupted operation.

Workflows for Business Advocate guidelines

Consider the following guidelines for each Workflow server that runs Business Advocate workflows in an Interaction Center system:

Qualification workflows and exception workflows: Run Business Advocate qualification workflows and exception workflows on the same dedicated Workflow server.

Voice qualification workflows: Configure at least one Workflow server for every Telephony Services Adaptor server in a LAN. Depending on the volume of voice contacts, multiple Workflow servers can run voice qualification workflows for a single Telephony Services Adaptor server.

Web Scheduled Callback guidelines

Consider the following guidelines if your Interaction Center system includes Web Scheduled Callback:

Supported agent desktop applications: Web Scheduled Callback is supported on Avaya Agent, Avaya Agent Web Client and custom application developed with the Client SDK.

Time zone requirements for Web Scheduled Callback: Web Scheduled Callback is a time-bound feature. For Web Scheduled Callback to work correctly, all Interaction Center servers and the database must be in the same time zone.

Important:
If the time on the computers that host the Interaction Center servers and the database is not synchronized, a time lag may occur between the scheduled time for the callback and the exact time that a Web Scheduled Callback request is delivered to an agent.

Calendar requirements for Web Scheduled Callback: Web Scheduled Callback requires the Gregorian calendar. Web Scheduled Callback does not work with any other calendar. For example, Web Scheduled Callback does not support the Thai B. E. (Buddhist Era) calendar or date format.

Port utilization

For complete port matrix information for Interaction Center, see Interaction Center Port Matrix at the Avaya Support website: http://support.avaya.com/security

For complete port matrix information for Operational Analyst, see Operational Analyst Port Matrix at the Avaya Support website: http://support.avaya.com/security

Ephemeral ports in Interaction Center and OA

A TCP/IPv4 connection consists of two endpoints. Each endpoint includes an IP address and a port number. When a client user connects to a server, an established connection is the combination of server IP, server port, client IP, and client port. Usually, the following three required:

- Client IP
- Server IP
- Server port number

When a connection is established, the client-side of the connection uses a port number. Unless a client program explicitly requests a specific port, the client port is an ephemeral port number.

Ephemeral ports are temporary ports assigned by the IP stack of a computer. The IP stack assigns ephemeral ports from a range of ports that is designated for this purpose. When the connection ends, the ephemeral port is available for reuse. However, most IP stacks will not reuse a port number until after the entire pool of ephemeral ports has been used. If the client program reconnects, the IP stack assigns a different ephemeral port number the client side of the new connection.

This section includes the following topics:

- Limits implied by the ephemeral port range on page 67
- Traditional configuration of the ephemeral port range on page 68
- Firewalling the ephemeral port range on page 68
- Changing the ephemeral port range on page 69

Limits implied by the ephemeral port range

The ephemeral port range limits the maximum number of connections from one computer to a specific service on a remote computer. The TCP/IP protocol uses the combination of server IP, server port, client IP, and client port to distinguish between connections. Therefore, if the ephemeral port range is only 4000 ports wide, a client computer can have only 4000 unique, simultaneous connections to a remote service.

A TCP connection must expire through the TIME_WAIT state before the connection is completed. For example, even if both sides of a connection properly close their ends of the connection, due to the error control for TCP, each side must wait until the TIME_WAIT state is expired before the disposing of the connection resources. The TIME_WAIT state is twice the maximum segment lifetime (MSL) which is usually configured at 240 seconds. This configuration means that a client computer can have only 4000 connections per 240 second window.

Traditional configuration of the ephemeral port range

The BSD Sockets TCP/IP stack uses ports 1024 through 4999 as ephemeral ports. Additionally, ports 1 through 1023 are reserved ports, used for systems services that run as the superuser.

The ephemeral port range for the BSD stack has a relatively small size of 3975 ports with a low numbered position. The current preferred default range is 49152 through 65535, which has a much larger size of 16383 ports and is at the top of the full port range.

Firewalling the ephemeral port range

For firewalls, administrators often restrict access to the maximum number of ports. Inbound connections to ephemeral ports can require administrators to open an entire range of ports. When a range of ports is opened on the firewall, no system services listen on ports in the open range.

Administrators can open a specific range on the firewall. Then for each computer on the internal network, administrators can ensure that the ephemeral port range on the computer coincides with the open range on the firewall.

The ephemeral port ranges on computers on the internal network often do not coincide with each other since different operating systems may use different ranges. The process to manually configure the ephemeral port range for individual computers to coincide with the open range on the firewall can be time-consuming. As a result, administrators adopt a policy of allowing all incoming ports and denying access to specific ports when needed.

You may not need to open the ephemeral port range on all computers. The ephemeral port range is usually only required when:

- The application serves FTP to the outside world. Passive PASV data connections use inbound ephemeral ports.
- An FTP client access must work in non-passive mode. PORT connections from the server use ephemeral ports when inbound to clients.

Changing the ephemeral port range

You must change the ephemeral port range to 49152 through 65535. If you need a larger range, you can have a value lesser than 49152, but the higher value must remain 65535. You should change the ephemeral port range for the following reasons:

- To use a larger range so that more simultaneous connections are possible.
- To shift the range to the higher numbered ports. The higher numbered ports should be used as ephemeral ports because they are less likely to be used as port numbers for system services. Well-known service ports have traditionally been assigned to lower port numbers.
- To change the range to coincide with other systems for purposes of firewalling and automatic network address translation.

The following sections describe how to change the ephemeral port range on the supported operating systems:

- Changing the port range for Microsoft Windows on page 69
- Changing the port range for Oracle Solaris on page 70
- Changing the port range for IBM AIX on page 72

Some systems already use the preferred range and do not need to be changed. Some operating systems also use two or more ranges.

Changing the port range for Microsoft Windows

Windows uses the traditional BSD range of 1024 through 4999 for its ephemeral port range. You can only set the upper bound of the ephemeral port range.

For more information about how to set the upper boundary of the ephemeral port, see Microsoft Knowledge base Article Q196271 on the Microsoft website.

Changing the port range for Oracle Solaris

Oracle Solaris uses the **ndd** utility program to change tunable IP stack parameters. The ephemeral ports on Oracle Solaris can be tuned individually for both TCP and UDP, so there are really two separate ephemeral port ranges. Oracle Solaris also provides options to change the privileged port range (ports only processes running with superuser privileges can use).

Oracle Solaris, by default, provides a large range at the end of the port range (32768 through 65535, or the upper 50%) so you are unlikely to need to change the range from the default values.

Important:
Use the default range. If you change the range values, you must do it each time the system starts up.

The example below shows how to query the existing range for the TCP ephemeral ports and change the range to 49152 through 61000:

1. Enter:

   ```
   /usr/sbin/ndd /dev/tcp tcp_smallest_anon_port
     tcp_largest_anon_port
   ```

   The current range (by default, 32768 to 65535) is displayed.

2. Enter the following commands to change the ephemeral port range to 49152 through 61000:

   ```
   /usr/sbin/ndd -set /dev/tcp tcp_smallest_anon_port 49152
   ```

   ```
   /usr/sbin/ndd -set /dev/tcp tcp_largest_anon_port 61000
   ```

3. Enter the following command to display the new range:

   ```
   /usr/sbin/ndd /dev/tcp tcp_smallest_anon_port
     tcp_largest_anon_port
   ```

   The new range, 49152 through 61000, is displayed.

For more information about tuning Oracle Solaris, see the *Oracle Solaris Tunable Parameters Reference Manual*.

The following is a sample script you can use to change the range at startup:

```
#!/sbin/sh
#
# Copy me to /etc/init.d/ephemports, then do
# "ln -s /etc/init.d/ephemports /etc/rc2.d/S70ephemports".
#
EPHEM_HI="65535"
EPHEM_LO="49152"

if [ "$#" -eq 0 ] ; then arg="start" ; else arg="$1" ; fi
case "$arg" in
'start')
  ;; # Fall through -- rest of script is the initialization code

'stop')
  exit 0
  ;;

'status')
  EPHEM_HI=`/usr/sbin/ndd /dev/udp udp_largest_anon_port`
  EPHEM_LO=`/usr/sbin/ndd /dev/udp udp_smallest_anon_port`
  echo "UDP ephemeral port range is ${EPHEM_LO}..${EPHEM_HI}."
  EPHEM_HI=`/usr/sbin/ndd /dev/tcp tcp_largest_anon_port`
  EPHEM_LO=`/usr/sbin/ndd /dev/tcp tcp_smallest_anon_port`
  echo "TCP ephemeral port range is ${EPHEM_LO}..${EPHEM_HI}."
  exit 0
  ;;

*)
  echo "Usage: $0 { start | stop | status }"
  exit 1
  ;;
esac

/usr/sbin/ndd -set /dev/udp udp_smallest_anon_port "${EPHEM_LO}"
/usr/sbin/ndd -set /dev/udp udp_largest_anon_port "${EPHEM_HI}"
/usr/sbin/ndd -set /dev/tcp tcp_smallest_anon_port "${EPHEM_LO}"
/usr/sbin/ndd -set /dev/tcp tcp_largest_anon_port "${EPHEM_HI}"

EPHEM_HI=`/usr/sbin/ndd /dev/udp udp_largest_anon_port`
EPHEM_LO=`/usr/sbin/ndd /dev/udp udp_smallest_anon_port`
echo "UDP ephemeral port range is ${EPHEM_LO}..${EPHEM_HI}."
EPHEM_HI=`/usr/sbin/ndd /dev/tcp tcp_largest_anon_port`
EPHEM_LO=`/usr/sbin/ndd /dev/tcp tcp_smallest_anon_port`
echo "TCP ephemeral port range is ${EPHEM_LO}..${EPHEM_HI}."

exit 0
```

Changing the port range for IBM AIX

AIX uses the **no** command to set network options. AIX uses two separate ephemeral port ranges, one each for TCP and UDP. Both ranges default to the values 32768 through 65535.

To display the current port range, enter:

```
/usr/sbin/no -a | fgrep ephemeral
```

The port range is displayed:

```
tcp_ephemeral_low = 32768
tcp_ephemeral_high = 65535
udp_ephemeral_low = 32768
udp_ephemeral_high = 65535
```

Important:
Use the default range. If you change the range values, you must do it each time the system starts up.

If necessary, you can change the default range with the **no** command.

For example, to set the TCP ephemeral port range to 49152 through 65535, enter:

```
/usr/sbin/no -o tcp_ephemeral_low=49152 -o
  tcp_ephemeral_high=65535
```

You can set the options with **no** each time the system starts up by editing **/etc/rc.tcpip** and inserting the **no** commands just before the script starts to run the server daemons.

OA server guidelines

The Event Collector server is the OA server that acts as a bridge between the ADU server in Interaction Center and the real-time subsystem in OA. The Event Collector server collects ADU data from the ADU server and delivers the data to the real-time subsystem.

In addition to the guidelines in the previous sections, consider the guidelines in this section when you deploy OA with your Interaction Center system.

This section includes the following topics:

- Event Collector server guidelines on page 73
- Event Collector Bridge guidelines on page 75
- Event Collector server failover guidelines on page 76

Event Collector server guidelines

This section describes the guidelines to follow when you deploy the OA Event Collector server and Real-time subsystem in an Interaction Center system. This section includes the following topics:

- Location of Event Collector server on page 73
- Event Collector server and Interaction Center domains on page 73
- Event Collector server and Interaction Center sites on page 73
- Event Collector server and ADU servers on page 74
- Event Collector server and Telephony on page 74
- Event Collector server and Business Advocate on page 74
- Limitations on ADU data collection on page 74

Location of Event Collector server

Install the Event Collector on a computer with the following:

- OA real-time subsystem
- Interaction Center secondary ORB server

For a single site, you can install all OA components on the same computer if the event traffic does not exceed the capacity of the computer.

Event Collector server and Interaction Center domains

Create a dedicated domain for the Event Collector server.

The Event Collector server does not need to be in the same domain as an ADU server.

Event Collector server and Interaction Center sites

Install and configure an Event Collector server and OA real-time subsystem for each Interaction Center site where an ADU server monitors agents. This Event Collector server must monitor all agent ADU servers at that site.

Event Collector server and ADU servers

The Event Collector server must monitor all ADU servers in an Interaction Center system.

Install the Event Collector server as follows:

- Install the Event Collector server with the OA real-time subsystem and a secondary ORB server.
- Do not install the Event Collector server on the same computer as an ADU server.

Event Collector server and Telephony

Ensure that the site administered for the Event Collector server matches the site administered for the Telephony servers in use at the site.

The Event Collector server does not receive voice queue ADU events from Telephony servers that are configured for different sites. The Event Collector server expects to receive Queue ADU data from all email and Web ADU servers across all sites. These ADU events are delivered via proxy through the local ADU server. However, voice ADU events are treated differently. These events are also delivered by proxy, but they are filtered based on the site specified in the Event Collector administration when you create and configure the Event Collector server.

Event Collector server and Business Advocate

For Interaction Center systems with Business Advocate, the Event Collector server must monitor the following Interaction Center domains:

- The Voice domain that contains an ADU server where the TSQS and TSA servers record queue and service class detail records. This ADU server is typically in the same domain as the Telephony server, or in a domain that fails over from the domain of the Telephony server.
- The Web domain that contains an ADU server where the WACD and WAA servers record queue and service class detail records. This ADU server is typically in the same domain as the WebACD server, or in a domain that fails over from the domain of the WebACD server.
- The User or Agent domains where agents are assigned for each site.

Limitations on ADU data collection

Limit ADU data collection from an Event Collector server to local site ADU servers and the proxying of remote ADU data through the local site ADU servers.

This configuration assumes that the local domain ADU handles agent data, and that the proxy data consists of queue statistics for the local site. Do not proxy agent ADU data, because this creates a proxy overhead of large agent ADU volumes. Collect agent ADU data directly from the Agent ADU server on the same physical system.

Event Collector Bridge guidelines

In an Interaction Center system, the Event Collector Bridge queries Business Advocate for administrative information and processes all administration-related events.

This section describes the guidelines to follow when you deploy an Event Collector Bridge. This section includes the following topics:

- Minimum deployment on page 75
- Event Collector Bridge and Resource Manager server on page 75

Minimum deployment

Install a minimum of two Event Collector Bridges in an Interaction Center system. One Event Collector Bridge will serve as the primary. The second Event Collector Bridge will serve as a standby or backup.

Event Collector Bridge and Resource Manager server

Install multiple Event Collector Bridges on each computer that hosts a Resource Manager server.

The Event Collector Bridge requires access to the same Windows Message Queuing service (MSMQ) as the Resource Manager server. Multiple Event Collector Bridges can compete for access to the MSMQ, but only one can use MSMQ.

This deployment provides redundancy and helps to ensure availability if an Event Collector Bridge fails.

Tip:
The deployment scenarios show only one Event Collector Bridge per Resource Manager server. However, redundancy requires a minimum of two Event Collector Bridges for each Resource Manager server.

Event Collector server failover guidelines

The following configuration guidelines for failover minimize the potential loss of data if an ADU server fails. If you follow these guidelines and an ADU server fails, each agent who logged in through that ADU server fails over to another ADU server in the failover configuration. Because both ADU servers are monitored by the same Event Collector server, OA records the agent data correctly.

Consider the following when you configure failover for the Event Collector server and ADU servers in your Interaction Center system:

Failover for Event Collector server: You cannot configure failover for an individual Event Collector server with its Real-time subsystem. The Event Collector servers must monitor all agent domains in the failover configuration.

Failover for ADU servers in agent domains: Ensure that an ADU server never fails over to an ADU server that is not monitored by an Event Collector server.

Normal failover paths may result in an agent ADU entry being created in the ADU server that the Telephony server and WebACD server use for queue ADU entries. This “channel ADU server” is not monitored by an Event Collector. Therefore, OA cannot report on the failed-over agents. Use the “Server Groups” feature of the channel ADU servers to ensure that no requests from agent domains are resolved to this server.

Failover for ADU servers in agent domains across multiple sites: Do not configure ADU servers to failover to an ADU server at another site, unless both sites are monitored by a single Event Collector server.

OA reporting problems caused by incorrect server deployment

If you do not follow the guidelines for deploying and configuring the Event Collector server and ADU servers, your OA reports may miss data or contain incorrect data.

This section includes the following topics:

- Agent fails over to an ADU server that is monitored by a different Event Collector server on page 77
- An agent fails over to an ADU server that is not monitored by an Event Collector server on page 77
- Two Event Collector servers monitor the same agent domains on page 77

For more information about OA server guidelines, see OA server guidelines on page 72, and OA *Installation and Configuration*.

Agent fails over to an ADU server

The following are the scenarios in which an Agent fails over to an ADU server:

- Agent fails over to an ADU server that is monitored by a different Event Collector server
- An agent fails over to an ADU server that is not monitored by an Event Collector server

Agent fails over to an ADU server that is monitored by a different Event Collector server

Agent fails over to an ADU server that is monitored by a different Event Collector server. For a brief period, the agent may appear to be logged in on both real-time sources simultaneously. OA will track contacts in progress at the time of failover incorrectly. However, subsequent contacts are tracked correctly. Historical data for the agent are associated with multiple sources.

This configuration is not recommended for the following reasons:

- Some data anomalies occur during the interval when the failover occurred. For example, an agent's data is spread between two real-time databases. Certain data about the contact in progress are lost.
- Historical report users encounter difficulty monitoring specific agents. To improve the performance of reports, the historical data is summarized into daily, weekly, and monthly summaries using containers. To correctly track the agent, you must add an entry for the agent to the container for each real-time database that contains data for the agent. Unfortunately, you cannot add these entries until after the failover has occurred.

An agent fails over to an ADU server that is not monitored by an Event Collector server

OA does not collect data for that agent after the failover. The agent will appear to be logged out.

Two Event Collector servers monitor the same agent domains

OA does not currently support this configuration.

If you configure two Event Collector servers to monitor the same agent domains, your OA system includes two real-time databases with the same real-time data.

Although this could provide some redundancy to your system and ensure that if one Event Collector server or Real-time subsystem fails, the other continues to collect data. However, you encounter the following problems if you use this configuration:

- The real-time reports do not support duplicate real-time data in multiple real-time databases. Report users need to be aware of the redundant databases and choose an appropriate source to monitor.
- If an Event Collector server fails, OA does not provide a failure indication to real-time report users. Report users see stale, unchanging data and do not receive an indication that the user needs to switch to another source.
- After an Event Collector server recovers, interval data is incomplete and do not match the other real-time database. No mechanism is available to resynchronize the databases.
- Historical data is duplicated across sources, doubling the amount of database space required to store Interaction Center summary data. Historical data during intervals when an Event Collector failed do not match between the sources.
- Historical reports may show misleading data if containers are administered that contain data from multiple duplicated sources. Data items that contain counts are double counted, and data collected during intervals when an Event Collector server failed may be difficult to interpret.

Chapter 4: Interaction Center single site deployment scenarios

This section includes scenarios of sample deployments for an Interaction Center system on a single site.

This section includes the following topics:

- Adapting deployment scenarios on page 79
- Items not shown in the deployment scenarios on page 82
- Scenario 1: Single site, voice only on page 82
- Scenario 2: Business Advocate for single site, voice only on page 88
- Scenario 3: Business Advocate for single site, high volume voice on page 92
- Scenario 4: Single site, multi-channel on page 96
- Scenario 5: Single site, multi-channel with high volume voice on page 104
- Scenario 6: Business Advocate for single site, multi-channel on page 112
- Scenario 7: Single site, chat and email only on page 117

For information about an Interaction Center integration with Siebel, see *Avaya IC for Siebel Integration* guide.

Adapting deployment scenarios

These scenarios estimate an average system load for a site with fewer than 1,200 agents. If your plan includes an Interaction Center site with a high system load, or more than 1,200 agents, you must adapt the deployment scenario. You can also adapt the recommended deployment scenarios to meet the specific needs of a contact center.

This section includes the following topics:

- Adding more servers and domains on page 80
- Adding more Tomcat servers for the Client SDK or Web Services on page 80
- Including additional servers in a deployment on page 80
- Co-locating servers on one computer on page 81
- Deploying servers on multi-processor computers on page 81

Adding more servers and domains

These deployment scenarios show the recommended number of computers, servers, and domains. If you expect an extremely high volume of contacts or a high volume of database lookups, you can adjust the scenario to include additional servers and domains.

For example, if the Interaction Center system has a high volume of database searches and lookups, host an extra Data server on each computer and place those Data servers in dedicated domains. For an example of how to deploy a "Data" domain and configure the failover for that domain and the other domains in the system, see Scenario 1: Single site, voice only on page 82.

Adding more Tomcat servers for the Client SDK or Web Services

These deployment scenarios include three Tomcat servers for every two user domains. You can increase the number of Tomcat servers to meet the failover and scalability requirements of a contact center.

Including additional servers in a deployment

You can add more servers in any of these deployment scenarios. These additional computers can:

- Improve throughput and system load capacity.
- Add physical redundancy and failover capacity in the event that a server fails.

For example, you can add servers to improve the throughput and system load capacity for Telephony. The increased number of servers can support an increased agent population or increased contact rate. These additional servers will be dedicated to servers in the same domain that serve a single purpose, such as:

- Computers dedicated to servers that support inbound routing, including a Telephony server, TSQS server, EDU server, ADU server, Report server, and Workflow server.
- Computers dedicated to servers that support agent handling, including a Blender server and a Workflow server that support only agents in a specific domain.

Co-locating servers on one computer

You can reduce the number of servers in a deployment scenario by co-locating some Interaction Center servers on the same computer. You can co-locate servers on a computer if:

- You need to reduce the number of physical computers.
- You do not require the Interaction Center servers on that computer to handle a high system load or provide rapid throughput.
- You do not need physical redundancy and failover for those servers in the event that the server fails.
- You ensure that your computer has sufficient CPU and memory capacity to support all co-located services.

For example, if the system load for the chat channel and email channel is light, you can co-locate these services on a single server.

Note:
Do not locate all Interaction Center servers on a single computer. Interaction Center system with all Interaction Center servers on a single computer is not supported.

Deploying servers on multi-processor computers

These deployment scenarios show servers on separate computers. With enough CPU capacity, memory, and disk resources, you can host some Interaction Center servers on different processors in multi-processor computers.

You can host Interaction Center servers on multi-processor computers if you need to reduce the number of servers. However, this deployment reduces the physical redundancy in the system. If that single computer fails, you will lose all servers on that computer.

Important:
Do not host IC Manager on a multi-processor computer.

If the plan for an Interaction Center system includes Interaction Center servers on different physical partitions in a multi-processor computer, use the Interaction Center Sizing Tool to determine the capacity required for those servers. The Interaction Center Sizing Tool takes the following into account:

- System load
- CPU capacity
- Memory
- Disk resources

For assistance with the Interaction Center Sizing Tool, contact your Avaya representative or Avaya Business Partner representative.

Items not shown in the deployment scenarios

The following items are not shown in these deployment scenarios but the following rules apply:

RDBMS computer: The deployment scenarios do not show an RDBMS computer, but the RDBMS software must be located on a separate computer.

Event Collector Bridge: The deployment scenarios show only one Event Collector Bridge for each Resource Manager server. If you want redundancy, a minimum of two Event Collector Bridges for each Resource Manager server is required.

SMPT/POP/IMAP server: The deployments do not show a SMTP/POP/IMAP server, but the SMTP/POP/IMAP server software must be located on a separate computer.

Scenario 1: Single site, voice only

This scenario is the recommended minimum configuration for a basic Telephony only deployment. If you customize your Telephony deployment, you may need to include additional Interaction Center components.

Topics for this scenario include:

- Scenario 1: Deployment overview on page 82
- Scenario 1: Interaction Center domain overview on page 83
- Scenario 1: Partitioning of servers on page 84
- Scenario 1: Failover strategy on page 85

Scenario 1: Deployment overview

This scenario shows a potential production system with the following deployment:

- Voice channel only (no other media channels)
- Single site
- Two computers for all Interaction Center servers

- One computer for OA Event Collector server and Real-time subsystem
- One computer for IC Manager, Database Designer, and Workflow Designer
- Three computers to host Webconnector for Avaya Agent Web Client (optional)
- Three computers to host Tomcat for Client SDK and/or Web Services (optional)
- One or more agent desktop computers
- Hardware redundancy
- Server (VESP) failover

Scenario 1: Interaction Center domain overview

The Interaction Center components and OA servers in this scenario are distributed across the following Interaction Center domains:

- Default
- Core2
- User1
- User2
- Voice1
- Voice1_Helper
- Voice2
- Voice2_Helper
- Prompter1
- Prompter2
- Data1
- Data2
- OA

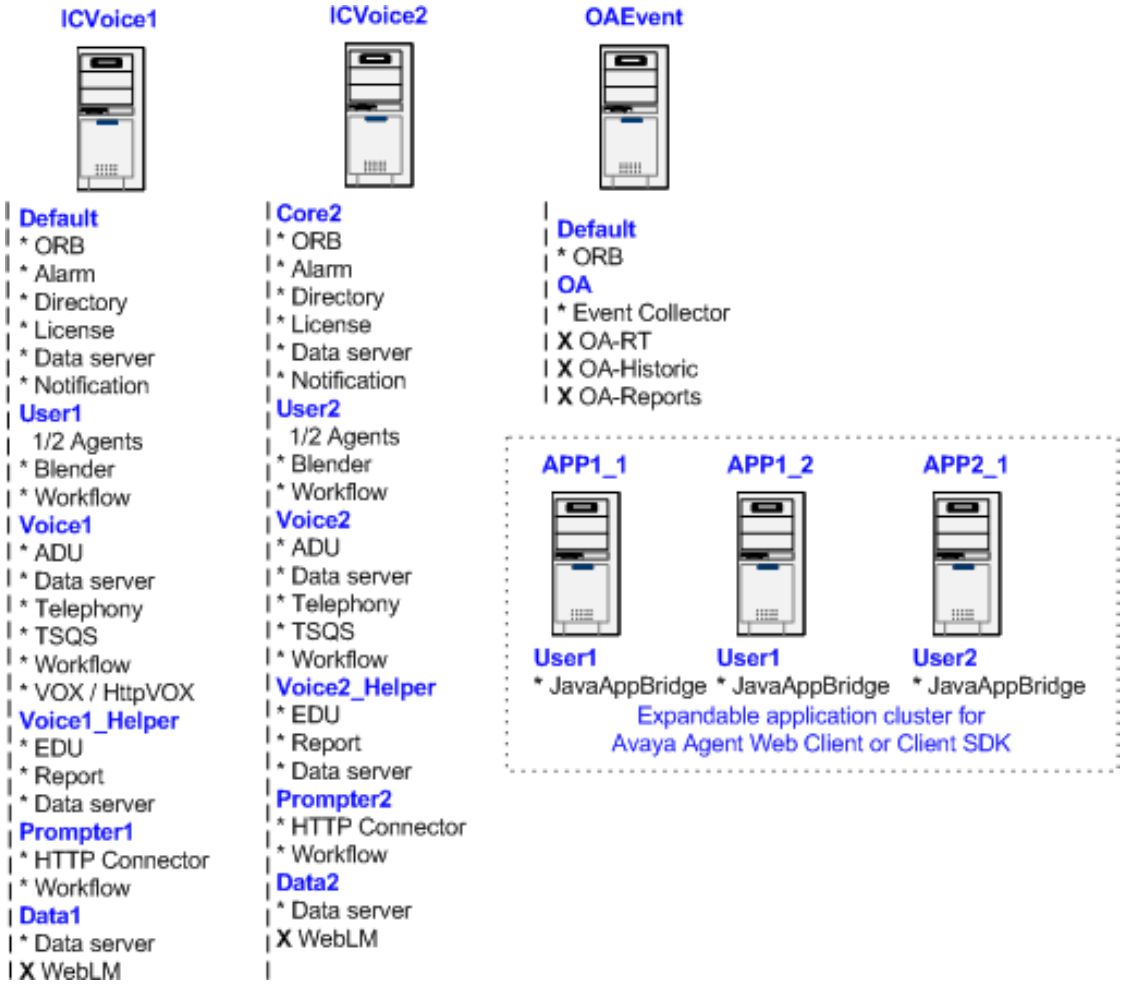
Tip:
These domains use the following naming convention: <*service*>. If you plan to scale the deployment to multiple sites, use a different naming convention for domains, such as <*site*>_<*service*>.

Scenario 1: Partitioning of servers

The physical partitioning of the servers reflects the distribution of the Interaction Center and OA components on the servers. The logical partitioning reflects the distribution of servers and agents across the Interaction Center domains.

Some of these components, such as the Web License Manager, are not servers.

The following figure shows the distribution of components on the servers. An **X** before a component indicates that component is installed on the computer, but does not belong to an Interaction Center domain.



Scenario 1: Failover strategy

The following table shows the failover strategy in this scenario. The components in the Interaction Center domain in the left column failover to the Interaction Center domains in the right column in the order listed.

Domain	Failover domains
Default	1. Default 2. Core2
Core2	1. Core2 2. Default
User1	1. User1 2. User2 3. Prompter1 4. Prompter2 5. Data1 6. Data2 7. Voice1 8. Voice1_Helper 9. Voice2 10.Voice2_Helper 11.Default 12.Core2
User2	1. User2 2. User1 3. Prompter2 4. Prompter1 5. Data2 6. Data1 7. Voice2 8. Voice2_Helper 9. Voice1 10.Voice1_Helper 11.Core2 12.Default

Domain	Failover domains
Voice1	1. Voice1 2. Data1 3. Voice1_Helper 4. Voice2 5. Data2 6. Voice2_Helper 7. Default 8. Core2
Voice1_Helper	1. Voice1_Helper 2. Data1 3. Voice2_Helper 4. Data2 5. Default 6. Core2
Voice2	1. Voice2 2. Data2 3. Voice2_Helper 4. Voice1 5. Data1 6. Voice1_Helper 7. Core2 8. Default
Voice2_Helper	1. Voice2_Helper 2. Data2 3. Voice1_Helper 4. Data1 5. Core2 6. Default

Domain	Failover domains
Prompter1	1. Prompter1 2. Prompter2 3. Data1 4. Data2 5. Default 6. Core2 7. Voice1 8. Voice1_Helper 9. Voice2 10.Voice2_Helper
Prompter2	1. Prompter2 2. Prompter1 3. Data2 4. Data1 5. Core2 6. Default 7. Voice2 8. Voice2_Helper 9. Voice1 10.Voice1_Helper
Data1	1. Data1 2. Default 3. Core2
Data2	1. Data2 2. Core2 3. Default
OA	1. OA 2. Voice1 3. Voice1_Helper 4. Voice2 5. Voice2_Helper 6. Default 7. Core2

Scenario 2: Business Advocate for single site, voice only

This scenario extends Scenario 1: Single site, voice only on page 82 to include Business Advocate. This scenario is the recommended minimum configuration for Business Advocate in a basic single site, voice only deployment. This scenario assumes a low to medium volume of voice contacts.

Topics for this scenario include:

- Scenario 2: Deployment overview on page 88
- Scenario 2: Interaction Center domain overview on page 89
- Scenario 2: Partitioning of Business Advocate servers on page 90
- Scenario 2: Failover strategy on page 91

Scenario 2: Deployment overview

This scenario adds Business Advocate servers to the computers that host Interaction Center servers, described in Scenario 1: Deployment overview on page 82. This deployment includes a single Logical Resource Manager with two Resource Manager servers. The Resource Manager server in RM1 is the primary. The Resource Manager server in RM2 is the standby.

If you host:

- Interaction Center servers on Windows, this scenario does not require additional computers.
- Interaction Center servers on Oracle Solaris or AIX, this scenario requires two Microsoft Windows computers to host the Resource Manager servers.
- Interaction Center and OA databases in DB2 on AIX, this scenario requires the following:
  - A Windows or Oracle Solaris computer to host the Business Advocate databases. If desired, you can install SQL Server on a computer that hosts a Resource Manager server.
  - An additional Data server on the same computers as the Resource Manager servers to provide Interaction Center with access to the Business Advocate database and data, such as service classes. Configure this Data server in its own domain, such as RM_Data. Add the RM_Data domain to the failover path for all domains that include Directory servers and Workflow servers that run contact qualification workflows.

Scenario 2: Interaction Center domain overview

The Business Advocate server components in this scenario are distributed across the following Interaction Center domains in addition to those listed in Scenario 1: Interaction Center domain overview on page 83:

- RM1
- RM2
- RM_Helper1
- RM_Helper2

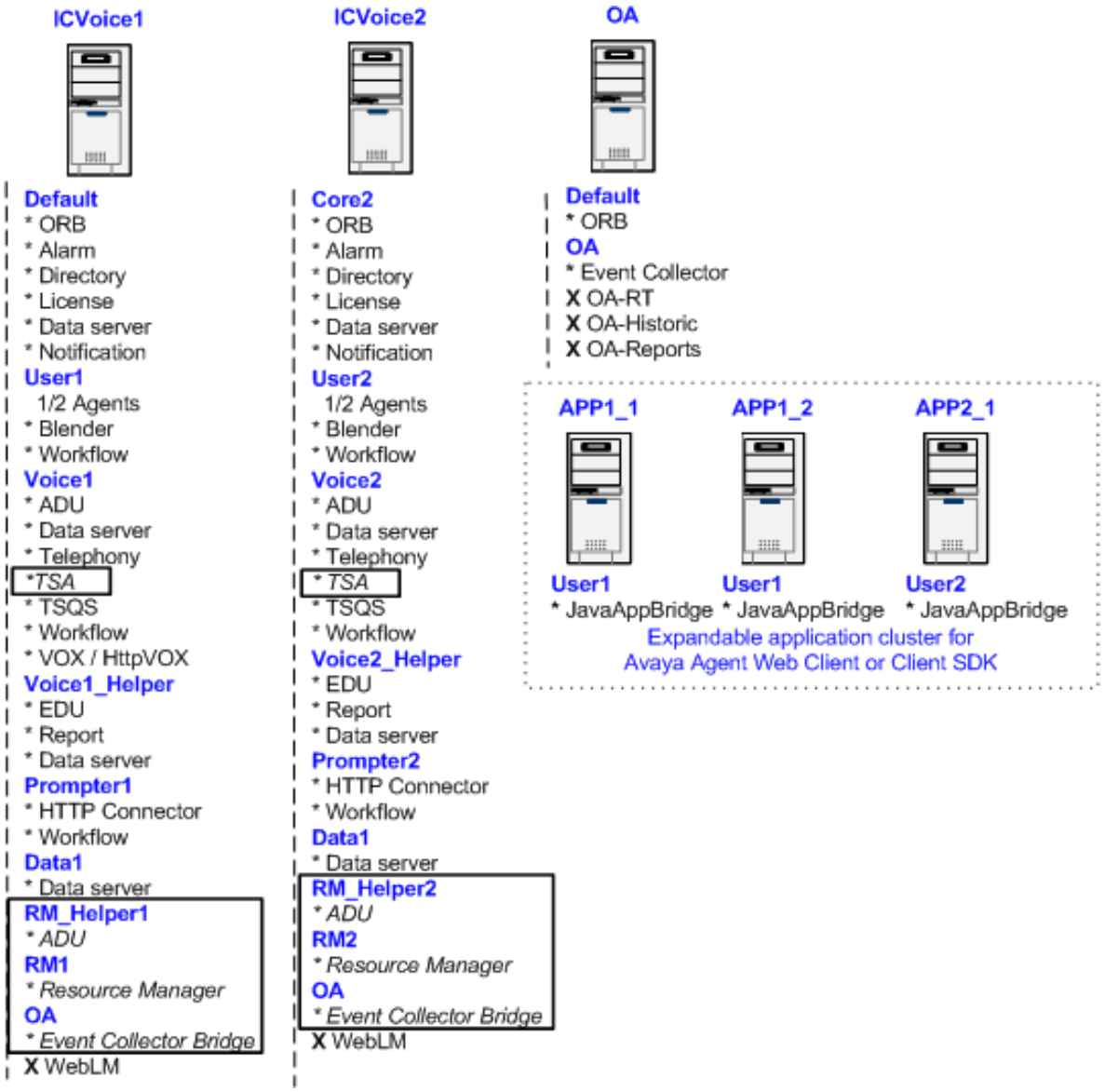


Tip:
These domains use the following naming convention: <*service*>. If you plan to scale the deployment to multiple sites, use a different naming convention for domains, such as <*site*>_<*service*>.

Scenario 2: Partitioning of Business Advocate servers

The physical partitioning of the servers reflects the distribution of the Business Advocate components on the servers. The logical partitioning reflects the distribution of servers and agents across the Interaction Center domains.

The following figure shows the distribution of Business Advocate servers on the servers. The highlighted servers are in addition to those components described in Scenario 1: Partitioning of servers on page 84.



Scenario 2: Failover strategy

Business Advocate has some unique failover strategies for the Resource Manager and the voice channel. For details about those strategies, see *IC Business Advocate Configuration and Administration Guide*.

The following table shows the failover strategy for the Business Advocate domains in this scenario. The Business Advocate domains do not failover to any of the other Interaction Center domains. The components in the domain in the left column failover to the domains in the right column in the order listed. For failover information for the domains not listed in the following table, see Scenario 1: Failover strategy on page 85.

Domain	Failover domains
RM_Helper1	1. RM_Helper1 2. Default 3. Core2
RM_Helper2	1. RM_Helper2 2. Default 3. Core2
RM1	1. RM1 2. RM_Helper1 3. RM_Helper2 4. Default 5. Core2
RM2	1. RM2 2. RM_Helper1 3. RM_Helper2 4. Default 5. Core2

Scenario 3: Business Advocate for single site, high volume voice

This scenario is the recommended minimum configuration to add Business Advocate components to Scenario 1: Single site, voice only in a contact center which expects a high volume of voice contacts.

This deployment shows a single Logical Resource Manager with two Resource Manager servers. The Resource Manager server in RM1 is the primary. The Resource Manager server in RM2 is the standby. The Logical Resource Manager components are hosted on dedicated processors to support the higher volume of contacts.

For more information, see *IC Business Advocate Configuration and Administration Guide*.

Topics for this scenario include:

- Scenario 3: Deployment overview on page 92
- Scenario 3: Interaction Center domain overview on page 93
- Scenario 3: Partitioning of Business Advocate servers on page 94
- Scenario 3: Failover strategy on page 95

Scenario 3: Deployment overview

This scenario adds Business Advocate servers to the computers that host Interaction Center servers, described in Scenario 1: Deployment overview on page 82. This scenario also adds the following:

- Two computers to host Telephony servers and other Interaction Center servers.
- Two computers to host Resource Manager servers and other Interaction Center servers.

If you host Interaction Center and OA databases in DB2 on AIX, this scenario also requires the following:

- A Windows or Oracle Solaris computer to host the Business Advocate databases. If required, you can install SQL Server on a computer that hosts a Resource Manager server.
- An additional Data server on the same computer as a Resource Manager server. This Data server will provide Interaction Center with access to the Business Advocate database and data, such as service classes. Configure this Data server in its own domain, such as RM_Data. Add the RM_Data domain to the failover path for all domains that include Directory servers and Workflow servers that run contact qualification workflows.

Scenario 3: Interaction Center domain overview

The Business Advocate server components in this scenario are distributed across the following Interaction Center domains in addition to those listed in Scenario 1: Interaction Center domain overview on page 83:

- Voice3
- Voice3_Helper
- Voice4
- Voice4_Helper
- RM1
- RM2
- RM_Helper1
- RM_Helper2

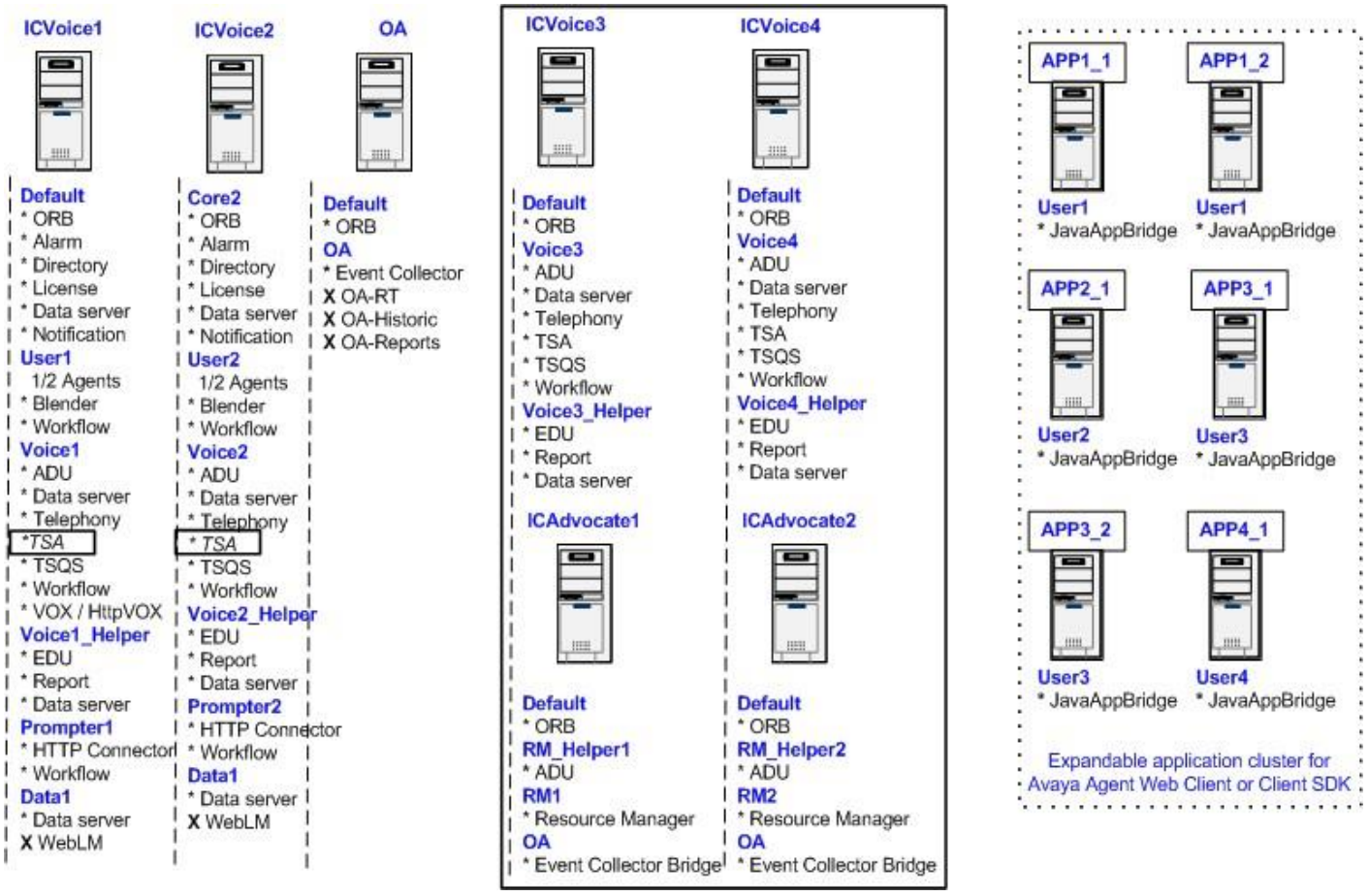


Tip:
These domains use the `<service>` naming convention. If you plan to scale the deployment to multiple sites, use a different naming convention for domains, such as `<site>_<service>`.

Scenario 3: Partitioning of Business Advocate servers

The physical partitioning of the servers reflects the distribution of the Business Advocate components on the servers. The logical partitioning reflects the distribution of servers and agents across the Interaction Center domains.

The following figure shows the distribution of Business Advocate servers on the servers. The highlighted servers are in addition to those components described in Scenario 1: Partitioning of servers on page 84.



Scenario 3: Failover strategy

Business Advocate has some unique failover strategies for the Resource Manager and the voice channel. For details about those strategies, see *IC Business Advocate Configuration and Administration Guide*.

The following table shows the failover strategy for the new Interaction Center domains and the Business Advocate domains in this scenario. For failover information for the domains not listed in this table, see Scenario 1: Failover strategy on page 85.

The Business Advocate domains do not failover to any of the other Interaction Center domains. The components in the domain in the left column failover to the domains in the right column in the listed order.

Domain	Failover domains
Voice3	1. Voice3 2. Voice3_Helper 3. Voice4 4. Voice4_Helper 5. Default 6. Core2
Voice3_Helper	1. Voice3_Helper 2. Voice4_Helper 3. Default 4. Core2
Voice4	1. Voice4 2. Voice4_Helper 3. Voice3 4. Voice3_Helper 5. Core2 6. Default
Voice4_Helper	1. Voice4_Helper 2. Voice3_Helper 3. Core2 4. Default
RM_Helper1	1. RM_Helper1 2. Default 3. Core2

Domain	Failover domains
RM_Helper2	1. RM_Helper2 2. Default 3. Core2
RM1	1. RM1 2. RM_Helper1 3. RM_Helper2 4. Default 5. Core2
RM2	1. RM2 2. RM_Helper1 3. RM_Helper2 4. Default 5. Core2

Scenario 4: Single site, multi-channel

This scenario is the recommended minimum configuration for a basic single site, multi-channel deployment. If you customize your multi-channel deployment, you may need to include additional computers and Interaction Center components.

Topics for this scenario include:

- Scenario 4: Deployment overview on page 96
- Scenario 4: Interaction Center domain overview on page 97
- Scenario 4: Partitioning of servers on page 99
- Scenario 4: Failover strategy on page 100

Scenario 4: Deployment overview

This scenario shows a potential production system with the following deployment:

- All media channels
- Single site
- One computer for the website and Web-related servers in the network DMZ
- Six computers for all other Interaction Center servers

- One computer for OA Event Collector server and Real-time subsystem
- One computer for IC Manager, Database Designer, and Workflow Designer
- Three computers to host Webconnector for Avaya Agent Web Client (optional)
- One or more agent desktop computers
- One computer for SMTP and POP / IMAP servers
- One computer for your RDBMS
- Hardware redundancy
- Server (VESP) failover
- One cluster per Poller, ICEMail and WACD servers respectively

Scenario 4: Interaction Center domain overview

The Interaction Center server components in this scenario are distributed across the following Interaction Center domains:

- Default
- Rome_Core2
- Rome_User1
- Rome_User2
- Rome_Voice1
- Rome_Voice1_Helper
- Rome_Voice2
- Rome_Voice2_Helper
- Rome_Prompter1
- Rome_Prompter2
- Rome_Web
- Rome_Web2
- Rome_Web_Helper
- Rome_Web2_Helper
- Rome_Website
- Rome_Email
- Rome_Email_Helper
- Rome_Email2_Helper

- Rome_Email2
- OA

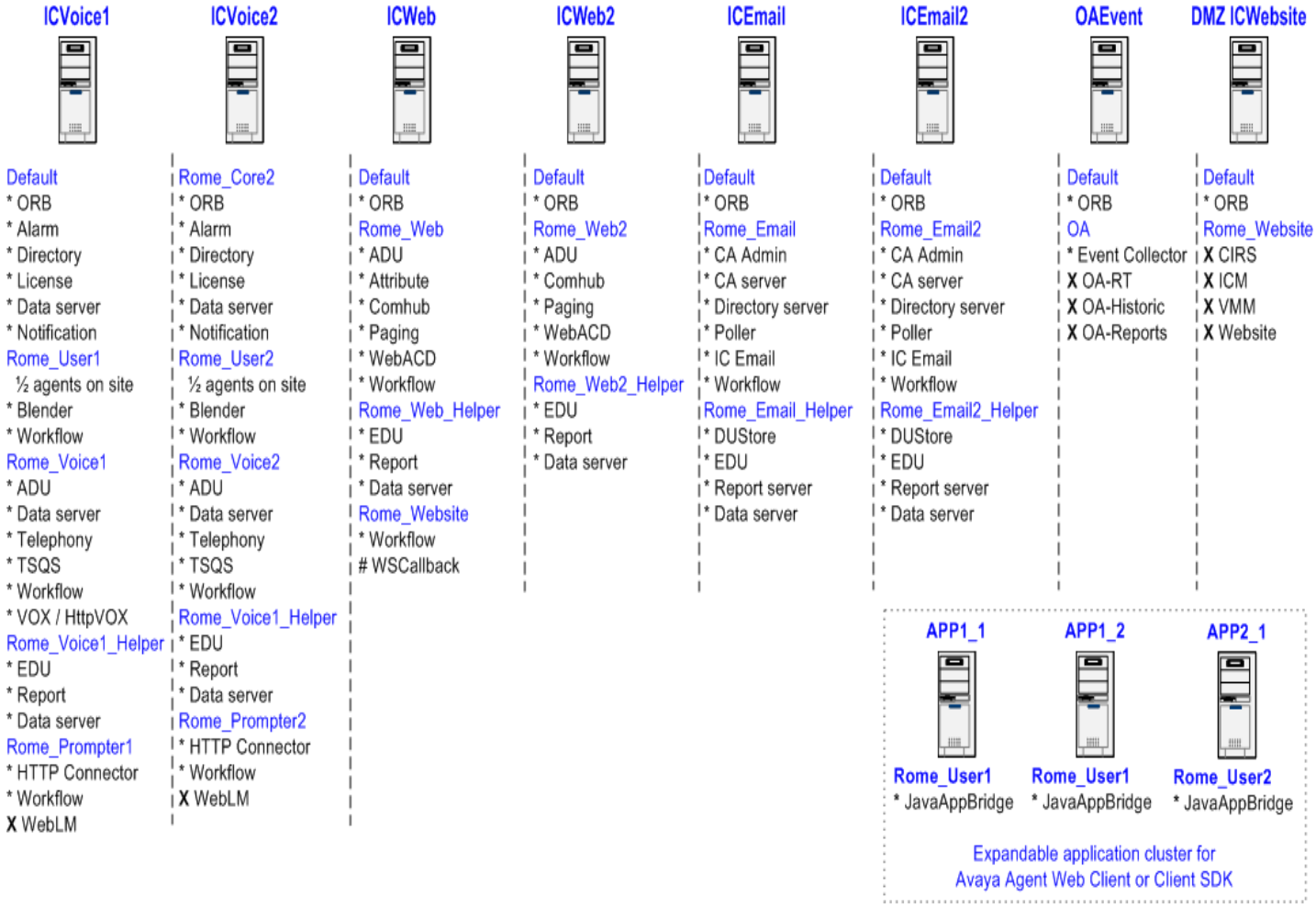


Tip:
These domains use the following naming convention: <*site*>_<*service*>. For a single site deployment that does not expand to more sites, you can use a different naming convention for domains, such as <*computer_name*>_<*service*>.

Scenario 4: Partitioning of servers

The physical partitioning of the servers reflects the distribution of the Interaction Center and OA components on the servers. The logical partitioning reflects the distribution of servers and agents across the Interaction Center domains.

The following figure shows the distribution of components on the servers. An **X** indicates that component is installed on the computer, but does not belong to an Interaction Center domain. A # indicates that component is installed only if the optional Avaya Agent Web Client or Client SDK components in the dotted-line box are not installed.



Scenario 4: Failover strategy

The following table shows the failover strategy in this scenario. The components in the Interaction Center domain in the left column failover to the Interaction Center domains in the right column in the listed order.

Domain	Failover domains
Default	1. Default 2. Rome_Core2
Rome_Core2	1. Rome_Core2 2. Default
Rome_User1	1. Rome_User1 2. Rome_User2 3. Rome_Prompter1 4. Rome_Prompter2 5. Default 6. Rome_Core2 7. Rome_Voice1 8. Rome_Voice1_Helper 9. Rome_Voice2 10.Rome_Voice2_Helper 11.Rome_Email 12.Rome_Email_Helper 13.Rome_Email2 14.Rome_Email2_Helper 15.Rome_Web 16.Rome_Web_Helper 17.Rome_Web2 18.Rome_Web2_Helper

Domain	Failover domains
Rome_User2	1. Rome_User2 2. Rome_User1 3. Rome_Prompter2 4. Rome_Prompter1 5. Rome_Core2 6. Default 7. Rome_Voice2 8. Rome_Voice2_Helper 9. Rome_Voice1 10.Rome_Voice1_Helper 11.Rome_Email 12.Rome_Email_Helper 13.Rome_Email2 14.Rome_Email2_Helper 15.Rome_Web 16.Rome_Web_Helper 17.Rome_Web2 18.Rome_Web2_Helper
Rome_Voice1	1. Rome_Voice1 2. Rome_Voice1_Helper 3. Rome_Voice2 4. Rome_Voice2_Helper 5. Default 6. Rome_Core2
Rome_Voice1_Helper	1. Rome_Voice1_Helper 2. Rome_Voice2_Helper 3. Default 4. Rome_Core2
Rome_Voice2	1. Rome_Voice2 2. Rome_Voice2_Helper 3. Rome_Voice1 4. Rome_Voice1_Helper 5. Rome_Core2 6. Default

Domain	Failover domains
Rome_Voice2_Helper	1. Rome_Voice2_Helper 2. Rome_Voice1_Helper 3. Rome_Core2 4. Default
Rome_Prompter1	1. Rome_Prompter1 2. Rome_Prompter2 3. Default 4. Rome_Core2 5. Rome_Voice1 6. Rome_Voice1_Helper 7. Rome_Voice2 8. Rome_Voice2_Helper
Rome_Prompter2	1. Rome_Prompter2 2. Rome_Prompter1 3. Rome_Core2 4. Default 5. Rome_Voice2 6. Rome_Voice2_Helper 7. Rome_Voice1 8. Rome_Voice1_Helper
Rome_Email	1. Rome_Email 2. Rome_Email_Helper 3. Default 4. Rome_Core2 **Note:** In case you modify the Analyze Workflow to access the ADU server, you need to modify Email domain failover sequence to have a domain that has an ADU server.
Rome_Email2	1. Rome_Email2 2. Rome_Email2_Helper 3. Default 4. Rome_Core2 **Note:** In case you modify the Analyze Workflow to access the ADU server, you need to modify Email domain failover sequence to have a domain that has an ADU server.
Rome_Email_Helper	1. Rome_Email_Helper 2. Default 3. Rome_Core2

Domain	Failover domains
Rome_Email2_Helper	1. Rome_Email2_Helper 2. Default 3. Rome_Core2
Rome_Web	1. Rome_Web 2. Rome_Web_Helper 3. Default 4. Rome_Core2 **Note:** If you do not configure the Event Collector server to monitor the ADU server in this domain, configure the server groups on the **Advanced** tab as follows: Rome_Web: Priority Value = 1
Rome_Web2	1. Rome_Web2 2. Rome_Web2_Helper 3. Default 4. Rome_Core2 **Note:** If you do not configure the Event Collector server to monitor the ADU server in this domain, configure the server groups on the **Advanced** tab as follows: Rome_Web2: Priority Value = 1
Rome_Web_Helper	1. Rome_Web_Helper 2. Default 3. Rome_Core2
Rome_Web2_Helper	1. Rome_Web2_Helper 2. Default 3. Rome_Core2
Rome_Website	1. Rome_Website 2. Rome_Web 3. Rome_Voice1 4. Rome_Voice1_Helper 5. Default 6. Rome_Core2
OA	1. OA 2. Rome_Voice1 3. Rome_Voice1_Helper 4. Rome_Voice2 5. Rome_Voice2_Helper 6. Default 7. Rome_Core2

Scenario 5: Single site, multi-channel with high volume voice

This scenario is the recommended minimum configuration for a single site, multi-channel deployment in a contact center that expects a high volume of voice contacts. If you customize your multi-channel deployment, you may need to include additional computers and Interaction Center components.

This deployment is similar to Scenario 4: Single site, multi-channel on page 96. However, the Voice services are on dedicated processors to increase their ability to handle higher voice contact transaction rates.

This deployment also shows how you can configure redundancy for Core and Voice services. Telephony Servers are paired for redundancy. Web and Email services do not have redundancy support.

Topics for this scenario include:

- Scenario 5: Deployment overview on page 104
- Scenario 5: Interaction Center domain overview on page 105
- Scenario 5: Partitioning of servers on page 106
- Scenario 5: Failover strategy on page 108

Scenario 5: Deployment overview

This scenario shows a potential production system with the following deployment:

- All media channels with high volume voice traffic.
- Single site.
- One computer for the website and Web-related servers in the network DMZ.
- Eight computers for all other Interaction Center servers.
- One computer for OA Event Collector server and Real-time subsystem.
- One computer for IC Manager, Database Designer, and Workflow Designer.
- Six computers to host Webconnector for Avaya Agent Web Client (optional).
- Six computers to host Tomcat for Client SDK and/or Web Services (optional).
- One or more agent desktop computers.
- One computer for SMTP and POP / IMAP servers.
- One computer for your RDBMS.

- Hardware redundancy.
- Server (VESP) failover.
- One cluster per Poller, ICEMail and WACD servers respectively.

Scenario 5: Interaction Center domain overview

The Interaction Center server components in this scenario are distributed across the following Interaction Center domains:

- Default
- Taos_User1
- Taos_User2
- Taos_Voice1
- Taos_Voice1_Helper
- Taos_Voice2
- Taos_Voice2_Helper
- Taos_Prompter1
- Taos_Prompter2
- Taos_Core2
- Taos_Web
- Taos_Web2
- Taos_Website
- Taos_Web_Helper
- Taos_Email
- Taos_Email_Helper
- Taos_Web2_Helper
- Taos_Email2
- Taos_Email2_Helper
- Taos_OA



Tip:
These domains use the following naming convention: <*site*>_<*service*>. For a single site deployment that does not expand to more sites, you can use a different naming convention for domains, such as <*computer_name*>_<*service*>.

Scenario 5: Partitioning of servers

The physical partitioning of the servers reflects the distribution of the Interaction Center and OA components on the servers. The logical partitioning reflects the distribution of servers and agents across the Interaction Center domains.

The following figure shows the distribution of components on the server. An **X** indicates that component is installed on the computer, but does not belong to an Interaction Center domain. A # indicates that component is installed only if the optional Avaya Agent Web Client or Client SDK components in the dotted-line box are not installed.


ICCore1
Default
* ORB
* Alarm
* Directory
* License
* Data server
* Notification
Taos_User1
½ agents on site
* Blender
* Workflow
Taos_Prompter1
* HTTP Connector
* Workflow
X WebLM
ICCore2
Taos_Core2
* ORB
* Alarm
* Directory
* License
* Data server
* Notification
Taos_User2
½ agents on site
* Blender
* Workflow
Taos_Prompter2
* HTTP Connector
* Workflow
X WebLM
ICVoice1
Default
* ORB
Taos_Voice1
* ADU
* Data server
* Telephony
* TSQS
* Workflow
* VOX / HttpVOX
Taos_Voice1_Helper
* EDU
* Report
* Data server
ICVoice2
Taos_Core2
* ORB
Taos_Voice2
* ADU
* Data server
* Telephony
* TSQS
* Workflow
* VOX / HttpVOX
Taos_Voice2_Helper
* EDU
* Report
* Data server
ICWeb
Default
* ORB
Taos_Web
* ADU
* Attribute
* Comhub
* Paging
* WebACD
* Workflow
Taos_Web_Helper
* EDU
* Report
* Data server
Taos_Website
* Workflow
ICWeb2
Default
* ORB
Taos_Web2
* ADU
* Comhub
* Paging
* WebACD
* Workflow
Taos_Web2_Helper
* EDU
* Report
* Data server
ICEmail
Default
* ORB
Taos_Email
* CA Admin
* CA server
* Directory server
* IC Email
* Poller
* Workflow
Taos_Email_Helper
* DUStore
* EDU
* Report
* Data server
ICEmail2
Default
* ORB
Taos_Email2
* CA Admin
* CA server
* Directory server
* IC Email
* Poller
* Workflow
Taos_Email2_Helper
* DUStore
* EDU
* Report
* Data server
OAEvent
Default
* ORB
Taos_OA
* Event Collector
X OA-RT
X OA-Historic
X OA-Reports
DMZ ICWebsite
Default
* ORB
Website
* Attribute
# WSCallback
X CIRS
X ICM
X VMM
X WebSite
APP1_1
Taos_User1
* JavaAppBridge
APP1_2
Taos_User1
* JavaAppBridge
APP2_1
Taos_User1
*JavaAppBridge
APP3_1
Taos_User2
* JavaAppBridge
APP3_2
Taos_User2
* JavaAppBridge
APP4_1
Taos_User2
* JavaAppBridge
Expandable application cluster for
Avaya Agent Web Client or Client SDK

Scenario 5: Failover strategy

The following table shows the failover strategy in this scenario. The components in the Interaction Center domain in the left column failover to the Interaction Center domains in the right column in the order listed.

Domain	Failover domains
Taos_User1	1. Taos_User1 2. Taos_User2 3. Taos_Prompter1 4. Taos_Prompter2 5. Default 6. Taos_Core2 7. Taos_Voice1 8. Taos_Voice1_Helper 9. Taos_Voice2 10.Taos_Voice2_Helper 11.Taos_Email_Helper 12.Taos_Email2_Helper 13.Taos_Web 14.Taos_Web_Helper 15.Taos_Web2 16.Taos_Web2_Helper
Taos_User2	1. Taos_User2 2. Taos_User1 3. Taos_Prompter2 4. Taos_Prompter1 5. Taos_Core2 6. Default 7. Taos_Voice2 8. Taos_Voice2_Helper 9. Taos_Voice1 10.Taos_Voice1_Helper 11.Taos_Email_Helper 12.Taos_Email2_Helper 13.Taos_Web 14.Taos_Web_Helper 15.Taos_Web2 16.Taos_Web2_Helper

Domain	Failover domains
Taos_Voice1	1. Taos_Voice1 2. Taos_Voice1_Helper 3. Taos_Voice2 4. Taos_Voice2_Helper 5. Default 6. Taos_Core2
Taos_Voice1_Helper	1. Taos_Voice1_Helper 2. Taos_Voice2_Helper 3. Default 4. Taos_Core2
Taos_Voice2	1. Taos_Voice2 2. Taos_Voice2_Helper 3. Taos_Voice1 4. Taos_Voice1_Helper 5. Taos_Core2 6. Default
Taos_Voice2_Helper	1. Taos_Voice2_Helper 2. Taos_Voice1_Helper 3. Taos_Core2 4. Default
Taos_Prompter1	1. Taos_Prompter1 2. Taos_Prompter2 3. Default 4. Taos_Core2 5. Taos_Voice1 6. Taos_Voice1_Helper 7. Taos_Voice2 8. Taos_Voice2_Helper
Taos_Prompter2	1. Taos_Prompter2 2. Taos_Prompter1 3. Taos_Core2 4. Default 5. Taos_Voice2 6. Taos_Voice2_Helper 7. Taos_Voice1 8. Taos_Voice1_Helper

Domain	Failover domains
Default	1. Default 2. Taos_Core2
Taos_Core2	1. Taos_Core2 2. Default
Taos_Email	1. Taos_Email 2. Taos_Email_Helper 3. Default 4. Taos_Core2 **Note:** In case you modify the Analyze Workflow to access the ADU server, you need to modify Email domain failover sequence to have a domain that has an ADU server.
Taos_Email2	1. Taos_Email2 2. Taos_Email2_Helper 3. Default 4. Taos_Core2 **Note:** In case you modify the Analyze Workflow to access the ADU server, you need to modify Email domain failover sequence to have a domain that has an ADU server.
Taos_Email_Helper	1. Taos_Email_Helper 2. Default 3. Taos_Core2
Taos_Email2_Helper	1. Taos_Email2_Helper 2. Default 3. Taos_Core2
Taos_Web	1. Taos_Web 2. Taos_Web_Helper 3. Default 4. Taos_Core2 **Note:** If you do not configure the Event Collector server to monitor the ADU server in this domain, configure the server groups on the **Advanced** tab as follows: Taos_Web: Priority Value = 1

Domain	Failover domains
Taos_Web2	1. Taos_Web2 2. Taos_Web2_Helper 3. Taos_Core2 4. Default **Note:** If you do not configure the Event Collector server to monitor the ADU server in this domain, configure the server groups on the **Advanced** tab as follows: Taos_Web2: Priority Value = 1
Taos_Web_Helper	1. Taos_Web_Helper 2. Default 3. Taos_Core2
Taos_Web2_Helper	1. Taos_Web2_Helper 2. Default 3. Taos_Core2
Taos_Website	1. Taos_Website 2. Taos_Web 3. Taos_Voice1 4. Taos_Voice1_Helper 5. Default 6. Taos_Core2
Taos_OA	1. Taos_OA 2. Taos_Voice1 3. Taos_Voice1_Helper 4. Taos_Voice2 5. Taos_Voice2_Helper 6. Default 7. Taos_Core2

Scenario 6: Business Advocate for single site, multi-channel

This scenario extends Scenario 4: Single site, multi-channel on page 96 to include Business Advocate. This scenario is the recommended minimum configuration to add Business Advocate components to a basic single site, multi-channel deployment in a contact center which does not expect a high volume of contacts.

A single instance of Business Advocate indicates that the Interaction Center system includes only one Logical Resource Manager for Business Advocate. For more information about Logical Resource Managers, see *IC Business Advocate Configuration and Administration Guide*.

Topics for this scenario include:

- Scenario 6: Deployment overview on page 113
- Scenario 6: Interaction Center domain overview on page 113
- Scenario 6: Partitioning of Business Advocate servers on page 115
- Scenario 6: Failover strategy on page 116

Scenario 6: Deployment overview

This scenario adds Business Advocate servers to the computers that host Interaction Center servers, described in Scenario 4: Deployment overview on page 96.

If you host:

- Interaction Center servers on Windows, this scenario does not require additional computers.
- Interaction Center servers on Oracle Solaris or AIX, this scenario requires two Windows computers to host the Resource Manager servers.
- Interaction Center and OA databases in DB2 on AIX, this scenario requires the following:
  - A Windows or Oracle Solaris computer to host the Business Advocate databases. If required, you can install SQL Server on a computer that hosts a Resource Manager server.
  - An additional data server on the same computer as a Resource Manager server. This data server provides Interaction Center with access to the Business Advocate database and data, such as service classes. Configure this Data server in its own domain, such as RM_Data. Add the RM_Data domain to the failover path for all domains that include Directory servers and Workflow servers that run contact qualification workflows.

Scenario 6: Interaction Center domain overview

The Business Advocate servers components in this scenario are distributed across the following Interaction Center domains in addition to those listed in Scenario 4: Interaction Center domain overview on page 97:

- Rome_RM1
- Rome_RM2

- Rome_RM_Helper1
- Rome_RM_Helper2

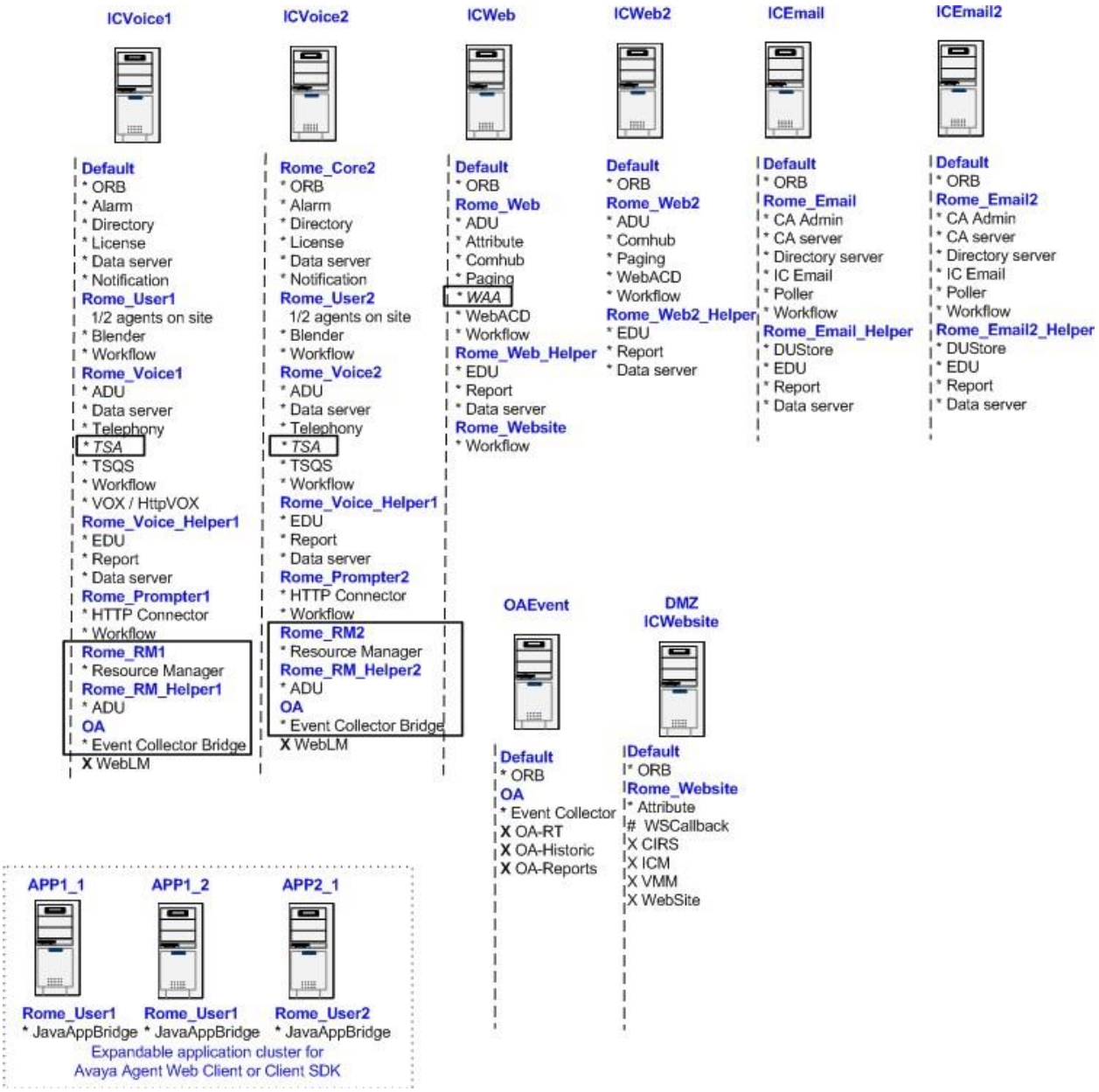


Tip:
These domains use the following naming convention: <*site*>_<*service*>. For a single site deployment that does not expand to more sites, you can use a different naming convention for domains, such as <*computer_name*>_<*service*>.

Scenario 6: Partitioning of Business Advocate servers

The physical partitioning of the servers reflects the distribution of the Business Advocate components on the servers. The logical partitioning reflects the distribution of servers and agents across the Interaction Center domains.

The following figure shows the distribution of Business Advocate servers on the servers. The highlighted servers are in addition to those components described in Scenario 4: Partitioning of servers on page 99.



Scenario 6: Failover strategy

Business Advocate has some unique failover strategies for the Resource Manager and the voice channel. For details about those strategies, see *IC Business Advocate Configuration and Administration Guide*.

The following table shows the failover strategy for the Business Advocate domains in this scenario. The Business Advocate domains do not failover to any of the other Interaction Center domains. The components in the domain in the left column failover to the domains in the right column in the order listed. For failover information for the domains not listed in this table, see Scenario 4: Failover strategy on page 100.

Domain	Failover domains
RM_Helper1	1. RM_Helper1 2. Default 3. Core2
RM_Helper2	1. RM_Helper2 2. Default 3. Core2
RM1	1. RM1 2. RM_Helper1 3. RM_Helper2 4. Default 5. Core2
RM2	1. RM2 2. RM_Helper1 3. RM_Helper2 4. Default 5. Core2

Note:

Advocate channel is disrupted if the computer that hosts Rome_Web is unavailable. However, WAA is enhanced to work with any WACD server available in any domain as it does not follow failover path for communication with WACD server.

Scenario 7: Single site, chat and email only

This scenario is the recommended minimum configuration for a basic single site deployment in a contact center which includes chat and email channels. This deployment does not include redundancy. If you customize this deployment, you may need to include additional computers and Interaction Center components.

Topics for this scenario include:

- Scenario 7: Deployment overview on page 117
- Scenario 7: Interaction Center domain overview on page 118
- Scenario 7: Partitioning of servers on page 119
- Scenario 7: Failover strategy on page 120

Scenario 7: Deployment overview

This scenario shows a potential production system with the following deployment:

- Chat and email media channels.
- Single site.
- One computer for the website and Web-related servers in the network DMZ.
- Four computers for all other Interaction Center servers.
- One computer for OA Event Collector server and Real-time subsystem.
- One computer for IC Manager, Database Designer, and Workflow Designer.
- Three computers to host Webconnector for Avaya Agent Web Client (optional).
- Three computers to host Tomcat for Client SDK and/or Web Services (optional).
- One or more agent desktop computers.
- One computer for SMTP and POP / IMAP servers.
- One computer for your RDBMS.
- Hardware redundancy.
- Server (VESP) failover.
- One cluster per Poller, ICEMail and WACD servers respectively.

Scenario 7: Interaction Center domain overview

The Interaction Center server components in this scenario are distributed across the following Interaction Center domains:

- Default
- Taos_User1
- Taos_Prompter1
- Taos_Web
- Taos_Web2
- Taos_Web_Helper
- Taos_Web2_Helper
- Taos_Website
- Taos_Email
- Taos_Email_Helper
- Taos_Email2
- Taos_Email2_Helper
- Taos_OA

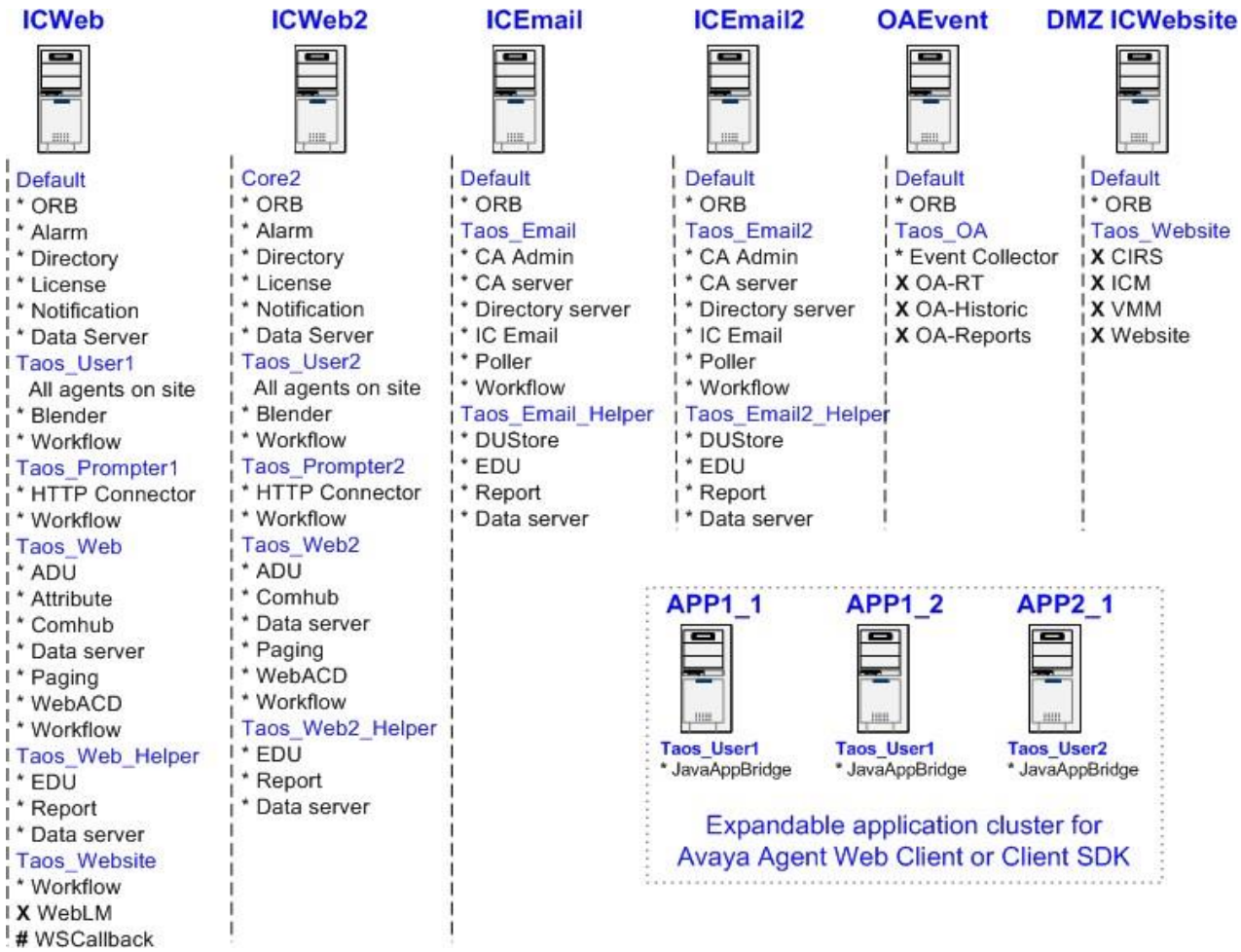


Tip:
These domains use the following naming convention: <*site*>_<*service*>. For a single site deployment that does not expand to more sites, you can use a different naming convention for domains, such as <*computer_name*>_<*service*>.

Scenario 7: Partitioning of servers

The physical partitioning of the servers reflects the distribution of the Interaction Center and OA components on the servers. The logical partitioning reflects the distribution of servers and agents across the Interaction Center domains.

The following figure shows the distribution of components on the servers. An **X** indicates that a component is installed on the computer, but does not belong to an Interaction Center domain. A # indicates that a component is installed only if the optional Avaya Agent Web Client or Client SDK components in the dotted-line box are not installed.



Scenario 7: Failover strategy

The following table shows the failover strategy in this scenario. The components in the Interaction Center domain in the left column failover to the Interaction Center domains in the right column in the order listed.

Domain	Failover domains
Taos_User1	1. Taos_User1 2. Taos_Prompter1 3. Default 4. Core2 5. Taos_Web 6. Taos_Web2 7. Taos_Email 8. Taos_Email_Helper 9. Taos_Email2 10.Taos_Email2_Helper 11.Taos_Web_Helper 12.Taos_Web2_Helper
Taos_User2	1. Taos_User2 2. Taos_Prompter2 3. Core2 4. Default 5. Taos_Web 6. Taos_Web2 7. Taos_Email 8. Taos_Email_Helper 9. Taos_Email2 10.Taos_Email2_Helper 11.Taos_Web_Helper 12.Taos_Web2_Helper
Taos_Prompter1	1. Taos_Prompter1 2. Default 3. Core2
Taos_Prompter2	1. Taos_Prompter2 2. Core2 3. Default

Domain	Failover domains
Default	1. Default 2. Core2
Core2	1. Core2 2. Default
Taos_Email	1. Taos_Email 2. Taos_Email_Helper 3. Default 4. Core2 **Note:** In case you modify the Analyze Workflow to access the ADU server, you need to modify Email domain failover sequence to have a domain that has an ADU server.
Taos_Email2	1. Taos_Email2 2. Taos_Email2_Helper 3. Core2 4. Default **Note:** In case you modify the Analyze Workflow to access the ADU server, you need to modify Email domain failover sequence to have a domain that has an ADU server.
Taos_Email_Helper	1. Taos_Email_Helper 2. Default 3. Core2
Taos_Email2_Helper	1. Taos_Email2_Helper 2. Core2 3. Default
Taos_Web	1. Taos_Web 2. Taos_Web_Helper 3. Default 4. Core2
Taos_Web2	1. Taos_Web2 2. Taos_Web2_Helper 3. Core2 4. Default
Taos_Web_Helper	1. Taos_Web_Helper 2. Default 3. Core2

Domain	Failover domains
Taos_Web2_Helper	1. Taos_Web2_Helper 2. Core2 3. Default
Taos_Website	1. Taos_Website 2. Default 3. Core2
Taos_OA	1. Taos_OA 2. Taos_Web 3. Taos_Web2 4. Default 5. Core2

Chapter 5: Interaction Center multi-site deployment scenarios

This section includes scenarios of sample deployments for an Interaction Center system with two sites. These scenarios estimate an average system load for a site with fewer than 1,200 agents. If your plan includes an Interaction Center site with a high system load, or more than 1,200 agents, you must adapt the deployment scenario.



Tip:
The deployment scenarios show only one Event Collector Bridge for each Resource Manager server. However, redundancy requires a minimum of two Event Collector Bridges for each Resource Manager server.

This section includes the following scenarios:

- Scenario 8: Two sites, voice only on page 124
- Scenario 9: Two sites, multi-channel on page 133
- Scenario 10: Single instance Business Advocate for two sites, multi-channel on page 145
- Scenario 11: Multi-instance Business Advocate for two sites, multi-channel on page 152
- Scenario 13: Two sites, multi-channel, data center on page 160
- Scenario 14: Business Advocate for two sites, multi-channel, data center on page 170

Note:
Scenario 12 is removed because it is invalid, as it needs a single computer in Site-2 and the IC environment does not allow running two WACD servers across sites. The scenarios are not renumbered, so as to avoid confusion for users who are upgrading from previous versions of Interaction Center.

If your Interaction Center system includes an integration with Siebel, see *Avaya IC for Siebel Integration* guide.

For more information about how to adapt these deployment scenarios, see Adapting deployment scenarios on page 79.

Scenario 8: Two sites, voice only

This scenario is the recommended minimum configuration for a basic multi-site, voice-media only deployment in a contact center. If you customize your Telephony deployment, you may need to include additional computers and Interaction Center components.

Topics for this scenario include:

- Scenario 8: Deployment overview on page 124
- Scenario 8: Interaction Center domain overview on page 125
- Scenario 8: Site overview on page 125
- Scenario 8: Partitioning of Interaction Center servers on page 126
- Scenario 8: Failover strategy on page 128

Scenario 8: Deployment overview

This scenario shows a potential production system with the following deployment:

- Voice channel only (no other media channels).
- Two sites (London and Chicago) connected by a WAN.
- Two computers at each site for your Interaction Center servers.
- One computer at each site for OA Event Collector server and Real-time subsystem.
- One computer for IC Manager, Database Designer, and Workflow Designer.
- Three computers at each site to host Webconnector for Avaya Agent Web Client (optional).
- Three computers at each site to host Tomcat for Client SDK and/or Web Services (optional).
- One or more agent desktop computers.
- One computer for SMTP and POP / IMAP servers.
- One computer for your RDBMS.

  Tip:
  You can locate the RDBMS computer in the London LAN with WAN access from Chicago, or at a third site with WAN access from London and Chicago. If you deploy one of these options, host the Data servers on computers that are local to the RDBMS. This scenario assumes that the RDBMS computer is in London.

- Hardware redundancy.

- Server (VESP) failover.

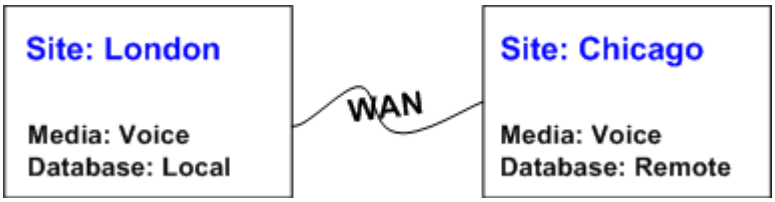
Scenario 8: Interaction Center domain overview

This scenario includes two sites: London and Chicago. The following table shows the Interaction Center domains in each site. The Default domain is used in both sites for failover.

Site 1 – London	Site 2 – Chicago
• London_User1 • London_User2 • London_Voice1 • London_Voice1_Helper • London_Voice2 • London_Voice2_Helper • London_Prompter1 • London_Prompter2 • Default • London_Core2 • London_Data1 • London_Data2 • London_OA	• Chicago_User1 • Chicago_User2 • Chicago_Voice1 • Chicago_Voice1_Helper • Chicago_Voice2 • Chicago_Voice2_Helper • Chicago_Prompter1 • Chicago_Prompter2 • Chicago_Core1 • Chicago_Core2 • Chicago_OA

Scenario 8: Site overview

The following diagram shows the primary characteristics of the London and Chicago sites.



Scenario 8: Partitioning of Interaction Center servers

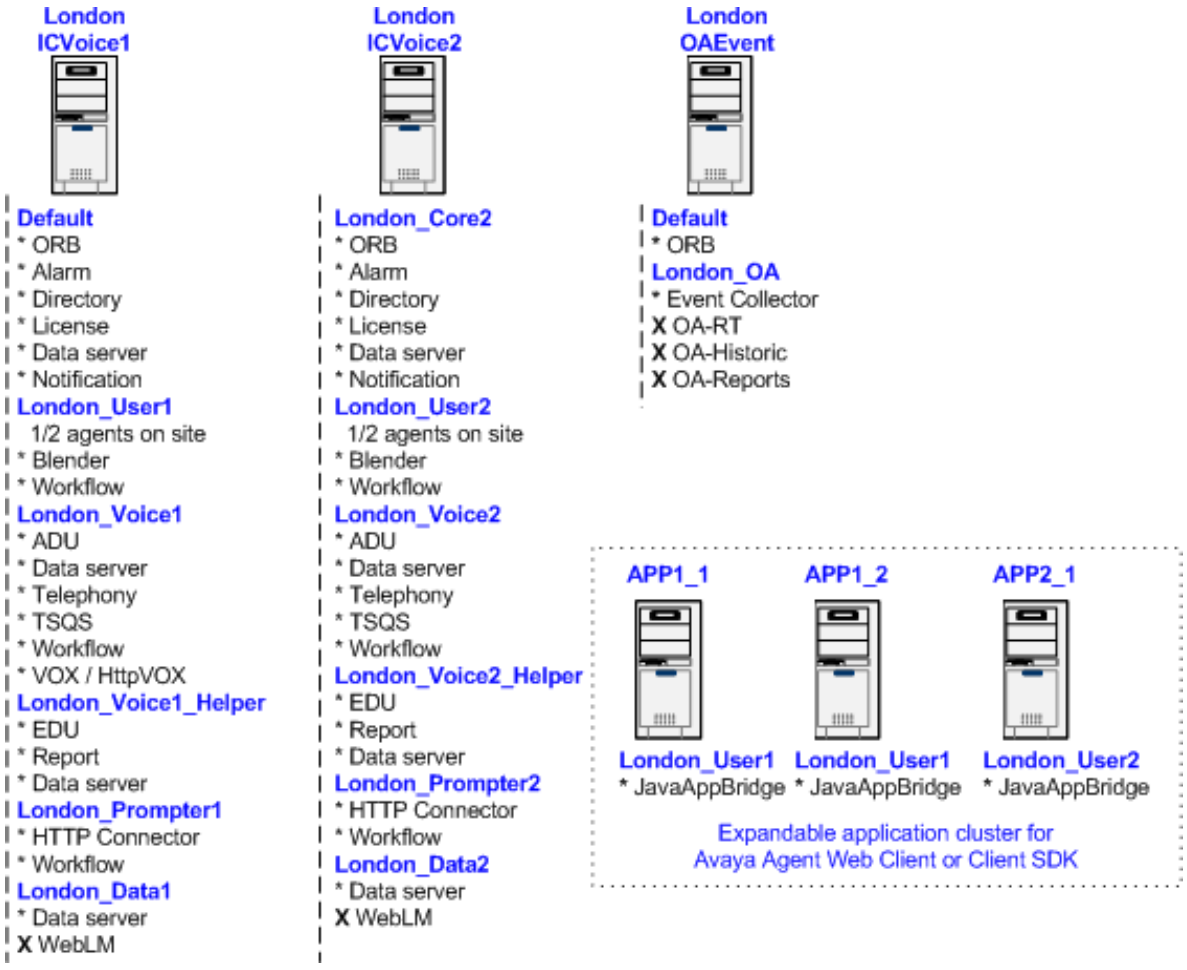
The physical partitioning of the servers reflects the distribution of the Interaction Center and OA components on the servers. The logical partitioning reflects the distribution of servers and agents across the Interaction Center domains.

This section includes the following topics:

- Partitioning at London site on page 126
- Partitioning at Chicago site on page 127

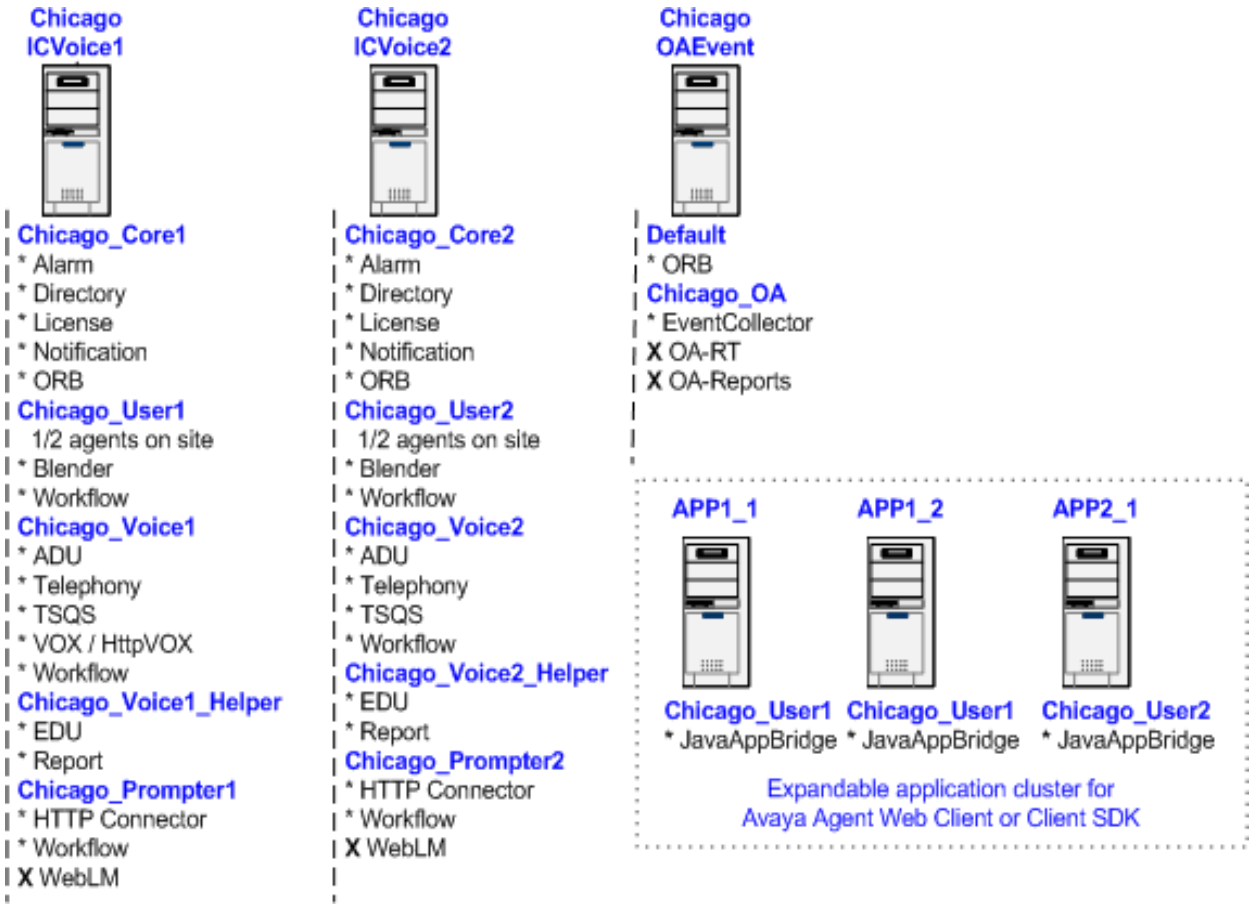
Partitioning at London site

The following figure shows the distribution of components on the servers at the London site. An **X** before a component indicates that component is installed on the computer, but does not belong to an Interaction Center domain.



Partitioning at Chicago site

The following figure shows the distribution of components on the servers at the Chicago site. An **X** before a component indicates that the component is installed on the computer, but does not belong to an Interaction Center domain.



Scenario 8: Failover strategy

The topics in this section are:

- Failover strategy at London site on page 128
- Failover strategy at Chicago site on page 131

Failover strategy at London site

The following table shows the failover strategy for the London site in this example. The components in the domain in the left column failover to the domains in the right column in the order listed.

Domain	Failover domains
London_User1	1. London_User1 2. London_User2 3. London_Prompter1 4. London_Prompter2 5. Default 6. London_Core2 7. London_Voice1 8. London_Voice1_Helper 9. London_Voice2 10.London_Voice2_Helper
London_User2	1. London_User2 2. London_User1 3. London_Prompter2 4. London_Prompter1 5. London_Core2 6. Default 7. London_Voice2 8. London_Voice2_Helper 9. London_Voice1 10.London_Voice1_Helper

Domain	Failover domains
London_Voice1	1. London_Voice1 2. London_Voice1_Helper 3. London_Voice2 4. London_Voice2_Helper 5. Default 6. London_Core2
London_Voice1_Helper	1. London_Voice1_Helper 2. London_Voice2_Helper 3. Default 4. London_Core2
London_Voice2	1. London_Voice2 2. London_Voice2_Helper 3. London_Voice1 4. London_Voice1_Helper 5. London_Core2 6. Default
London_Voice2_Helper	1. London_Voice2_Helper 2. London_Voice1_Helper 3. London_Core2 4. Default
London_Prompter1	1. London_Prompter1 2. London_Prompter2 3. Default 4. London_Core2 5. London_Voice1 6. London_Voice1_Helper 7. London_Voice2 8. London_Voice2_Helper
London_Prompter2	1. London_Prompter2 2. London_Prompter1 3. London_Core2 4. Default 5. London_Voice2 6. London_Voice2_Helper 7. London_Voice1 8. London_Voice1_Helper

Domain	Failover domains
London_OA	1. London_OA 2. London_Voice1 3. London_Voice1_Helper 4. London_Voice2 5. London_Voice2_Helper 6. Default 7. London_Core2
London_Data1	1. London_Data1 2. Default 3. London_Core2
London_Data2	1. London_Data2 2. Default 3. London_Core2
Default	1. Default 2. London_Core2
London_Core2	1. London_Core2 2. Default

Failover strategy at Chicago site

The following table shows the failover strategy for the Chicago site in this example. The components in the domain in the left column failover to the domains in the right column in the order listed.

Domain	Failover domains
Chicago_User1	1. Chicago_User1 2. Chicago_User2 3. Chicago_Prompter1 4. Chicago_Prompter2 5. London_Data1 6. London_Data2 7. Chicago_Voice1 8. Chicago_Voice1_Helper 9. Chicago_Voice2 10.Chicago_Voice2_Helper 11.Chicago_Core1 12.Chicago_Core2
Chicago_User2	1. Chicago_User2 2. Chicago_User1 3. Chicago_Prompter2 4. Chicago_Prompter1 5. London_Data2 6. London_Data1 7. Chicago_Voice2 8. Chicago_Voice2_Helper 9. Chicago_Voice1 10.Chicago_Voice1_Helper 11.Chicago_Core2 12.Chicago_Core1
Chicago_Voice1	1. Chicago_Voice1 2. Chicago_Voice1_Helper 3. Chicago_Voice2 4. Chicago_Voice2_Helper 5. London_Data1 6. London_Data2 7. Chicago_Core1 8. Chicago_Core2

Domain	Failover domains
Chicago_Voice1_Helper	1. Chicago_Voice1_Helper 2. Chicago_Voice2_Helper 3. Chicago_Core1 4. Chicago_Core2 5. London_Data1 6. London_Data2
Chicago_Voice2	1. Chicago_Voice2 2. Chicago_Voice2_Helper 3. Chicago_Voice1 4. Chicago_Voice1_Helper 5. London_Data2 6. London_Data1 7. Chicago_Core2 8. Chicago_Core1
Chicago_Voice2_Helper	1. Chicago_Voice2_Helper 2. Chicago_Voice1_Helper 3. Chicago_Core2 4. Chicago_Core1 5. London_Data1 6. London_Data2
Chicago_Prompter1	1. Chicago_Prompter1 2. Chicago_Prompter2 3. London_Data1 4. London_Data2 5. Chicago_Core1 6. Chicago_Core2 7. Chicago_Voice1 8. Chicago_Voice1_Helper 9. Chicago_Voice2 10.Chicago_Voice2_Helper

Domain	Failover domains
Chicago_Prompter2	1. Chicago_Prompter2 2. Chicago_Prompter1 3. London_Data2 4. London_Data1 5. Chicago_Core2 6. Chicago_Core1 7. Chicago_Voice2 8. Chicago_Voice2_Helper 9. Chicago_Voice1 10.Chicago_Voice1_Helper
Chicago_OA	1. Chicago_OA 2. Chicago_Voice1 3. Chicago_Voice1_Helper 4. Chicago_Voice2 5. Chicago_Voice2_Helper 6. Chicago_Core1 7. Chicago_Core2
Chicago_Core1	1. Chicago_Core1 2. Chicago_Core2 3. Default 4. London_Core2
Chicago_Core2	1. Chicago_Core2 2. Chicago_Core1 3. London_Core2 4. Default

Scenario 9: Two sites, multi-channel

This scenario is the recommended minimum configuration for a basic multi-site, multi-channel deployment. This scenario includes two sites: York and Paris. This configuration combines the following previous scenarios:

- York: Scenario 1: Single site, voice only on page 82
- Paris: Scenario 4: Single site, multi-channel on page 96

In this scenario, you add Email and Web domains to the end of the York agent lists to bridge the York agent pools to Paris for non-voice channels. If you customize your multi-site, multi-channel deployment, you may need to include additional computers and Interaction Center components.

Topics for this scenario include:

- Scenario 9: Deployment overview on page 134
- Scenario 9: Interaction Center domain overview on page 135
- Scenario 9: Site overview on page 135
- Scenario 9: Partitioning of servers on page 136
- Scenario 9: Failover strategy on page 138

Scenario 9: Deployment overview

This scenario shows a potential production system with the following deployment:

- All media channels.
- Two sites connected by a WAN.
- Two computers for Interaction Center Telephony components at York.
- Seven computers for all other Interaction Center components at Paris.
- One computer at each site for OA Event Collector server and Real-time subsystem.
- One computer for IC Manager, Database Designer, and Workflow Designer.
- One computer for the website and Web-related servers in the network DMZ.
- Three computers at each site to host Webconnector for Avaya Agent Web Client (optional).
- Three computers at each site to host Tomcat for Client SDK and/or Web Services (optional).
- One or more agent desktop computers.
- One computer for SMTP and POP / IMAP servers.
- One computer for your RDBMS.

  Tip:
  You can locate the RDBMS computer in the Paris LAN with WAN access from York, or at a third site with WAN access from York and Paris. This scenario assumes that the RDBMS computer is in Paris with database replication in York.

- Hardware redundancy.
- Server (VESP) failover.
- One cluster for each Poller, ICEMail and WACD servers respectively.

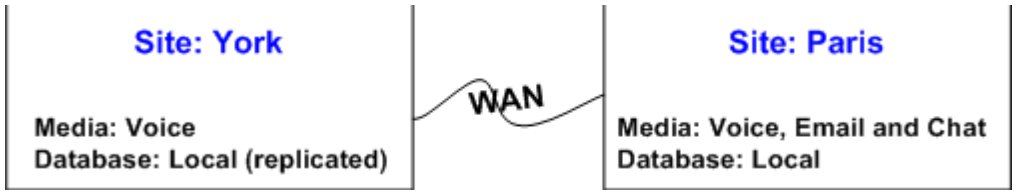
Scenario 9: Interaction Center domain overview

This scenario includes two sites: York and Paris. The following table shows the Interaction Center domains in each site. The default domain is used in both sites for failover.

Site 1 – York	Site 2 – Paris
• York_User1 • York_User2 • York_Voice1 • York_Voice1_Helper • York_Voice2 • York_Voice2_Helper • York_Prompter1 • York_Prompter2 • York_Core1 • York_Core2 • York_OA	• Paris_User1 • Paris_User2 • Paris_Voice1 • Paris_Voice1_Helper • Paris_Voice2 • Paris_Voice2_Helper • Paris_Prompter1 • Paris_Prompter2 • Default • Paris_Core2 • Paris_Web • Paris_Web_Helper • Paris_Email • Paris_Email_Helper • Paris_Web2 • Paris_Web2_Helper • Paris_Email2 • Paris_Email2_Helper • Paris_Website • Paris_OA

Scenario 9: Site overview

The following diagram shows the primary characteristics of the York and Paris sites:



Scenario 9: Partitioning of servers

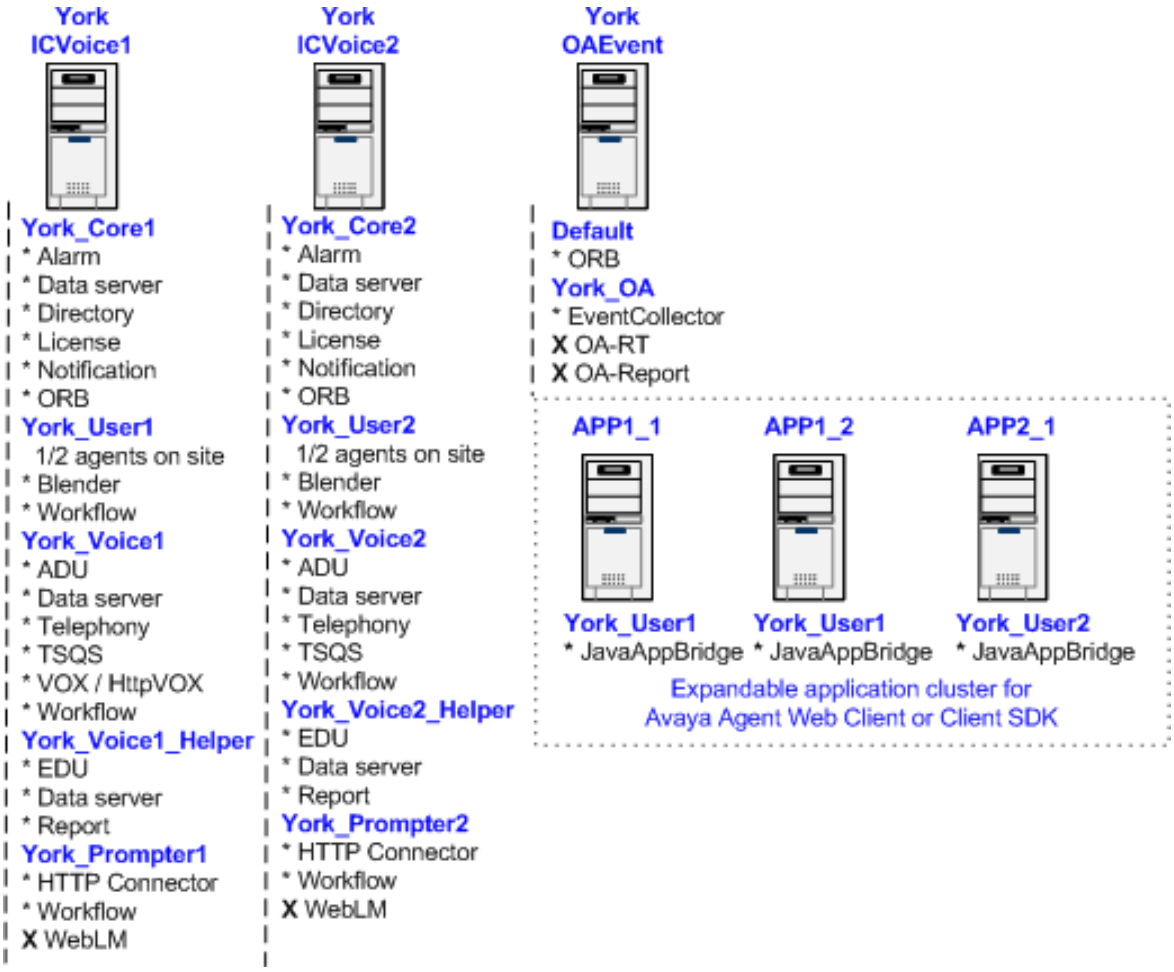
The physical partitioning of the servers reflects the distribution of the Interaction Center and OA components on the servers. The logical partitioning reflects the distribution of servers and agents across the Interaction Center domains.

This section includes the following topics:

- Partitioning at York site on page 136
- Partitioning at Paris site on page 137

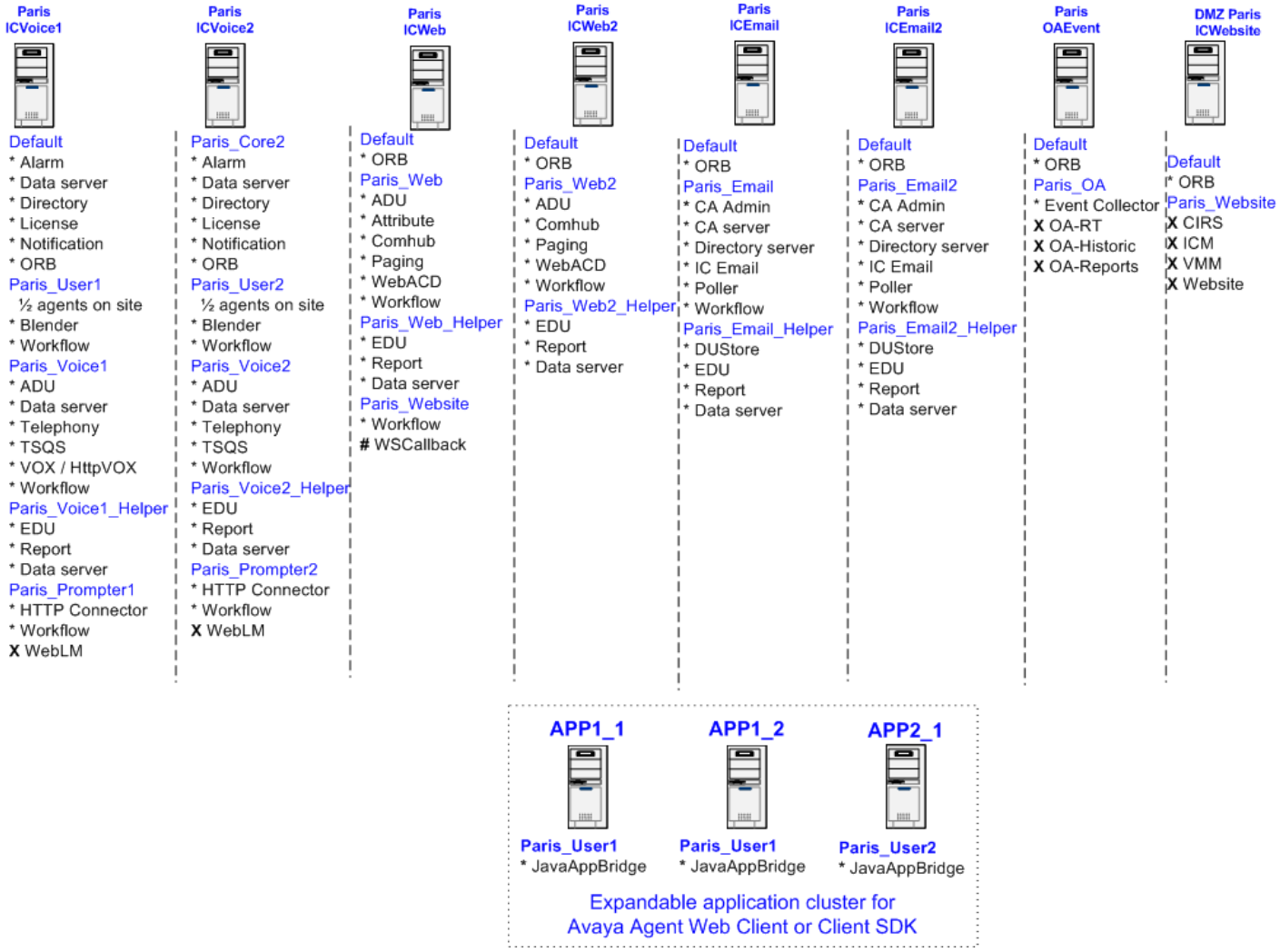
Partitioning at York site

The following figure shows the distribution of components on the servers at the York site. An **X** before a component indicates that component is installed on the computer, but does not belong to an Interaction Center domain.



Partitioning at Paris site

The following figure shows the distribution of components on the servers at the Paris site. An **X** indicates that component is installed on the computer, but does not belong to an Interaction Center domain. A # indicates that the component is installed only if the optional Avaya Agent Web Client or Client SDK components in the dotted-line box are not installed.



Scenario 9: Failover strategy

This section includes the following topics:

- Failover strategy at York site on page 138
- Failover strategy at Paris site on page 141

Failover strategy at York site

The following table shows the failover strategy at the York site in this example. The components in the domain in the left column failover to the domains in the right column in the order listed.

Domain	Failover domains
York_User1	1. York_User1 2. York_User2 3. York_Prompter1 4. York_Prompter2 5. York_Core1 6. York_Core2 7. Default 8. Paris_Core2 9. York_Voice1 10.York_Voice1_Helper 11.York_Voice2 12.York_Voice2_Helper 13.Paris_Email 14.Paris_Email_Helper 15.Paris_Email2 16.Paris_Email2_Helper 17.Paris_Web 18.Paris_Web2 19.Paris_Web_Helper 20.Paris_Web2_Helper

Domain	Failover domains
York_User2	1. York_User2 2. York_User1 3. York_Prompter2 4. York_Prompter1 5. York_Core2 6. York_Core1 7. Paris_Core2 8. Default 9. York_Voice2 10.York_Voice2_Helper 11.York_Voice1 12.York_Voice1_Helper 13.Paris_Email 14.Paris_Email_Helper 15.Paris_Email2 16.Paris_Email2_Helper 17.Paris_Web 18.Paris_Web_Helper 19.Paris_Web2 20.Paris_Web2_Helper
York_Voice1	1. York_Voice1 2. York_Voice1_Helper 3. York_Voice2 4. York_Voice2_Helper 5. York_Core1 6. York_Core2 7. Default 8. Paris_Core2
York_Voice1_Helper	1. York_Voice1_Helper 2. York_Voice2_Helper 3. York_Core1 4. York_Core2 5. Default 6. Paris_Core2

Domain	Failover domains
York_Voice2	1. York_Voice2 2. York_Voice2_Helper 3. York_Voice1 4. York_Voice1_Helper 5. York_Core2 6. York_Core1 7. Paris_Core2 8. Default
York_Voice2_Helper	1. York_Voice2_Helper 2. York_Voice1_Helper 3. York_Core2 4. York_Core1 5. Paris_Core2 6. Default
York_Prompter1	1. York_Prompter1 2. York_Prompter2 3. York_Core1 4. York_Core2 5. York_Voice1 6. York_Voice2 7. Default 8. Paris_Core2
York_Prompter2	1. York_Prompter2 2. York_Prompter1 3. York_Core2 4. York_Core1 5. York_Voice2 6. York_Voice1 7. Paris_Core2 8. Default
York_OA	1. York_OA 2. York_Voice1 3. York_Voice2 4. York_Core1 5. York_Core2

Domain	Failover domains
York_Core1	1. York_Core1 2. York_Core2 3. Default 4. Paris_Core2
York_Core2	1. York_Core2 2. York_Core1 3. Paris_Core2 4. Default

Failover strategy at Paris site

The following table shows the failover strategy at the Paris site in this example. The components in the domain in the left column failover to the domains in the right column in the order listed.

Domain	Failover domains
Paris_User1	1. Paris_User1 2. Paris_User2 3. Paris_Prompter1 4. Paris_Prompter2 5. Default 6. Paris_Core2 7. Paris_Voice1 8. Paris_Voice1_Helper 9. Paris_Voice2 10.Paris_Voice2_Helper 11.Paris_Web 12.Paris_Web_Helper 13.Paris_Web2 14.Paris_Web2_Helper 15.Paris_Email 16.Paris_Email_Helper 17.Paris_Email2 18.Paris_Email2_Helper

Domain	Failover domains
Paris_User2	1. Paris_User2 2. Paris_User1 3. Paris_Prompter2 4. Paris_Prompter1 5. Paris_Core2 6. Default 7. Paris_Voice2 8. Paris_Voice2_Helper 9. Paris_Voice1 10.Paris_Voice1_Helper 11.Paris_Web 12.Paris_Web_Helper 13.Paris_Web2 14.Paris_Web2_Helper 15.Paris_Email 16.Paris_Email_Helper 17.Paris_Email2 18.Paris_Email2_Helper
Paris_Voice1	1. Paris_Voice1 2. Paris_Voice1_Helper 3. Paris_Voice2 4. Paris_Voice2_Helper 5. Default 6. Paris_Core2
Paris_Voice1_Helper	1. Paris_Voice2_Helper 2. Paris_Voice1_Helper 3. Default 4. Paris_Core2
Paris_Voice2	1. Paris_Voice2 2. Paris_Voice2_Helper 3. Paris_Voice1 4. Paris_Voice1_Helper 5. Paris_Core2 6. Default

Domain	Failover domains
Paris_Voice2_Helper	1. Paris_Voice2_Helper 2. Paris_Voice1_Helper 3. Paris_Core2 4. Default
Paris_Prompter1	1. Paris_Prompter1 2. Paris_Prompter2 3. Default 4. Paris_Core2 5. Paris_Voice1 6. Paris_Voice1_Helper 7. Paris_Voice2 8. Paris_Voice2_Helper
Paris_Prompter2	1. Paris_Prompter2 2. Paris_Prompter1 3. Paris_Core2 4. Default 5. Paris_Voice2 6. Paris_Voice2_Helper 7. Paris_Voice1 8. Paris_Voice1_Helper
Default	1. Default 2. Paris_Core2
Paris_Core2	1. Paris_Core2 2. Default
Paris_Email	1. Paris_Email 2. Paris_Email_Helper 3. Default 4. Paris_Core2 **Note:** In case you modify the Analyze Workflow to access the ADU server, you need to modify Email domain failover sequence to have a domain that has an ADU server.

Domain	Failover domains
Paris_Email2	1. Paris_Email2 2. Paris_Email2_Helper 3. Paris_Core2 4. Default **Note:** In case you modify the Analyze Workflow to access the ADU server, you need to modify Email domain failover sequence to have a domain that has an ADU server.
Paris_Email_Helper	1. Paris_Email_Helper 2. Default 3. Paris_Core2
Paris_Email2_Helper	1. Paris_Email2_Helper 2. Paris_Core2 3. Default
Paris_Web	1. Paris_Web 2. Paris_Web_Helper 3. Default 4. Paris_Core2 **Note:** If you do not configure the Event Collector server to monitor the ADU server in this domain, configure the server groups on the **Advanced** tab as follows: Paris_Web: Priority Value = 1
Paris_Web_Helper	1. Paris_Web_Helper 2. Default 3. Paris_Core2
Paris_Web2	1. Paris_Web2 2. Paris_Web2_Helper 3. Paris_Core2 4. Default **Note:** If you do not configure the Event Collector server to monitor the ADU server in this domain, configure the server groups on the **Advanced** tab as follows: Paris_Web2: Priority Value = 1
Paris_Web2_Helper	1. Paris_Web2_Helper 2. Paris_Core2 3. Default

Domain	Failover domains
Paris_Website	1. Paris_Website 2. Paris_Web 3. Paris_Web2 4. Paris_Voice1 5. Paris_Voice1_Helper 6. Default 7. Paris_Core2
Paris_OA	1. Paris_OA 2. Paris_Voice1 3. Paris_Voice1_Helper 4. Paris_Voice2 5. Paris_Voice2_Helper 6. Default 7. Paris_Core2

Scenario 10: Single instance Business Advocate for two sites, multi-channel

This scenario extends Scenario 9: Two sites, multi-channel on page 133 to include Business Advocate. This scenario is the recommended minimum configuration to add one instance of Business Advocate to a basic multi-site, multi-channel deployment in a contact center. If you customize your multi-channel deployment, you might need to include additional computers and Interaction Center components.

Note:

This scenario uses the same Workflow servers as Scenario 9: Two sites, multi-channel on page 133. However, to function with Business Advocate, these Workflow servers must run the Business Advocate workflows to qualify and transfer contacts.

A single instance of Business Advocate indicates that the Interaction Center system includes only one Logical Resource Manager for Business Advocate. For more information about Logical Resource Managers, see *IC Business Advocate Configuration and Administration Guide*.

Topics for this scenario include:

- Scenario 10: Deployment overview on page 146
- Scenario 10: Interaction Center domain overview on page 147
- Scenario 10: Site overview on page 148
- Scenario 10: Partitioning of Business Advocate servers on page 148
- Scenario 10: Failover strategy for Business Advocate domains on page 151

Scenario 10: Deployment overview

This scenario adds Business Advocate servers to some of the computers that host Interaction Center servers, described in Scenario 9: Deployment overview on page 134. This scenario also adds two computers to host the Resource Manager server and the other Interaction Center servers in the Paris domain.

If you host Interaction Center and OA databases in DB2 on AIX, this scenario requires the following:

- A Windows or Oracle Solaris computer to host the Business Advocate databases. If required, you can install SQL Server on a computer that hosts a Resource Manager server.
- An additional Data server on the same computer as a Resource Manager server. This Data server provides Interaction Center with access to the Business Advocate database and data, such as service classes. Configure this Data server in its own domain, such as RM_Data. Add the RM_Data domain to the failover path for all domains that include Directory servers and Workflow servers that run contact qualification workflows.

Scenario 10: Interaction Center domain overview

This scenario includes two sites: York and Paris. The Business Advocate servers in this scenario are distributed across the following Interaction Center domains including those listed in Scenario 9: Interaction Center domain overview on page 135.

The following table shows the Interaction Center domains in each site:

Site 1 – York	Site 2 – Paris
• York_User1 • York_User2 • York_Voice1 • York_Voice1_Helper • York_Voice2 • York_Voice2_Helper • York_Prompter1 • York_Prompter2 • York_Core1 • York_Core2 • York_OA	• Paris_User1 • Paris_User2 • Paris_Voice1 • Paris_Voice1_Helper • Paris_Voice2 • Paris_Voice2_Helper • Paris_Prompter1 • Paris_Prompter2 • Default • Paris_Core2 • Paris_Website • Paris_OA • Paris_RM1 • Paris_RM2 • Paris_RM_Helper1 • Paris_RM_Helper2 • Paris_Web • Paris_Web_Helper • Paris_Email • Paris_Email_Helper • Paris_Web2 • Paris_Web2_Helper • Paris_Email2 • Paris_Email2_Helper

Scenario 10: Site overview

The following diagram shows the primary characteristics of the York and Paris sites:



Scenario 10: Partitioning of Business Advocate servers

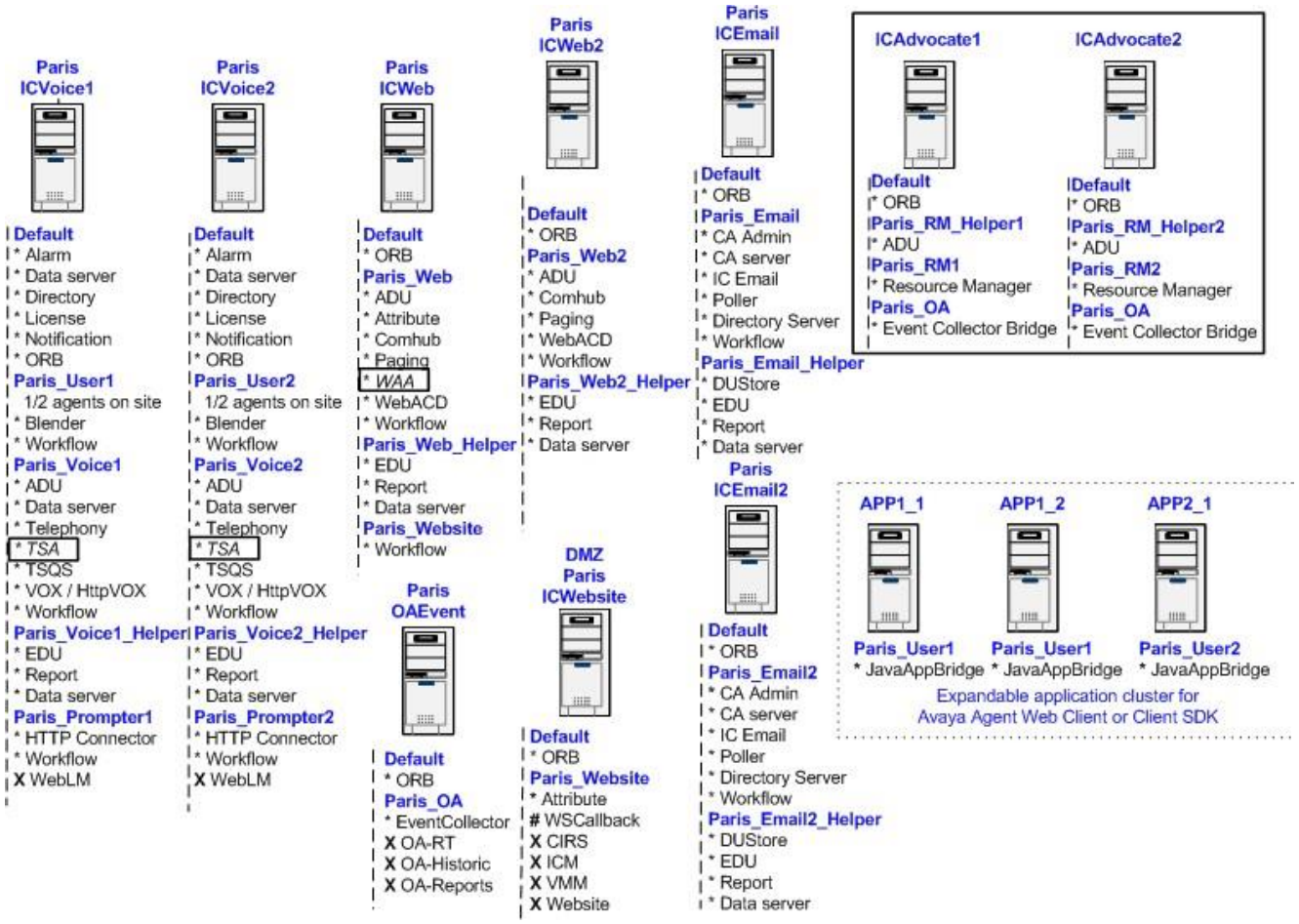
The physical partitioning of the servers reflects the distribution of the Business Advocate components on the servers. The logical partitioning reflects the distribution of servers and agents across the Interaction Center domains.

This section includes the following topics:

- Partitioning of Business Advocate servers at Paris site on page 149
- Partitioning of Business Advocate servers at York site on page 150

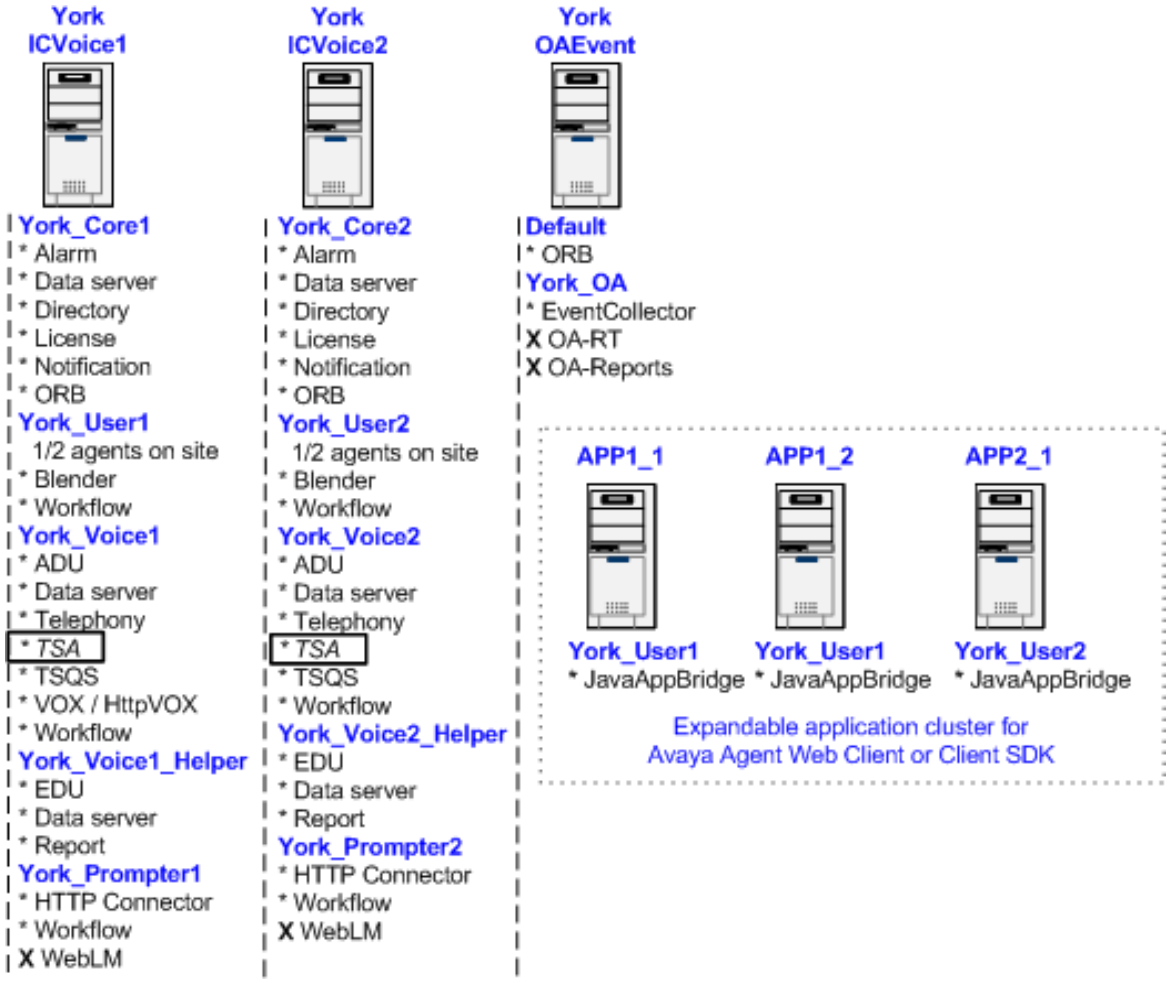
Partitioning of Business Advocate servers at Paris site

The following figure shows the distribution of Business Advocate servers on the servers at the Paris site. The highlighted servers are in addition to those components described in Scenario 9: Partitioning of servers on page 136.



Partitioning of Business Advocate servers at York site

The following figure shows the distribution of Business Advocate servers on the servers at the York site. The highlighted servers are in addition to those components described in Scenario 9: Partitioning of servers on page 136.



Scenario 10: Failover strategy for Business Advocate domains

Business Advocate has some unique failover strategies for the Resource Manager and the voice channel. For details about those strategies, see *IC Business Advocate Configuration and Administration Guide*.

The following table shows the failover strategy for the Business Advocate domains in this example. The Business Advocate domains do not failover to any of the other Interaction Center domains. The components in the domain in the left column failover to the domains in the right column in the order listed. For failover information for the domains not listed in this table, see Scenario 9: Failover strategy on page 138.

Domain	Failover domains
Paris_RM_Helper1	1. Paris_RM_Helper1 2. Default 3. Paris_Core2
Paris_RM_Helper2	1. Paris_RM_Helper2 2. Default 3. Paris_Core2
Paris_RM1	1. Paris_RM1 2. Paris_RM_Helper1 3. Paris_RM_Helper2 4. Default 5. Paris_Core2
Paris_RM2	1. Paris_RM2 2. Paris_RM_Helper1 3. Paris_RM_Helper2 4. Default 5. Paris_Core2
Paris_OA	1. Paris_OA 2. Paris_Voice1 3. Paris_Voice1_Helper 4. Paris_Voice2 5. Paris_Voice2_Helper 6. Default 7. Paris_Core2

Scenario 11: Multi-instance Business Advocate for two sites, multi-channel

This scenario extends Scenario 9: Two sites, multi-channel on page 133 to include Business Advocate. This scenario is the recommended minimum configuration to add two instances of Business Advocate to a basic multi-site, multi-channel deployment in a contact center. If you customize your multi-channel deployment, you might need to include additional computers and Interaction Center components.

Note:

This scenario uses the same Workflow servers as Scenario 9: Two sites, multi-channel on page 133. However, to correctly run with Business Advocate, these Workflow servers must run the Business Advocate workflows to qualify and transfer contacts.

Multi-instance Business Advocate indicates that the Interaction Center system includes more than one Logical Resource Manager for Business Advocate. Each Logical Resource Manager handles a separate population of agents.

You can configure a Logical Resource Manager:

- For groups of agents across all sites who handle specific types of contacts.
- For agents in each site.

You must not configure a Logical Resource Manager for each Telephony switch in an Interaction Center system.

For more information about Logical Resource Managers, see *IC Business Advocate Configuration and Administration Guide*.

Topics for this scenario include:

- Scenario 11: Deployment overview on page 153
- Scenario 11: Interaction Center domain overview on page 154
- Scenario 11: Site overview on page 155
- Scenario 11: Partitioning of Business Advocate servers on page 155
- Scenario 11: Failover strategy for Business Advocate domains on page 158

Scenario 11: Deployment overview

Use this deployment in the following circumstances:

- To provide on-site physical redundancy.
- To configure Business Advocate for a contact center that exceeds the capacities of a single instance of Business Advocate.

This scenario does not prevent delivery of contacts to another site. If you want to prevent delivery of contacts to another site, you must create a qualifier to represent each site. For more information about qualifiers, see *IC Business Advocate Configuration and Administration Guide*.

This scenario adds Business Advocate servers to some of the computers that host Interaction Center servers, described in Scenario 9: Deployment overview on page 134. This scenario also adds two computers at each site to host a Resource Manager server and an ADU server.

If you host Interaction Center and OA databases in DB2 on AIX, this scenario also requires the following:

- A Windows or Oracle Solaris computer to host the Business Advocate databases. If required, you can install SQL Server on a computer that hosts a Resource Manager server.
- An additional Data server on the same computer as a Resource Manager server. This Data server provides Interaction Center with access to the Business Advocate database and data, such as service classes. Configure this Data server in its own domain, such as RM_Data. Add the RM_Data domain to the failover path for all domains that include Directory servers and Workflow servers that run contact qualification workflows.

Scenario 11: Interaction Center domain overview

This scenario includes two sites: York and Paris. The Business Advocate servers in this scenario are distributed across the following Interaction Center domains including those listed in Scenario 9: Interaction Center domain overview on page 135.

The following table shows the Interaction Center domains in each site:

Site 1 – York	Site 2 – Paris
• York_User1 • York_User2 • York_Voice1 • York_Voice1_Helper • York_Voice2 • York_Voice2_Helper • York_Prompter1 • York_Prompter2 • York_Core1 • York_Core2 • York_OA • York_RM1 • York_RM2 • York_RM_Helper1 • York_RM_Helper2	• Paris_User1 • Paris_User2 • Paris_Voice1 • Paris_Voice1_Helper • Paris_Voice2 • Paris_Voice2_Helper • Paris_Prompter1 • Paris_Prompter2 • Default • Paris_Core2 • Paris_Website • Paris_OA • Paris_RM1 • Paris_RM2 • Paris_RM_Helper1 • Paris_RM_Helper2 • Paris_Web • Paris_Web_Helper • Paris_Email • Paris_Email_Helper • Paris_Web2 • Paris_Web2_Helper • Paris_Email2 • Paris_Email2_Helper

Scenario 11: Site overview

The following diagram shows the primary characteristics of the York and Paris sites:



Scenario 11: Partitioning of Business Advocate servers

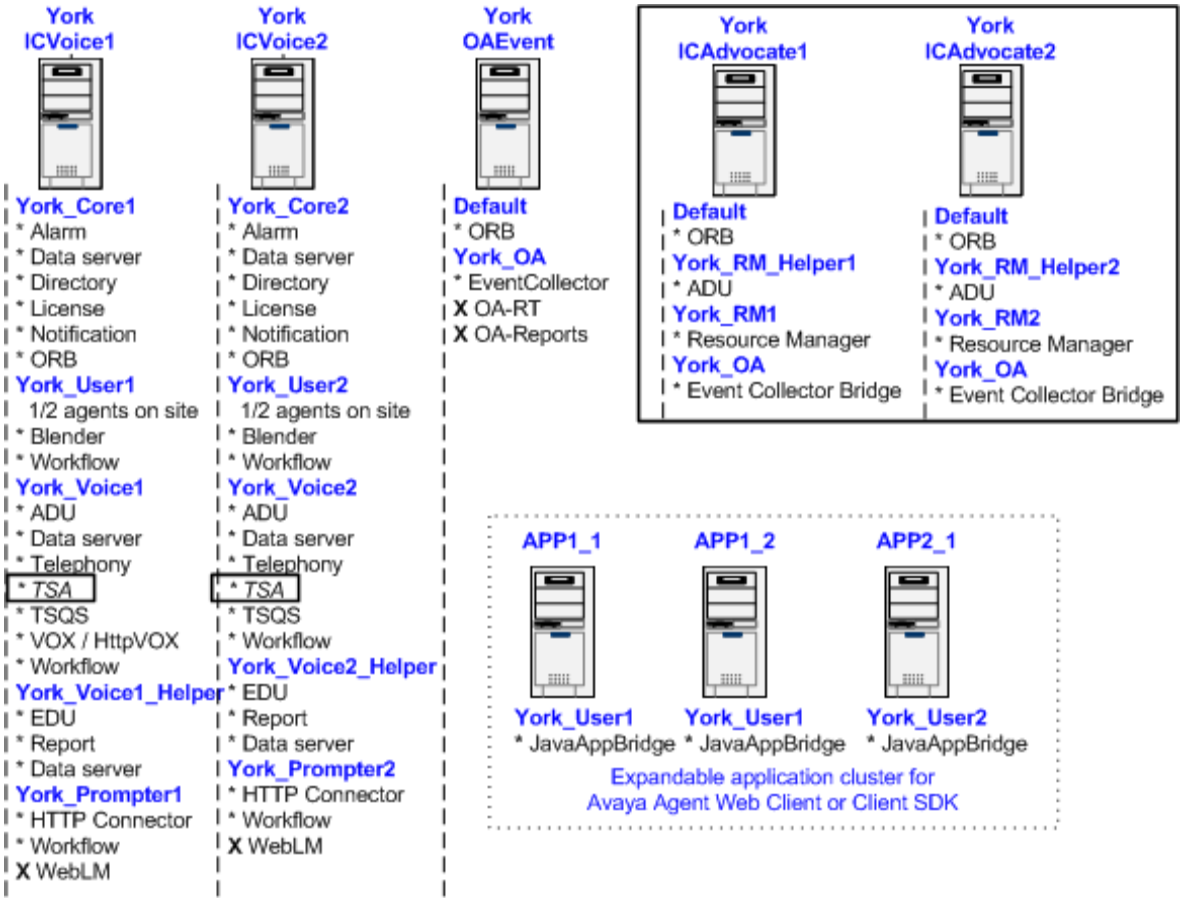
The physical partitioning of the servers reflects the distribution of the Business Advocate components on the servers. The logical partitioning reflects the distribution of servers and agents across the Interaction Center domains.

This section includes the following topics:

- Partitioning of Business Advocate servers at York site on page 156
- Partitioning of Business Advocate servers at Paris site on page 157

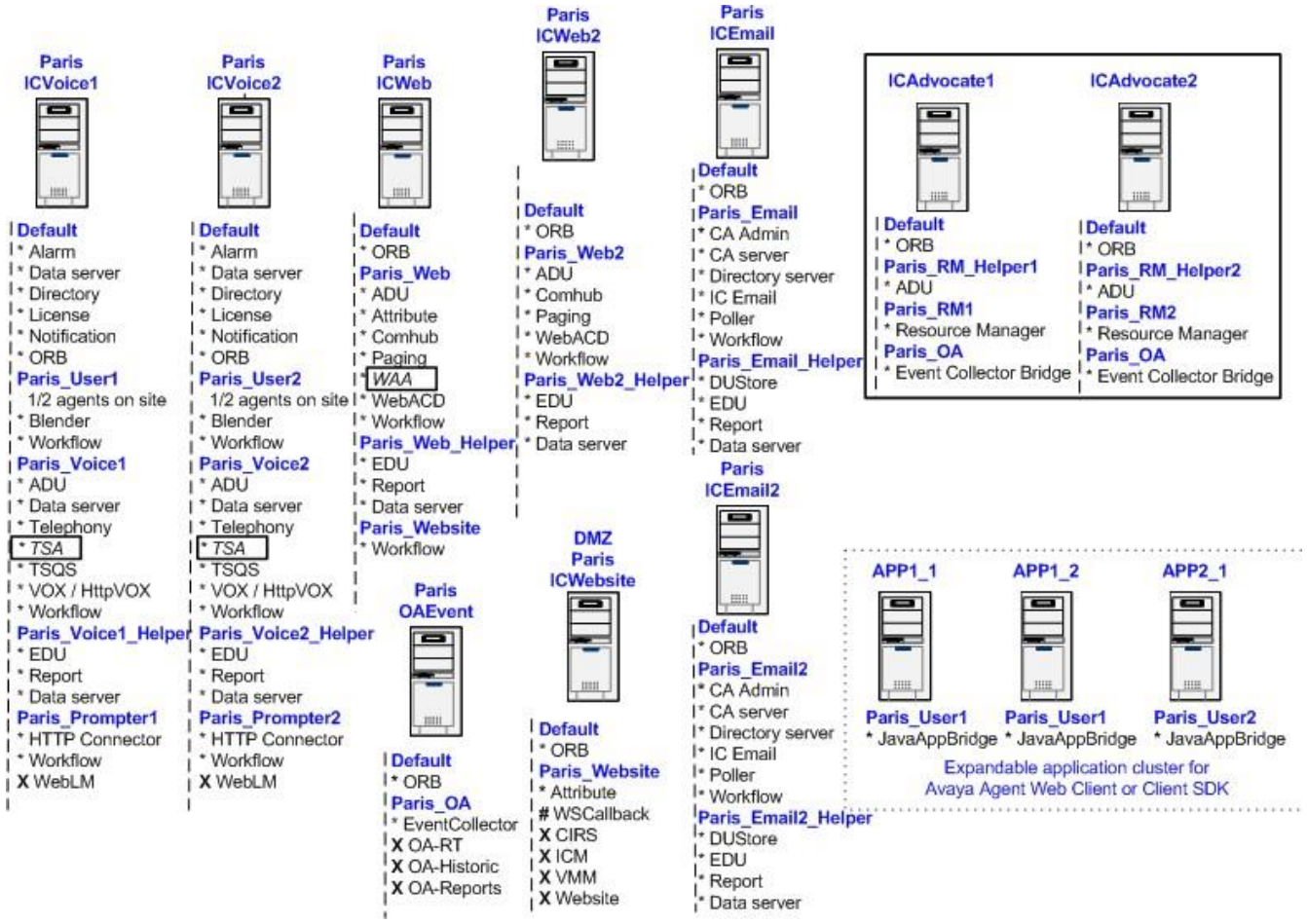
Partitioning of Business Advocate servers at York site

The following figure shows the distribution of Business Advocate servers on the servers at the York site. The highlighted servers are in addition to those components described in Scenario 9: Partitioning of servers on page 136.



Partitioning of Business Advocate servers at Paris site

The following figure shows the distribution of Business Advocate servers on the servers at the Paris site. The highlighted servers are in addition to those components described in Scenario 9: Partitioning of servers on page 136.



Scenario 11: Failover strategy for Business Advocate domains

Business Advocate has some unique failover strategies for the Resource Manager and the voice channel. For details about those strategies, see *IC Business Advocate Configuration and Administration Guide*.

This section includes the following topics:

- Failover strategy at York site on page 158
- Failover strategy at Paris site on page 159

Failover strategy at York site

The following table shows the failover strategy for the Business Advocate domains at the York site in this example. The Business Advocate domains do not failover to any of the other Interaction Center domains. The components in the domain in the left column failover to the domains in the right column in the order listed. For failover information for the domains not listed in this table, see Scenario 9: Failover strategy on page 138.

Domain	Failover domains
York_RM_Helper1	1. York_RM_Helper1 2. York_Core1 3. York_Core2
York_RM_Helper2	1. York_RM_Helper2 2. York_Core2 3. York_Core1
York_RM1	1. York_RM1 2. York_RM_Helper1 3. York_RM_Helper2 4. York_Core1 5. York_Core2

Domain	Failover domains
York_RM2	1. York_RM2 2. York_RM_Helper1 3. York_RM_Helper2 4. York_Core2 5. York_Core1
York_OA	1. York_OA 2. York_Voice1 3. York_Voice1_Helper 4. York_Voice2 5. York_Voice2_Helper 6. York_Core2 7. York_Core1

Failover strategy at Paris site

The following table shows the failover strategy for the Business Advocate domains at the Paris site in this example. The Business Advocate domains do not failover to any of the other Interaction Center domains. The components in the domain in the left column failover to the domains in the right column in the order listed. For failover information for the domains not listed in this table, see Scenario 9: Failover strategy on page 138.

Domain	Failover domains
Paris_RM_Helper1	1. Paris_RM_Helper1 2. Default 3. Paris_Core2
Paris_RM_Helper2	1. Paris_RM_Helper2 2. Default 3. Paris_Core2
Paris_RM1	1. Paris_RM1 2. Paris_RM_Helper1 3. Paris_RM_Helper2 4. Default 5. Paris_Core2

Domain	Failover domains
Paris_RM2	1. Paris_RM2 2. Paris_RM_Helper1 3. Paris_RM_Helper2 4. Default 5. Paris_Core2
Paris_OA	1. Paris_OA 2. Paris_Voice1 3. Paris_Voice1_Helper 4. Paris_Voice2 5. Paris_Voice2_Helper 6. Default 7. Paris_Core2

Scenario 13: Two sites, multi-channel, data center

This scenario is a modification of Scenario 9: Two sites, multi-channel on page 133 to include a single data center. Both sites access the data center.

In this scenario, the site with the data center includes the RDBMS, all Data servers, the Event Collector server, Web servers, and Email servers. The data center does not support agents or Voice servers. The second site includes all agents and Voice servers. You can deploy several satellite sites with the same configuration, but different domains, as the second site.

To implement a data center, the WAN connection between the sites must have sufficient bandwidth and must always be available to prevent any disruption to service that a single site dependency can cause.

Topics for this scenario include:

- Scenario 13: Deployment overview on page 161
- Scenario 13: Interaction Center domain overview on page 162
- Scenario 13: Site overview on page 162
- Scenario 13: Partitioning of servers on page 162
- Scenario 13: Failover strategy on page 165

Scenario 13: Deployment overview

This scenario shows a potential production system with the following deployment:

- All media channels.
- Two sites connected by a WAN.
- Eight computers for the data center, Web components, and Email components at the Paris site.
- Two computers for agent services and Voice components at the York site.
- One computer for the OA Event Collector server and Real-time subsystem at each site.
- One computer for IC Manager, Database Designer, and Workflow Designer.
- One computer for the website and Web-related servers at the Paris site, in the network DMZ.
- Three computers at each site to host Webconnector for Avaya Agent Web Client (optional).
- Three computers at each site to host Tomcat for Client SDK and/or Web Services (optional).
- One or more agent desktop computers.
- One computer for SMTP and POP / IMAP servers.
- One computer for your RDBMS at the Paris site.
- Hardware redundancy.
- Server (VESP) failover.
- One cluster for each Poller, ICEMail and WACD servers respectively.

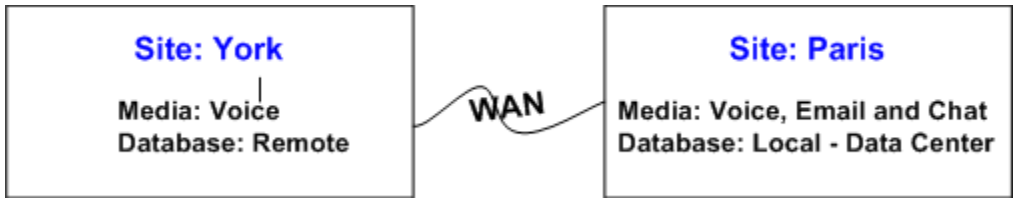
Scenario 13: Interaction Center domain overview

This scenario includes two sites: York and Paris. The following table shows the Interaction Center domains in each site. The default domain is used in both sites for failover.

Site 1 – Paris	Site 2 – York
• Default • Paris_Core2 • Paris_Website • Paris_Data1 • Paris_Data2 • Paris_OA • Paris_Web • Paris_Web_Helper • Paris_Email • Paris_Email_Helper • Paris_Web2 • Paris_Web2_Helper • Paris_Email2 • Paris_Email2_Helper	• York_Core1 • York_Core2 • York_User1 • York_User2 • York_Voice1 • York_Voice1_Helper • York_Voice2 • York_Voice2_Helper • York_Prompter1 • York_Prompter2 • York_OA

Scenario 13: Site overview

The following diagram shows the primary characteristics of the York and Paris sites:



Scenario 13: Partitioning of servers

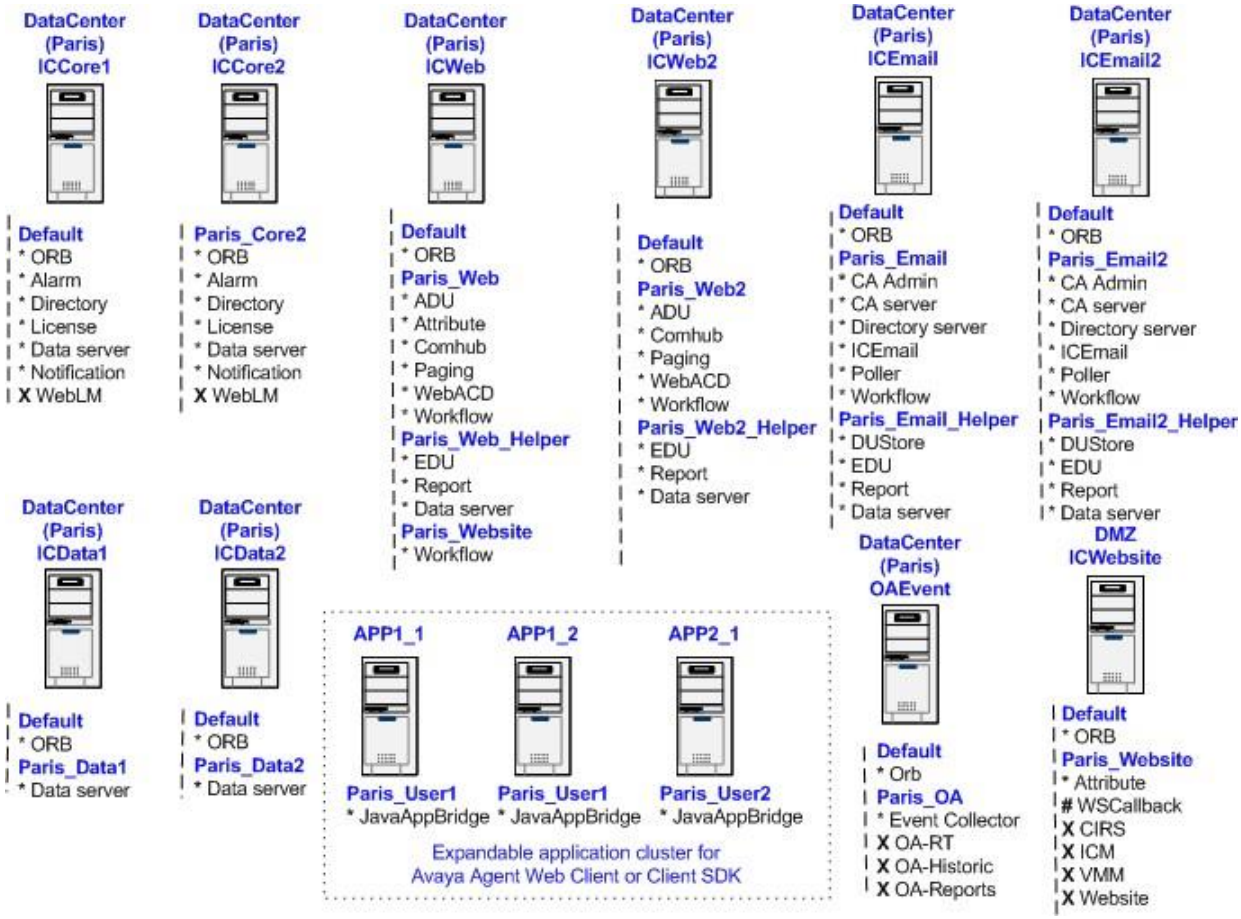
The physical partitioning of the servers reflects the distribution of the Interaction Center and OA components on the servers. The logical partitioning reflects the distribution of servers and agents across the Interaction Center domains.

This section includes the following topics:

- Partitioning at Paris site on page 163
- Partitioning at York site on page 164

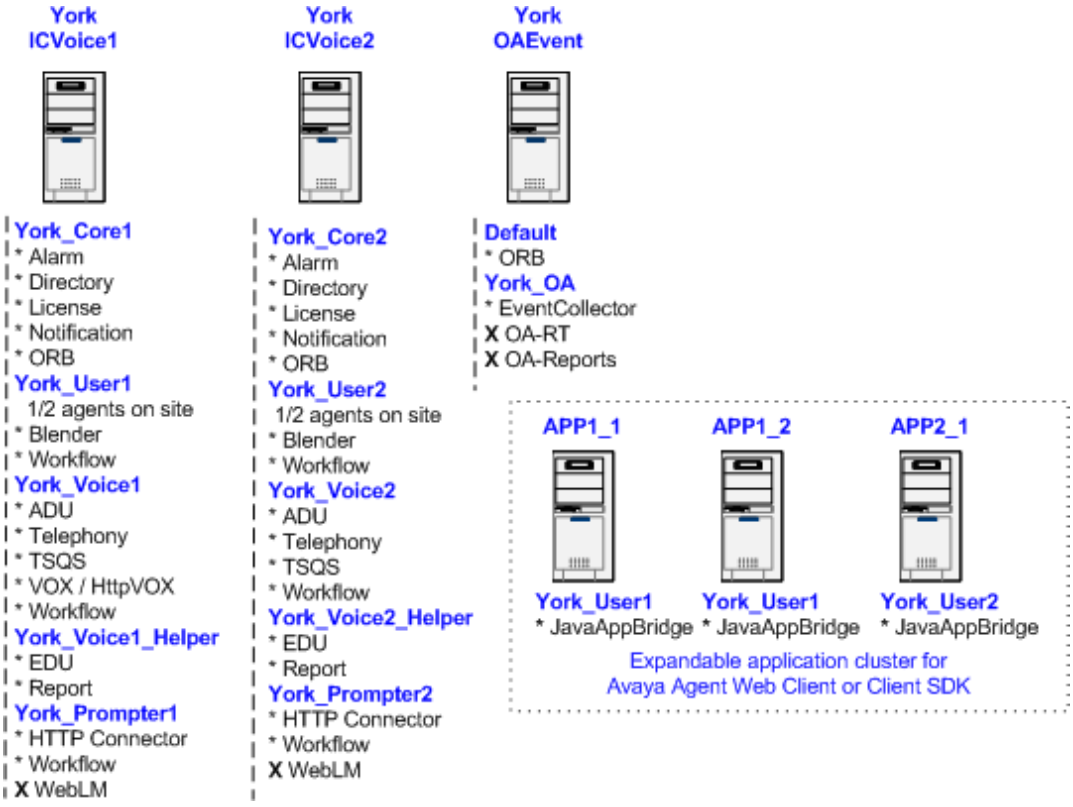
Partitioning at Paris site

The following figure shows the distribution of components on the servers at the Paris site. An **X** indicates that component is installed on the computer, but does not belong to an Interaction Center domain. A # indicates that component is installed only if the optional Avaya Agent Web Client or Client SDK components in the dotted-line box are not installed.



Partitioning at York site

The following figure shows the distribution of components on the servers at the York site. An **X** before a component indicates that component is installed on the computer, but does not belong to an Interaction Center domain.



Comments on this document? infodev@avaya.com

Scenario 13: Failover strategy

This section includes the following topics:

- Failover strategy at York site on page 138
- Failover strategy at Paris site on page 141

Failover strategy at Paris site

The following table shows the failover strategy at the Paris site in this example. The components in the domain in the left column failover to the domains in the right column in the order listed.

Domain	Failover domains
Default	1. Default 2. Paris_Core2
Paris_Core2	1. Paris_Core2 2. Default
Paris_Data1	1. Paris_Data1 2. Default 3. Paris_Core2
Paris_Data2	1. Paris_Data2 2. Paris_Core2 3. Default
Paris_Email	1. Paris_Email 2. Paris_Email_Helper 3. Default 4. Paris_Core2 **Note:** In case you modify the Analyze Workflow to access the ADU server, you need to modify Email domain failover sequence to have a domain that has an ADU server.
Paris_Email2	1. Paris_Email2 2. Paris_Email2_Helper 3. Default 4. Paris_Core2 **Note:** In case you modify the Analyze Workflow to access the ADU server, you need to modify Email domain failover sequence to have a domain that has an ADU server.

Domain	Failover domains
Paris_Email_Helper	1. Paris_Email_Helper 2. Default 3. Paris_Core2
Paris_Email2_Helper	1. Paris_Email2_Helper 2. Default 3. Paris_Core2
Paris_Web	1. Paris_Web 2. Paris_Web_Helper 3. Default 4. Paris_Core2 **Note:** If you do not configure the Event Collector server to monitor the ADU server in this domain, configure the server groups on the **Advanced** tab as follows: Paris_Web: Priority Value = 1
Paris_Web2	1. Paris_Web2 2. Paris_Web2_Helper 3. Default 4. Paris_Core2 **Note:** If you do not configure the Event Collector server to monitor the ADU server in this domain, configure the server groups on the **Advanced** tab as follows: Paris_Web2: Priority Value = 1
Paris_Web_Helper	1. Paris_Web_Helper 2. Default 3. Paris_Core2
Paris_Web2_Helper	1. Paris_Web2_Helper 2. Default 3. Paris_Core2
Paris_Website	1. Paris_Website 2. Paris_Web 3. York_Voice1 4. York_Voice1_Helper 5. Default 6. Paris_Core2
Paris_OA	1. Paris_OA 2. Paris_Web 3. Default 4. Paris_Core2

Failover strategy at York site

The following table shows the failover strategy at the York site in this example. The components in the domain in the left column failover to the domains in the right column in the order listed.

Domain	Failover domains
York_Core1	1. York_Core1 2. York_Core2 3. Paris_Data1 4. Paris_Data2
York_Core2	1. York_Core2 2. York_Core1 3. Paris_Data2 4. Paris_Data1
York_User1	1. York_User1 2. York_User2 3. York_Prompter1 4. York_Prompter2 5. Paris_Data1 6. Paris_Data2 7. York_Voice1 8. York_Voice1_Helper 9. York_Voice2 10.York_Voice2_Helper 11.York_Core1 12.York_Core2 13.Paris_Email_Helper 14.Paris_Email2_Helper 15.Paris_Web 16.Paris_Web_Helper 17.Paris_Web2 18.Paris_Web2_Helper

Domain	Failover domains
York_User2	1. York_User2 2. York_User1 3. York_Prompter2 4. York_Prompter1 5. Paris_Data2 6. Paris_Data1 7. York_Voice2 8. York_Voice2_Helper 9. York_Voice1 10.York_Voice1_Helper 11.York_Core2 12.York_Core1 13.Paris_Email_Helper 14.Paris_Email2_Helper 15.Paris_Web 16.Paris_Web_Helper 17.Paris_Web2 18.Paris_Web2_Helper
York_Voice1	1. York_Voice1 2. York_Voice1_Helper 3. York_Voice2 4. York_Voice2_Helper 5. York_Core1 6. York_Core2 7. Paris_Data1 8. Paris_Data2
York_Voice1_Helper	1. York_Voice1_Helper 2. York_Voice2_Helper 3. York_Core1 4. York_Core2 5. Paris_Data1 6. Paris_Data2

Domain	Failover domains
York_Voice2	1. York_Voice2 2. York_Voice2_Helper 3. York_Voice1 4. York_Voice1_Helper 5. York_Core2 6. York_Core1 7. Paris_Data2 8. Paris_Data1
York_Voice2_Helper	1. York_Voice2_Helper 2. York_Voice1_Helper 3. York_Core2 4. York_Core1 5. Paris_Data2 6. Paris_Data1
York_Prompter1	1. York_Prompter1 2. York_Prompter2 3. York_Core1 4. York_Core2 5. Paris_Data1 6. Paris_Data2 7. York_Voice1 8. York_Voice1_Helper 9. York_Voice2 10.York_Voice2_Helper

Domain	Failover domains
York_Prompter2	1. York_Prompter2 2. York_Prompter1 3. York_Core2 4. York_Core1 5. Paris_Data2 6. Paris_Data1 7. York_Voice2 8. York_Voice2_Helper 9. York_Voice1 10.York_Voice1_Helper
York_OA	1. York_OA 2. York_Voice1 3. York_Voice1_Helper 4. York_Voice2 5. York_Voice2_Helper 6. York_Core1 7. York_Core2

Scenario 14: Business Advocate for two sites, multi-channel, data center

This scenario is a modification of Scenario 13: Two sites, multi-channel, data center on page 160 to include Business Advocate. Both sites access the data center.

A single instance of Business Advocate indicates that the Interaction Center system includes only one Logical Resource Manager for Business Advocate. This Logical Resource Manager can monitor all agents in the network and select a qualified, available agent for a contact.

Note:

This scenario uses the same Workflow servers as Scenario 13: Two sites, multi-channel, data center on page 160. However, to correctly run with Business Advocate, these Workflow servers must run the Business Advocate workflows to qualify and transfer contacts.

In this scenario, the site with the data center includes the Business Advocate Logical Resource Manager, the RDBMS, all Data servers, the Event Collector server, Web servers, and Email servers. The data center does not support agents or Voice servers. The second site includes all agents and Voice servers. You can deploy several satellite sites with the same configuration, but different domains, as the second site.

To implement a data center, the WAN connection between the sites must have sufficient bandwidth and must always be available to prevent any disruption to service that a single site dependency can cause.

Topics for this scenario include:

- Scenario 14: Deployment overview on page 171
- Scenario 14: Interaction Center domain overview on page 172
- Scenario 14: Site overview on page 173
- Scenario 14: Partitioning of servers on page 173
- Scenario 14: Failover strategy on page 176

Scenario 14: Deployment overview

This scenario adds Business Advocate servers to some of the computers that host Interaction Center servers, described in Scenario 13: Two sites, multi-channel, data center on page 160. This scenario also adds two computers to host the Resource Manager servers and other Interaction Center servers in the Paris domain.

If you host Interaction Center and OA databases in DB2 on AIX, this scenario requires the following:

- A Windows or Oracle Solaris computer to host the Business Advocate databases. If required, you can install SQL Server on a computer that hosts a Resource Manager server.
- An additional Data server on the same computer as a Resource Manager server. This Data server will provide Interaction Center with access to the Business Advocate database and data, such as service classes. Configure this Data server in its own domain, such as RM_Data. Add the RM_Data domain to the failover path for all domains that include Directory servers and Workflow servers that run contact qualification workflows.

Scenario 14: Interaction Center domain overview

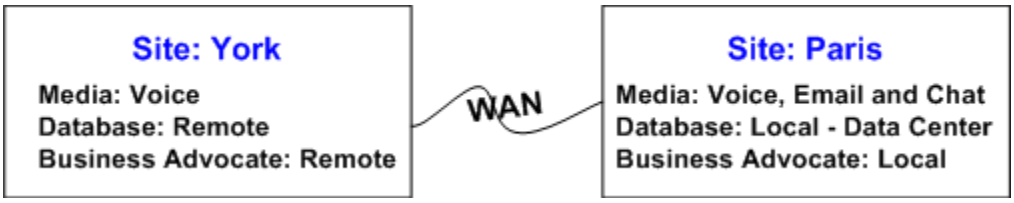
This scenario includes two sites: Paris and York. The Business Advocate servers in this scenario are distributed across the following Interaction Center domains including those listed in Scenario 13: Two sites, multi-channel, data center on page 160.

The following table shows the Interaction Center domains in each site. The highlighted domains were added to support Business Advocate. The following table shows the Interaction Center domains in each site. The default domain is used in both sites for failover.

Site 1 – Paris	Site 2 – York
• Default • Paris_Core2 • Paris_Web • Paris_Web_Helper • Paris_Email • Paris_Email_Helper • Paris_Web2 • Paris_Web2_Helper • Paris_Email2 • Paris_Email2_Helper • Paris_Website • Paris_Data1 • Paris_Data2 • Paris_OA • Paris_RM1 • Paris_RM2 • Paris_RM_Helper1 • Paris_RM_Helper2	• York_Core1 • York_Core2 • York_User1 • York_User2 • York_Voice1 • York_Voice1_Helper • York_Voice2 • York_Voice2_Helper • York_Prompter1 • York_Prompter2 • York_OA

Scenario 14: Site overview

The following diagram shows the primary characteristics of the York and Paris sites:



Scenario 14: Partitioning of servers

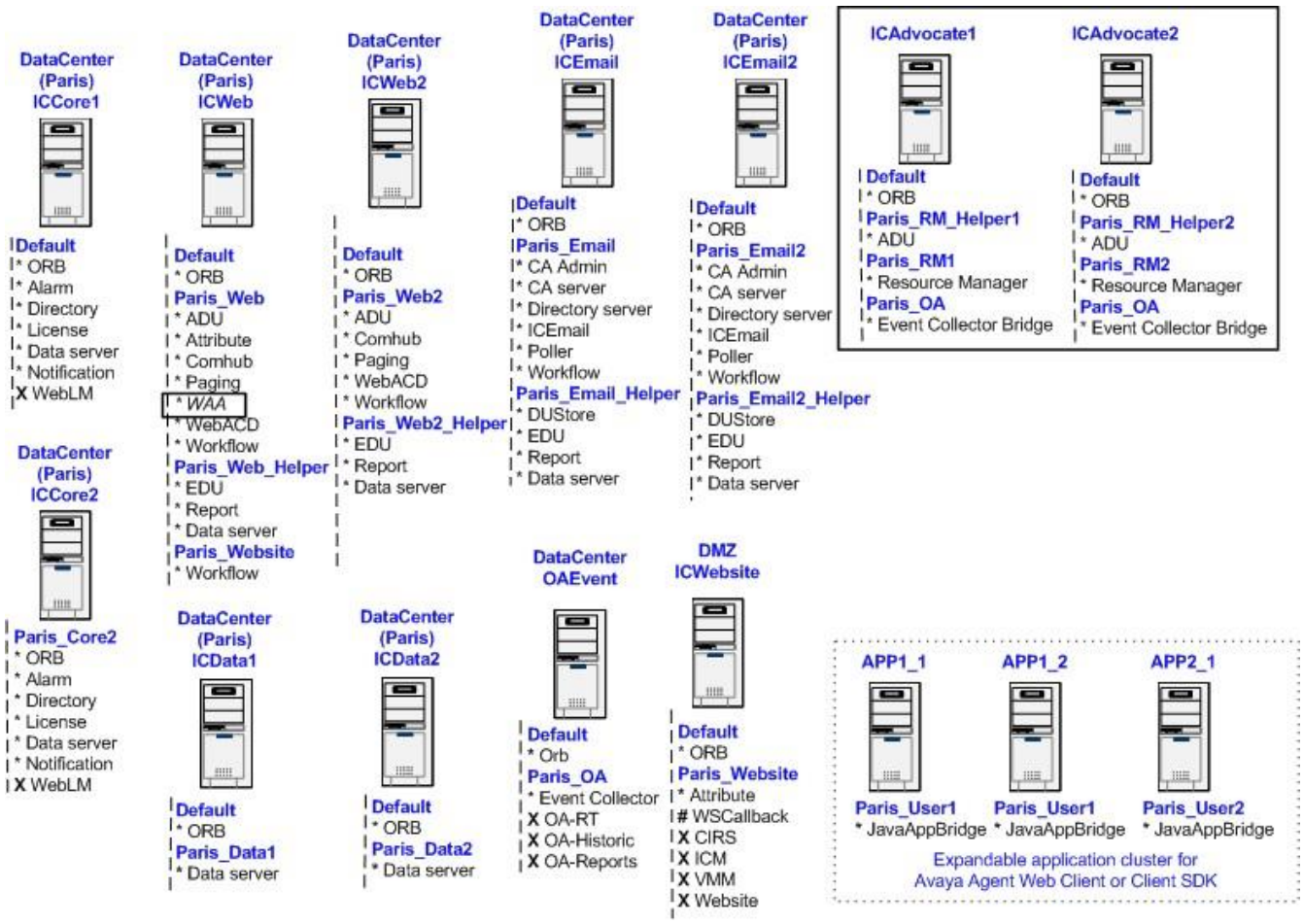
The physical partitioning of the servers reflects the distribution of the Interaction Center and OA components on the servers. The logical partitioning reflects the distribution of servers and agents across the Interaction Center domains.

This section includes the following topics:

- Partitioning at Paris site on page 174
- Partitioning at York site on page 175

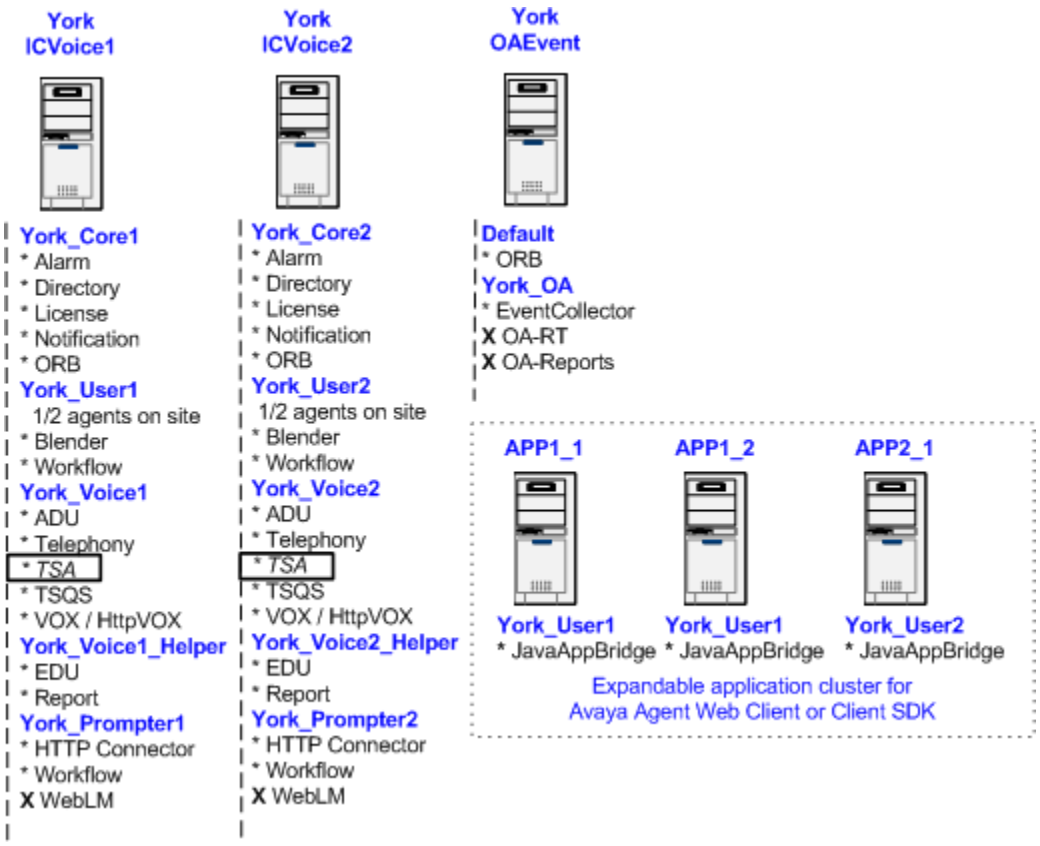
Partitioning at Paris site

The following figure shows the distribution of Business Advocate servers on the servers at the Paris site. The highlighted servers are in addition to those components described in Scenario 13: Partitioning of servers on page 162.



Partitioning at York site

The following figure shows the distribution of Business Advocate servers on the servers at the York site. The highlighted servers are in addition to those components described in Scenario 13: Partitioning of servers on page 162.



Scenario 14: Failover strategy

Business Advocate has some unique failover strategies for the Resource Manager and the voice channel. For details about those strategies, see *IC Business Advocate Configuration and Administration Guide*.

The following table shows the failover strategy for the Business Advocate domains in this example. The Business Advocate domains do not failover to any of the other Interaction Center domains. The components in the domain in the left column failover to the domains in the right column in the order listed. For failover information for the domains not listed in this table, see Scenario 13: Failover strategy on page 165.

Domain	Failover domains
Paris_RM1	1. Paris_RM1 2. Paris_RM2 3. Paris_RM_Helper1 4. Default 5. Paris_Core2
Paris_RM2	1. Paris_RM2 2. Paris_RM1 3. Paris_RM_Helper2 4. Default 5. Paris_Core2
Paris_RM_Helper1	1. Paris_RM_Helper1 2. Default 3. Paris_Core2
Paris_RM_Helper2	1. Paris_RM_Helper2 2. Default 3. Paris_Core2

Chapter 6: Avaya Agent Web Client server deployment scenarios

This section includes scenarios of sample deployments of the Avaya Agent Web Client software with Interaction Center 7.3.x. Avaya Agent Web Client provides a browser based application interface for the agents in your contact center. Agents access the interface by connecting to the Avaya Agent Web Client server through a Web browser. With the Java Application Bridge server, the Avaya Agent Web Client application can communicate with the Interaction Center servers.

You can use these deployment scenarios across multiple sites. All sites do not have to use the same deployment scenario. A site with a large agent population or a high availability requirement might require a cluster of WebConnectors with load balancing while a smaller branch site might only require a single computer to host Avaya Agent Web Client.

This section includes the following topics:

- Avaya Agent Web Client deployment guidelines on page 178
- Agent configuration guidelines on page 179
- Overview of deployment scenarios on page 180
- Basic deployment on page 180
- Load balancing deployment on page 182
- Multi-site deployment on page 187

Use these deployment scenarios with the following Interaction Center server deployments:

- Interaction Center single site deployment scenarios on page 79
- Interaction Center multi-site deployment scenarios on page 123

Avaya Agent Web Client deployment guidelines

The following guidelines apply for all Avaya Agent Web Client deployments:

- All WebConnector application servers that are part of the same cluster must be located at the same site.
- All computers that host WebConnector must be on the same subnet as the primary Interaction Center servers.

  For example, if a contact center has remote voice users, the computer that hosts WebConnector must be on the same subnet as the Interaction Center Telephony server. The Interaction Center Data server can be on a different subnet.
- If you require multiple instances of webclient, refer to Multi-site deployment on page 187
- All clients must be within the enterprise network security perimeter. Remote clients must be connected through a VPN.
- Avaya Agent Web Client supports SSL. Avaya Agent Web Client is able to use this support to provide encrypted communications between the browser-based application and the Avaya Agent Web Client process running on WebConnector.
- Proxy servers are not supported. Clients must have a direct connection to a HTTP server, or a load balancer. For load balancing a separate HTTP server needs to be installed on a separate system.
- Redundancy and failover are supported, but recovery is not transparent. Agents need to re-login following a failure.
- If Avaya Agent Web Client is installed on a system with other enterprise applications, you must consider the system capacity required to run all of the applications at the same time. If the system does not have sufficient capacity, it impacts the performance of Avaya Agent Web Client. For information on system requirements, see Requirements for Avaya Agent Web Client on page 309.
- For optimum performance, you must deploy the AAWC on a dedicated system.
- Do not run any other applications on the WebConnector server that hosts Avaya Agent Web Client. If you do, WebConnector could fail.
- The Java Application Bridge must be in an Interaction Center user domain. For more information, see *IC Installation and Configuration Guide* and *IC Administration Guide*.

Agent configuration guidelines

Agent configuration for all deployments: For all Avaya Agent Web Client deployments, agents must:

- Belong to a single domain only.
- Use the URL of a Network Dispatcher or HTTP Server which resides in that domain.

Agent configuration for a multi-site deployment: If you use this Avaya Agent Web Client deployment with a multi-site Interaction Center deployment, ensure that all agents who belong to one site can only reach a WebConnector server deployed on that site. For example, you can configure your system by having agents on different sites access the Avaya Agent Web Client from different URLs.

Overview of deployment scenarios

IC 7.3.x supports the following types of deployments:

- Basic
- Load balancing

The following table lists the main advantages and disadvantages for each type of deployment:

Note:
Additional points of failure could exist depending on your Interaction Center deployment.

Deployment type	Advantages	Disadvantages
Basic	• Appropriate for low volume or less than 500 users. • Easiest deployment to administer • Single computer solution	No redundancy to support failover recovery
Load balancing	• Inherits the benefits of the clustered deployment • No single point of failure for Avaya Agent Web Client.	• More complex configuration setup and administration • More hardware resources required

Basic deployment

The basic deployment is the simplest scenario.

This section includes the following topics:

- Overview of a basic deployment on page 180
- Overview of network structure for a basic deployment on page 181

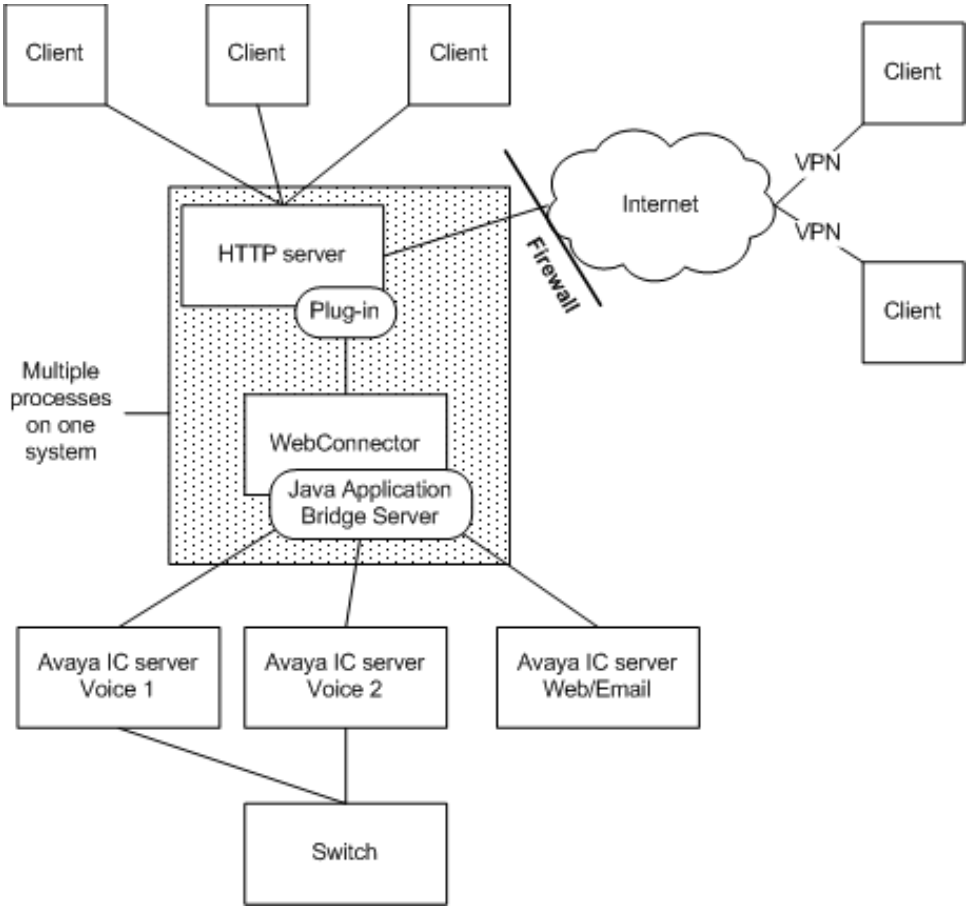
Overview of a basic deployment

The basic Avaya Agent Web Client server deployment scenario has a single computer installed with the HTTP server software. All network clients communicate to the WebConnector software through the HTTP server. Clients external to the business network must establish a VPN connection to the network.

The HTTP server software, WebConnector software, and the computer, on which the software is installed and running, are single points of failure. If any of these components stop functioning, some Interaction Center services are interrupted until normal operations are resumed. Avaya Agent Web Client services are interrupted if the WebConnector fails. New logins do not succeed if the HTTP server fails, but active sessions should be uninterrupted.

Overview of network structure for a basic deployment

The following diagram provides an overview of the network structure for a basic deployment:



Load balancing deployment

This section includes the following topics:

- Overview of a Load balancing deployment on page 182
- Benefits of a Load balancing deployment on page 182
- Overview of network structure for a load balancing deployment on page 183

Overview of a Load balancing deployment

The Load balancing Avaya Agent Web Client server deployment scenario has the WebConnector software installed and running on two computers with similar configurations.

A separate computer has the HTTP server software installed. The HTTP server loads balance between the different webConnectors. After the session has been created, no further interaction takes place between the client browser and HTTP server.

Benefits of a Load balancing deployment

With a Load balancing deployment, you can:

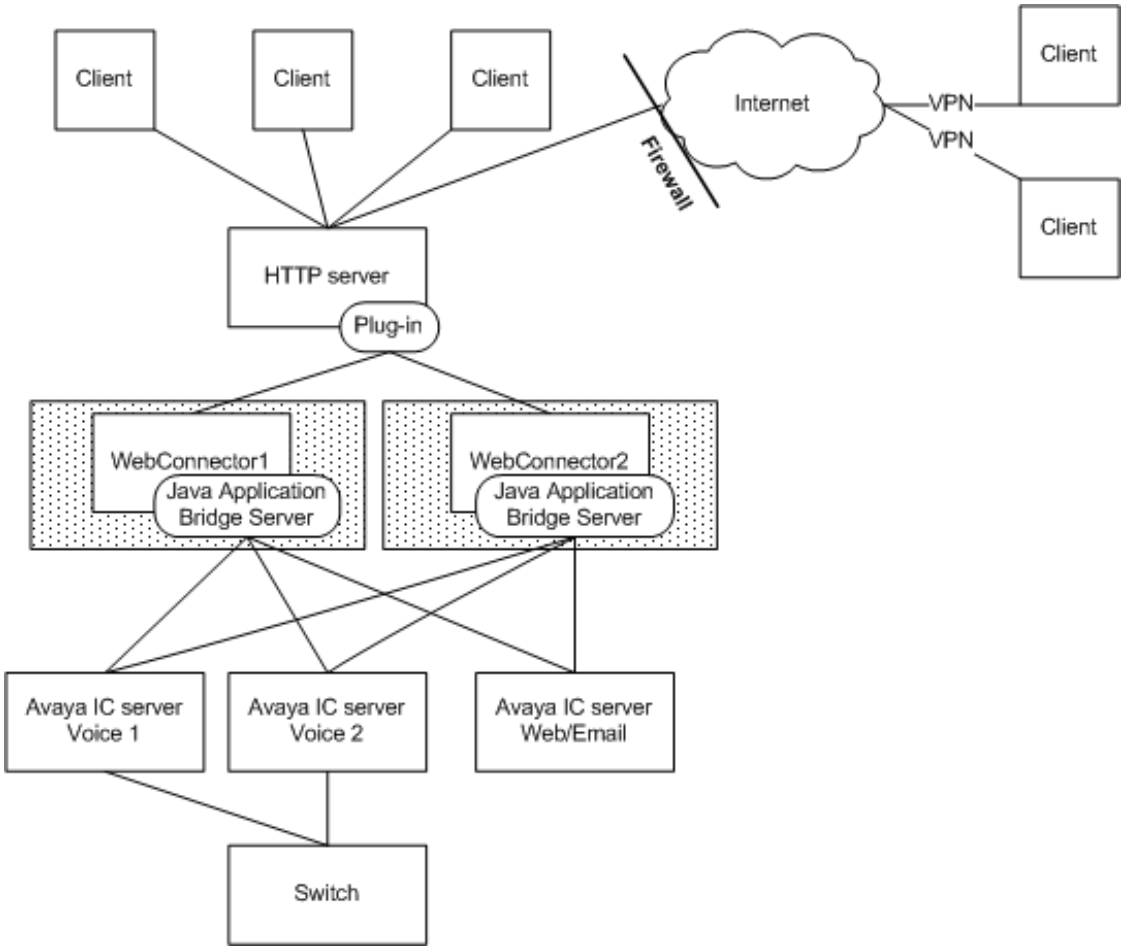
- Increase availability. If one WebConnector fails the second WebConnector can handle all the client requests.
- Improve scalability because load balancing is performed by the HTTP server at the beginning of each client session.

Note:

All client requests fail to WebConnector2 only if IC domain failover is not properly configured. For information on configuring domain failover, see *IC Installation and Configuration Guide* and *IC Administration Guide*

Overview of network structure for a load balancing deployment

The following diagram provides an overview of the network structure for a load balancing deployment:



Implementing Load Balancing with AAWC or SDK Clients

This section provides technical considerations relative to fronting Avaya Agent Web Client (AAWC) and Avaya Software Development Kit (SDK) with load balancing technology.

AIC 7.3 AAWC and SDK support distribution of client connections through the use of load balancers (LB). Avaya does not recommend any particular LB product or heuristic, but there are some factors which must be taken into consideration when configuring a LB in front of either AAWC or SDK servers.

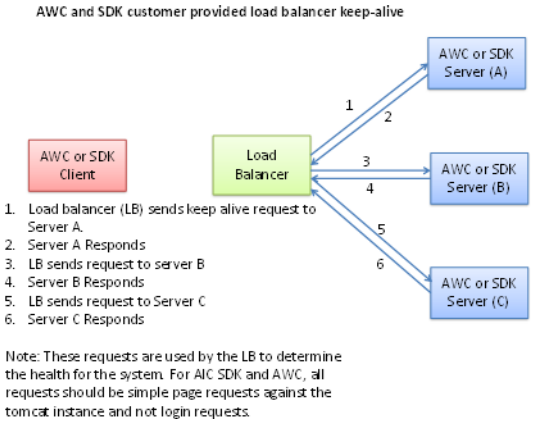
Summary

- The WebConnector software (Tomcat) is expected to be deployed on two or more similar servers.
- The load balancer is deployed between the WebConnector (AAWC/SDK) servers and the agent client endpoints.
- If an HTTP server is to be used for load balancing it cannot be hosted co-resident with the AAWC/SDK server.
- Proxy servers and Network Address Translation are not supported for AAWC/SDK.
- Clustering of AAWC/SDK servers is not supported.
- Connections to AAWC/SDK are "stateful" and will persist of the life of ADUs associated with agents unless terminated by a logout event. Memory consumed by session threads will persist until recovered by the jvm garbage collector.
- Load balanced connections with HTTP requests and IC WebService requests are "stateless" non-persistent and do not require sticky sessions.
- AIC is unaware of and indifferent to the heuristic employed for load balancing provided the client load is distributed such that the number of agents connected to any given client server is within recommended limits (up to 500 for multimedia agents and up to 800 voice-only agents per server depending on contact load).
- Heart beats from LB, if concerned with application status rather than host status, should be stateless and interact only with the Tomcat server (and not the application).

Heart beat

State of health of a target server can be examined at the host level via a simple ICMP ping, which will indicate whether the platform is available via a network connection. This does not indicate the health of the application itself. If this level of granularity is desired it is necessary to "ping" the tomcat application directly. Care must be taken in this case to avoid connecting to the tomcat server in a manner which will cause a login attempt to AIC, as this will result in the creation of session within tomcat. This session will persist either until an explicit logoff request is made or (potentially) for the life of the ADU configured for that server and IC domain (which could be as much as 9 hours).

A better solution for this is to create a simple html document (such as <HTML>ping</HTML>) which would be saved as a .jsp file in a virtual directory NOT associated with AIC and which sends a cookie to the load balancer to establish a single, reused session for communication. This is very light weight, provides proof that the tomcat server is running, and avoids placing load on any additional AIC components such as blender or ADU servers.



Port utilization is described in Appendix A of Avaya Interaction Center Security Guide. The following are pertinent to this discussion:

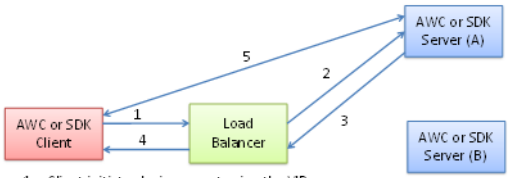
- SDK and AAWC server messaging ports: 8000-9000 (The servers will choose two available ports in this range at startup)
- AAWC default HTTP listener port: 9080
- SDK default HTTP listener port: 9700

If there is a firewall between the agent computers that run Avaya Agent Web Client and the computer that hosts WebConnector, you must open two configurable ports. The two ports are required because Avaya Agent Web Client receives data in real-time rather than by polling. The first port allows incoming HTTP traffic to the server, and the second port permits the server to notify the client of events.

Sessions

Connections between agents and the agent client (AAWC or SDK) are stateful and must persist. As such the load balancer must establish sticky sessions to ensure the establishment of this link. The method for implementing this varies by load balancer product and is beyond the scope of this document; however the load balancers reviewed in preparing this document appear to fully support sticky sessions without special considerations. Note that both the AIC AAWC and SDK have built-in redirection that establishes communication directly with the server (see above) after initial login and session creation. The response to the login request includes the server and port that the client will use for all subsequent interactions. The load balancer should be concerned only with the initial request.

AWC and SDK communication with a customer provided load balancer



1. Client initiates login request using the VIP address. This address can be on a standard http or https port.
2. Load balancer sends request to the "best" AWC or SDK server.
3. ACW or SDK server responds with a session ID, and server and port information. In this case Server (A) is returned with port 9800.
4. LB forwards response.
5. Client connects directly to the server for all subsequent messages both to the server and from the server to the client.

Multi-site deployment

The Avaya Agent Web Client server deployment scenario for multiple cells is similar to the Avaya Agent Web Client deployment scenario for load balancing.

This section includes the following topics:

- Overview of multi-site deployment on page 187
- Benefits of a multi-site deployment on page 187
- Overview of network structure for a multi-site deployment on page 188

Overview of multi-site deployment

This deployment consists of multiple clusters with each cluster in its own cell. A cell is created to partition the administration as well as the agent population. Each cell has a specific set of WebConnectors forming its cluster. Agents are assigned to a specific cluster.

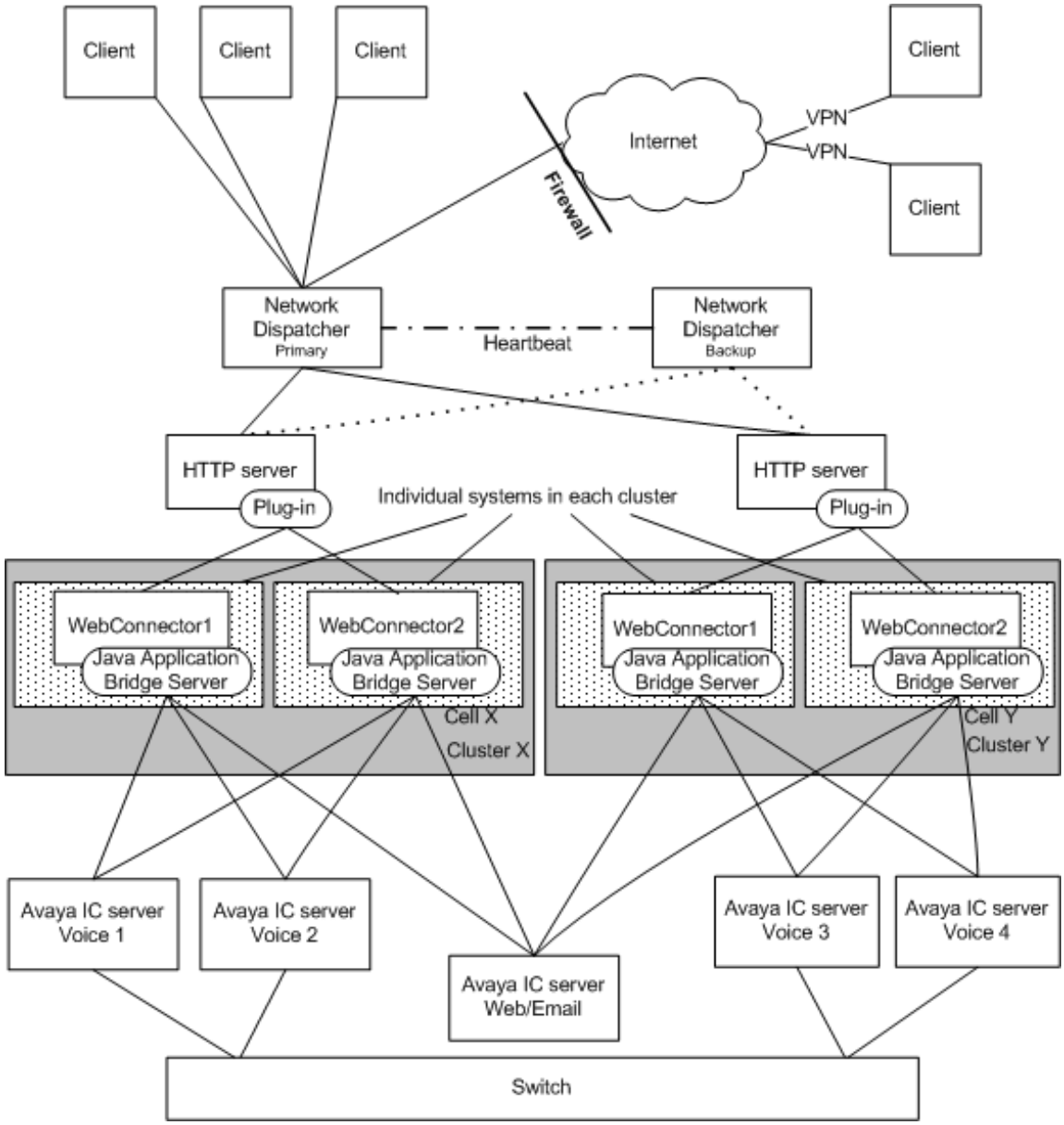
Benefits of a multi-site deployment

With a multi-site deployment you can:

- Partition agents to support organization structures or optimize agent network connectivity.
- Locate each cell and cluster across multiple sites to increase availability. To prevent a WAN outage from impacting all remote sites, distribute network dispatchers and HTTP servers to multiple sites.
- Support the transition to Avaya Agent Web Client updates with new customization or fixes. You can create a new cell for a new version of Avaya Agent Web Client without impacting the currently working version. Both cells can be active until the transition is successful.

Overview of network structure for a multi-site deployment

The following diagram provides an overview of the network structure for a multi-site deployment:



Comments on this document? infodev@avaya.com

Chapter 7: Interaction Center hardware requirements

The hardware requirements mentioned in this section are the minimum requirements for an Avaya Interaction Center (Interaction Center) installation.

These hardware requirements do not include third-party components, such as database management, email, telephony, and web-hosting services. For information about requirements for these components, see the manufacturer's documentation.

This information includes estimated hardware requirements for OA components that run on the same computers as Interaction Center components. If you plan to run all the OA components on dedicated computers, you must use the hardware requirements for OA for those computers. For more information about the hardware requirements for OA, see OA *Installation Planning and Prerequisites*.

Important:
The following hardware requirements are estimates only. Contact your Avaya representative or Avaya Business Partner representative for assistance with sizing your Interaction Center system.

This section includes the following topics:

- Hardware requirements for deploying Interaction Center on page 189
- Hardware guidelines for Interaction Center servers on page 190
- Hardware requirements for Design & Administration Tools on page 193
- Required hardware for agent workstations on page 195
- Required hardware for IV Chat on page 197

Hardware requirements for deploying Interaction Center

Interaction Center servers, Design and Administration Tools, and agent desktop applications have different hardware requirements. You cannot install them on the same computers.

For example:

Servers: Do not install and run Interaction Center servers on the same computer as Design & Administration Tools or agent desktop applications.

Design & Administration Tools: Do not install and run Design & Administration Tools on the same computer as Interaction Center servers or agent desktop applications. Do not run more than one IC Manager concurrently. You can run all of the Design & Administration Tools on the same computer.

Agent desktop applications: Do not install and run agent desktop applications on the same computer as Interaction Center servers or Design & Administration Tools. You can run Avaya Agent, Avaya Agent Web Client, and Client SDK on the same computer, but only one at a time.

Hardware guidelines for Interaction Center servers

Interaction Center can run on a variety of computers from different hardware vendors. All computers that host Interaction Center servers require fast CPUs and sufficient available memory. To increase the availability of your Interaction Center servers, replicate the servers on independent servers. For examples of how to replicate your servers to meet the needs of your Interaction Center system, see Interaction Center single site deployment scenarios on page 79, and Interaction Center multi-site deployment scenarios on page 123.

The performance of your Interaction Center servers is completely dependent on the hardware and networking systems being available and properly configured.

This section includes the following topics which describe guidelines that typically result in good performance and reliability:

- Hardware requirements on page 191
- Server distribution on page 191
- Server failover on page 191
- Server speed on page 191
- Server configuration impact on page 191
- Disk space for Interaction Center servers on page 192
- Disk space for server log files on page 192
- Validation of Hardware configuration on page 192
- IBM Logical Partition (LPAR) technology on page 192

Hardware requirements

The hardware requirements for servers depend upon the deployment of an Interaction Center system, the volume of contacts in the contact center, and performance requirements.

Your Avaya representative or Avaya Business Partner representative has documentation and information to estimate hardware sizing for an Interaction Center system. For assistance with sizing an Interaction Center system, contact your Avaya representative or Avaya Business Partner representative.

Server distribution

Distribute application servers across multiple physical computers to meet performance and fault tolerance requirements.

Note:

If you run CPU-intensive third-party applications on the same computers as Interaction Center servers, the third-party applications impact the performance of your Interaction Center system.

Server failover

Failure of a single server should not impact all agents in the contact center. Partition Interaction Center servers appropriately across physical computers, and configure failover appropriately.

Server speed

Install application servers on computers with fast CPUs and adequate memory. These servers primarily require disk space for paging tasks and temporary files.

Server configuration impact

If your configuration includes certain conditions, such as large reporting loads or integration program loads, you may need to re-size the computers that host the servers or configure secondary application servers.

Disk space for Interaction Center servers

Allocate sufficient disk space on each Interaction Center server. Interaction Center copies all server files to a computer, even if that computer does not host all the servers. You must have 10 GB of free space on the system where you plan to install the IC server. The partition where the temp folder resides must have at least 3 GB of free space.

Disk space for server log files

Interaction Center installs most servers with a default log size of 2.5-MB. However, IC provides the ability to configure log file size, log file count, and log day count parameters using which the customer can decide the amount of logs to be captured and stored on the server. You can configure these parameters in IC Manager. Therefore, the disk space needed for the server logs needs to be calculated as per the configuration.

Validation of Hardware configuration

Validate your hardware, network, security, and database to meet the recommended guidelines for Avaya IC.

IBM Logical Partition (LPAR) technology

Interaction Center provides the following support for the IBM Logical Partition (LPAR) technology:

1. The following platforms are supported for all IC servers.
   - Single/Multi CPU POWER3
   - Single/Multi CPU POWER4
   - Single/Multi CPU POWER5
2. All AIX computers must be upgraded to the latest levels of the respective hardware microcode.

Note:

When you deploy Interaction Center components, the type of CPU, the number of CPUs, and the LPAR technology are not the determining factors for determining supportability.

Hardware requirements for Design & Administration Tools

The following table lists the minimum hardware requirements for design and administration workstations in a Windows environment.

These hardware requirements do not include third-party components, such as database management, email, telephony, and web-hosting services. For information about requirements for these components, see the manufacturer's documentation.

CAUTION:
Do not run IC Manager on a multi-processor computer.

Component	Minimum Requirement
CPU	Physical Hardware:1 CPU with 2 Cores each of 2.20 GHz Virtual Machine Hardware: 2.20 GHz • Number of virtual sockets: 1 • Number of cores per socket: 2
RAM	2 GB **Note:** If you are using Microsoft Windows 8.1 then you must have minimum 4 GB RAM.
Free Disk Space	10 GB
Free space on the partition where temp folder resides	3 GB
Monitor Resolution	1280x1024 (16 bit/32 bit colors)
Minimum Monitor Resolution	1024x768 (256 colors)

Note:
The above hardware requirements are also applicable for setting up a virtual machine.

Hardware requirements for IC servers

The following table lists the minimum hardware requirements for IC Server.

These hardware requirements do not include third-party components, such as database management. For information about requirements for these components, see the manufacturer's documentation.

Component	Minimum Requirement
CPU	Physical Hardware:1 CPU with 4 Cores each of 2.80 GHz Virtual Machine Hardware: 2.80 GHz • Number of virtual sockets: 2 • Number of cores per socket: 2
RAM	4 GB **Note:** If you are using Microsoft Windows Server 2012 then you must have minimum 6 GB RAM.
Free Disk Space	80 GB **Note:** The free disk space is the minimum requirement. If you plan to have large amount of application log files, plan the disk space accordingly.
Free space on the partition where temp folder resides	10 GB

Note:
The above hardware requirements are also applicable for setting up a virtual machine.

Required hardware for Avaya Agent WebConnector / SDK

The following table lists the minimum hardware requirements for Avaya Agent WebConnector.

CPU	Physical Hardware:1 CPU with 4 Cores each of 2.80 GHz Virtual Machine Hardware: 2.80 GHz • Number of virtual sockets: 2 • Number of cores per socket: 2
RAM	4 GB **Note:** If you are using Microsoft Windows Server 2012 then you must have minimum 6 GB RAM.
Free Disk Space	10 GB
Free space on the partition where temp folder resides	3 GB

Note:
The above hardware requirements are also applicable for setting up a virtual machine.

Required hardware for agent workstations

This section describes the minimum hardware requirements for agent workstations in a Windows environment.

These hardware requirements do not include third-party components, such as database management, email, telephony, and web-hosting services. For information about requirements for these components, see the manufacturer's documentation.

This section includes the following topics:

- Required hardware for the Avaya Agent interface on page 196
- Required hardware for the Avaya Agent Web Client interface on page 197

Required hardware for the Avaya Agent interface

The following table lists the minimum hardware requirements for agent workstations installed with Avaya Agent.

If you plan to run additional components on the agent desktop computer, you must allow a minimum of 1 GB of RAM and 400-MB of free disk space for Interaction Center agent applications.

Hardware component	Minimum Requirement
CPU	Physical Hardware:1 CPU with 2 Cores each of 2.20 GHz Virtual Machine Hardware: 2.20 GHz • Number of virtual sockets: 1 • Number of cores per socket: 2
RAM	2 GB **Note:** If you are using Microsoft Windows 8.1 then you must have minimum 4 GB RAM.
Free Disk Space	5 GB
Free space on the partition where temp folder resides	3 GB
Recommended Monitor Resolution	1280x1024 (16 bit/32 bit colors)
Minimum Monitor Resolution	1024x768 (256 colors)

Note:
The above hardware requirements are also applicable for setting up a virtual machine.

Required hardware for the Avaya Agent Web Client interface

The following table lists the minimum hardware requirements for the workstations of agents who use Avaya Agent Web Client:

Hardware component	Microsoft Windows
CPU	Physical Hardware:1 CPU with 2 Cores each of 2.20 GHz Virtual Machine Hardware: 2.20 GHz • Number of virtual sockets: 1 • Number of cores per socket: 2
RAM	2 GB **Note:** If you are using Microsoft Windows 8.1 then you must have minimum 4 GB RAM.
Free Disk Space	Diskless workstations are not supported.
Monitor Resolution	1280x1024 (16 bit/32 bit colors)
Minimum Ethernet connection	100-Mbps

Note:
The above hardware requirements are also applicable for setting up a virtual machine.

Required hardware for IV Chat

The Communication Manager must have at least one TN2302 Medpro board to work with Voice chat, as the VMM service requires the G.723-5.3 IP codec.

For configuring IVChat, see *Avaya Interaction Center Installation and Configuration guide*.

Chapter 8: Interaction Center licensing

You must obtain a license file for your configuration of Avaya Interaction Center (Interaction Center) before you complete your installation and configure your Interaction Center system. Interaction Center cannot function without a valid license file for all components included in your Interaction Center system. The steps you must take to obtain a license file begin when you select and purchase your Interaction Center system.

You must obtain a license for the Interaction Center systems, including the production, development, and test systems. Licenses for production systems include all of the features and capacities that you purchased for your Interaction Center system. Licenses for non-production systems include up to ten concurrent users.

Note:
If your upgrade includes new servers, you must obtain a new license.

To obtain an Interaction Center license file, consult your Avaya representative or Avaya Partner representative and perform the steps in the following sections:

- Prerequisites for license files on page 199
- Identifying a physical address on page 200
- Requesting a license file on page 202
- Updating a license file on page 203
- Requesting a replacement license file on page 204
- Identifying a physical address for license files on page 200

Prerequisites for license files

The contents of your license file reflect your Interaction Center system. Before you apply for and obtain a license file, you must plan the hardware and software configuration of your Interaction Center system. Your Avaya representative or Avaya Partner representative can assist you with this task.

You need to consider all options in your Interaction Center system to determine the hardware and software configuration for your Interaction Center license file, including:

- Platform architecture, such as how many servers you require and which, if any, telephony equipment you have.
- Reliability objectives.
- Network topology.

- Interaction Center components required by your system.
- Number and type of media channels.
- Number of Interaction Center sites.
- Number of concurrently logged in agents and supervisors per site.
- Number of concurrently logged in agents and supervisors using each media channel and component.
- Number of Web License Managers and License servers.
- Physical addresses of the computers that will host the License server components for your Interaction Center system. These physical addresses are also known as Host IDs.

Identifying a physical address

You must provide a physical address for each server that hosts WebLM for your Interaction Center. The physical address is also known as the host ID.

The Interaction Center installer automatically identifies the physical address when you install the server files. You do not need to install a license file to install Interaction Center or view the physical address in the Web License Manager (WebLM). To make sure that you identify the physical address for the correct NIC and server, you must use this method. For more information about how to install Interaction Center and set up the Web License Manager, see *IC Installation and Configuration Guide*.

The WebLM displays the physical address in the Server Properties field.

Identifying a physical address for license files

If you cannot use the WebLM to identify the physical address for one or more computers, perform the steps in one of the following sections to identify a physical address:

- Identifying a physical address in Windows on page 201
- Identifying a physical address on Oracle Solaris on page 201
- Identifying a physical address on AIX on page 201

Identifying a physical address in Windows

To identify a physical address on a Windows computer:

1. Open a command window.

   To open a command window, select **Start** > **Run** and enter **cmd** in the **Open** field.

2. At the prompt, enter: **ipconfig /all**
3. Windows displays the physical address on a separate line, such as:

   ```
   Physical Address. . . . . . . . : 00-53-45-00-00-00
   ```

Identifying a physical address on Oracle Solaris

To identify a physical address on an Oracle Solaris computer:

1. Run the following command: **hostid**
2. Oracle Solaris displays the physical address as a list of hexadecimal digits on a separate line, such as:

   ```
   831800e9
   ```

Identifying a physical address on AIX

To identify a physical address on an AIX computer:

1. Run the following command: **uname -m**
2. AIX displays the physical address as a list of hexadecimal digits on a separate line, such as:

   ```
   000C066A4C00
   ```

Requesting a license file

You must request a separate license file for each Interaction Center system. For example, if you plan to create a development system and a production system, you must have a different license file for each system. You must send a separate request for each license file.

To request an Interaction Center license file:

1. Send an email message to icoakeyrequest@avaya.com with the following information about your Interaction Center system:

Required information	Description
SAP order numbers	Avaya assigns one or more numbers to the customer's order in the SAP system.
Avaya sold-to number	Avaya assigns this number to the customer.
Customer name	Name of the customer who purchased the Interaction Center system.
System purpose	The system purpose must be one of the following: • Production • Development • Test If you need license files for two systems, send two separate email requests.
Return email address	Avaya emails the license file to you. You must provide a secure email address where you want to receive the license file.
Physical addresses	Physical addresses of the computers that hosts the Web License Manager (WebLM) and License server components for this particular Interaction Center system. These Physical addresses are also known as Host IDs. For more information, see Identifying a physical address on page 200.

2. You receive an Interaction Center license file from Avaya at the email address designated by your enterprise.
3. Install and activate the license file in your Interaction Center system. For instructions on how to install and activate a license file, see *IC Installation and Configuration Guide*.

Important:
Maintain a copy of your license files in a safe location for future use.

Updating a license file

If your enterprise purchases additional components for your Interaction Center system, or adds more concurrent users, you must update your Interaction Center license file.

To update an Interaction Center license file:

1. Send an email message to icoakeyrequest@avaya.com with the following information about your Interaction Center system:

Required information	Description
SAP order numbers	You must provide the original order numbers for your Interaction Center system, and the order numbers for the new components or capacities. Avaya assigns one or more numbers to the customer's order in the SAP system.
Avaya sold-to number	Avaya assigns this number to the customer.
Customer name	Name of the customer that purchased the Interaction Center system.
System purpose	The system purpose must be one of the following: • Production • Development • Test If you need license files for two systems, send two separate email requests.
Return email address	Avaya emails the license file to you. You must provide a secure email address where you want to receive the license file.
Physical addresses	Physical addresses of the computers that host the Web License Manager (WebLM) and License server components for this particular Interaction Center system. These Physical addresses are also known as Host IDs. For more information, see Identifying a physical address on page 200.

2. You will receive an Interaction Center license file from Avaya at the email address designated by your enterprise.
3. Install and activate the license file. For instructions on how to install and activate a license file, see *IC Installation and Configuration Guide*.

Requesting a replacement license file

If you change or upgrade your network, you may need to obtain a replacement license file. Changes that affect the license file include:

- Replacement of the network card on the computer that hosts a Web License Manager.
- Transfer of a Web License Manager to a new computer.
- After upgrading WebLM from 6.3.4 to 7.0.1 version, HostID will be changed.

To obtain a replacement license file:

1. Send an email message to icoakeyrequest@avaya.com with the following information about your Interaction Center system:

Required information	Description
SAP order numbers	You must provide the original order numbers for your Interaction Center system, and any additional order numbers for new components or capacities. Avaya assigns one or more numbers to the customer's order in the SAP system.
Avaya sold-to number	Avaya assigns this number to the customer.
Customer name	Name of the customer that purchased the Interaction Center system.
System purpose	The system purpose must be one of the following: • Production • Development • Test If you need license files for two systems, send two separate email requests.
Return email address	Avaya emails the license file to you. You must provide a secure email address where you want to receive the license file.
Physical addresses	Physical addresses of the computers that host the Web License Manager (WebLM) and License server components for this particular Interaction Center system. These Physical addresses are also known as Host IDs. For more information, see Identifying a physical address on page 200.

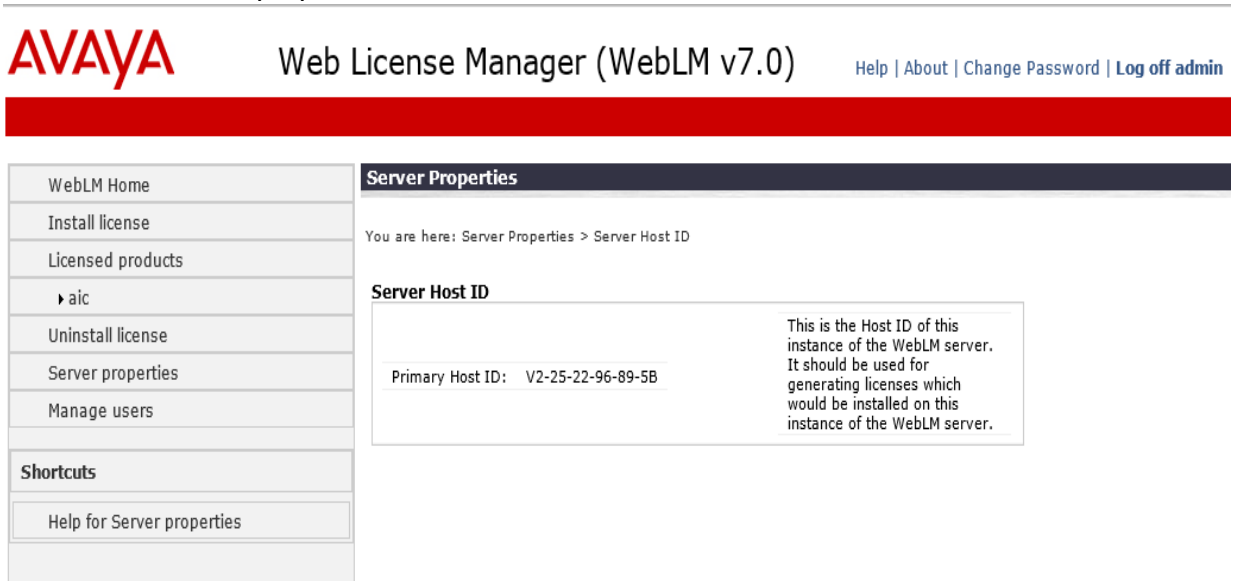
2. You will receive an Interaction Center license file from Avaya at the email address designated by your enterprise.

3. Install and activate the license file. For instructions on how to install and activate a license file, see *IC Installation and Configuration Guide*.

Identifying HostID

To get Server ID or Host ID when license is not installed yet, do the following:

1. In the Web browser, navigate to the following URL for the WebLM: https://<system_name>.<domain>:<webLM_port>/WebLM/LicenseServer.
   For example: https://testbox.xyzcorp.com:52233/WebLM/LicenseServer
2. Enter the default user name and password. The default user name is **admin** and the password is **weblmadmin**. WebLM prompts you to change the password immediately.
3. Click **Server** properties.



Troubleshooting IC License Server

IC License Server using extra TotalAgents license

Problem Description

Issue: License Server procures extra "TotalAgents" license when the Telephone Server (voice) and WebACD (email+chat) requests different License Servers for the same agent having all channels enabled in multi-domain, multi-LS environment.

Solution

The issue seems to occur when the request of licenses for a single agent is going to two different License Servers (LS), first from TS (for voice channel), and the second from WACD (for email and chat).

TS could be requesting from the primary LS, whereas WACD is requesting from the secondary LS or vice versa.

Essentially, for a particular agent, license request for all media channels should go to the same LS, that is, TS and WACD should request from the same LS.

License Server procures a "TotalAgents" license for the first time if it has not already been done for that agent, irrespective of the channel requesting it. For subsequent request from remaining channels for the same agent, the License Server does not request for "TotalAgents" license.

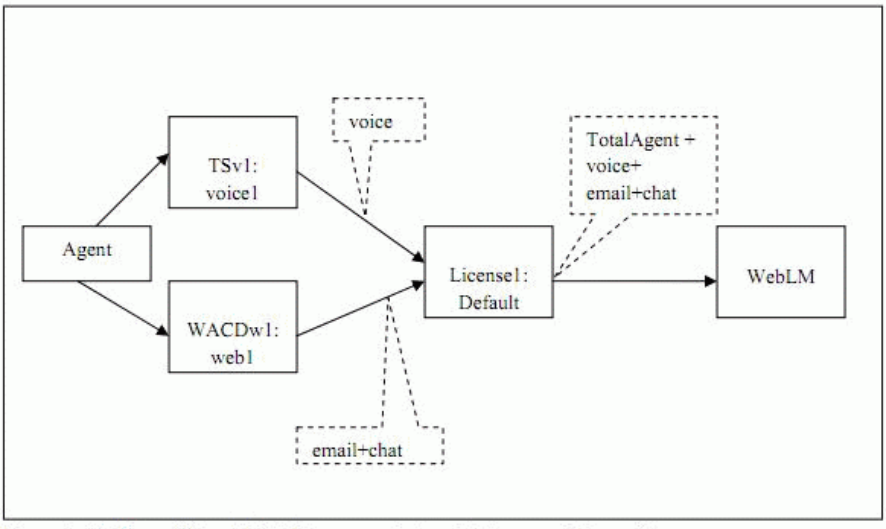


Figure 1: No Issue - TS and WACD communicates with the same License Server

Comments on this document? infodev@avaya.com

The TotalAgents parameter is a local resident value per LS and not across multiple LSs. So if the multiple license requests of different channels for the same agent go to the same LS, there is no issue (Figure 1).

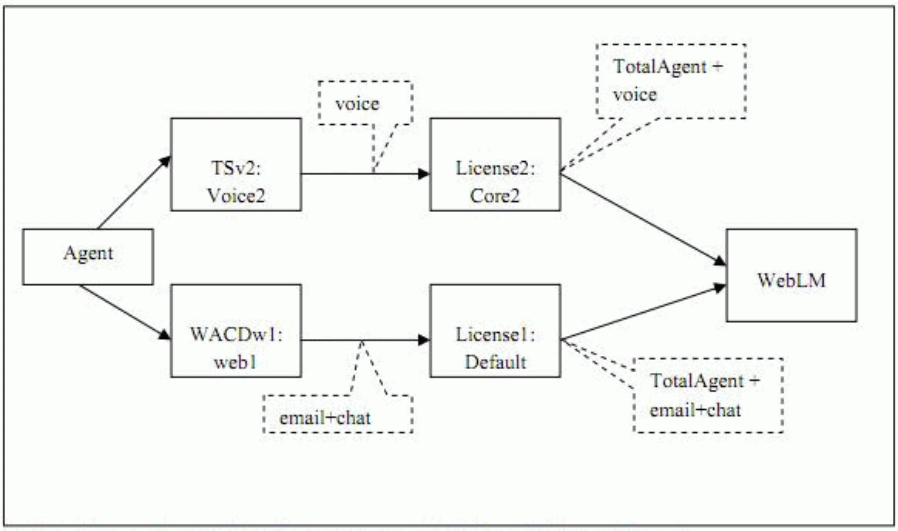


Figure 2: Issue - TS and WACD communicates with different License Servers

However, if the different license requests (from TS and WACD) go to different LSs, then each LS procures a "TotalAgents" license, in addition to the license for the channel. This is so, because either of the LS is not aware of the other LS procuring the "TotalAgents" license for the same agent (Figure 2).

Another factor is that only one WACD can be active at a given time.

An example of this issue is when an active WACDs domain failover for LS does not match with TSv2 in domain Voice2, and both the active WACD and TSv2 send requests to different LSs.

Chapter 9: Supported database management systems

A Relational Database Management System (RDBMS) is a required prerequisite for Avaya Interaction Center. Interaction Center servers and client applications access databases to:

- Store employee, contact, and configuration information.
- Deliver statistical information to managers.
- Deliver customer contact information to agents.

OA uses data stored in the IC Repository database. Before you install Interaction Center, make sure that you perform all prerequisite steps for OA. For more information and some guidelines for installing and configuring your database software, see OA *Installation Planning and Prerequisites*.

This section describes the required databases and optional databases for Interaction Center and OA, and provides information that you need to configure a RDBMS for Interaction Center. This section includes the following topics:

- About Interaction Center databases on page 210
- Mixed operating system combinations on page 210
- Exceptions to supported database management systems on page 210
- Requirements for database login on page 211
- Installing database servers on page 211
- Installing database client software on page 212
- Configuring binary sort order for Web Management on page 214
- Microsoft SQL Server on page 214
- Oracle on page 220
- IBM DB2 on page 225

Tip:
For more information about supported database management systems, see Prerequisites for the databases on page 290.

About Interaction Center databases

Your Interaction Center databases interact with:

- Interaction Center software
- Interaction Center data store units
- OA software

At a minimum, your Interaction Center system must include the IC Repository database and the CCQ database. Some Interaction Center applications, such as Business Advocate, also require dedicated databases. Depending on the components in your implementation, your Interaction Center system may also require one or more of these optional Interaction Center databases.

The Avaya Customer Interaction Repository includes the Interaction Center, the OA database, and the storage components used by an Interaction Center system.

Mixed operating system combinations

A mixed operating system combination occurs when the databases are on one supported operating system and the Interaction Center servers are on a different supported operating system.

For mixed operating system support, contact your Avaya representative.

Exceptions to supported database management systems

Business Advocate does not support the Business Advocate databases on DB2 and AIX.

If you host your Interaction Center and Interaction Center databases on AIX and DB2, configure a Windows or Oracle Solaris computer with a supported SQL Server or Oracle database to host the Business Advocate databases. You must also configure a Data server on a computer that hosts a Resource Manager server to connect to the Business Advocate database.

Requirements for database login

The Interaction Center Data server requires an administrative login with DBA privileges for your database. The administrative login must be a DBA login ID for the database server. Do not use the DBA login for a database client.

Interaction Center and OA must use the same administrative login. The following table shows typical values for this administrative login. If you choose to use a different administrative login, make sure that login has the same permissions as the logins listed in the table.

Property	SQL Server	Oracle	DB2
Database Administration Login	sa	system	db2inst1
Database Administration Password	*password* for sa	*password* for system	*password* for db2inst1

Installing database servers

Database servers act as a central repository for all the information that Interaction Center stores and retrieves. You can install and configure database servers in a number of ways to provide scalability, fault tolerance, and security to meet the specific requirements of your organization.

Install the database client and any required libraries on every computer that hosts an Interaction Center Data server.

Database server installation and configuration are beyond the scope of this manual. If you have not yet deployed your chosen database platform, consult a Database Administrator (DBA).

Installing database client software

Interaction Center servers communicate with the RDBMS through a database client. You need to install the appropriate database client for the RDBMS.

Important:
For all supported databases, you must install the 32-bit version of the database client. Interaction Center does not support the use of 64-bit versions of database clients, even with 64-bit database server components.

Interaction Center supports the database clients in the following table. For more details about the definition of supported versions and about the subsequent updates or service packs of the software, see About the supported versions on page 286.

Database	Database client (32-bit only)
IBM DB2 9.5	IBM DB2 9.5 Administrative Client
Oracle 10g	Oracle 10g client
Oracle 11g, 11g Release 2	Oracle 11g client
Oracle 12c IC Release 7.3.3 and later supports Oracle 12c only on: • Microsoft Windows operating system. • without pluggable database container	Oracle 12c client
Microsoft SQL Server 2008 R2	SQL Server 2008 R2 client **Note:** You do not require the SQL Server 2008 R2 client on the IC server system. However, if you are using SQL Server 2008 R2, you must require the SQL Server 2008 R2 client on the OA server system.
Microsoft SQL Server 2012	SQL Server 2012 client
Microsoft SQL Server 2014	SQL Server 2014 client

Location for database clients

Certain Interaction Center servers and applications require access to a database client. You must install a database client on the same computer as these servers and applications.

You must install the database client on the computers that host the Interaction Center servers and applications listed in the following table:

Interaction Center component	Servers and applications that require database client
Core servers	Data server
Web Management	WebACD server, Attribute server, ICM server, CIRS server, and all websites
Business Advocate	Resource Manager server, Component Manager, and Advocate Admin

The database administrator (DBA) must ensure that the database client can connect to the database server.

Note:

- If you are configuring IC with SQL Server 2008 R2, you do not need to install the SQL Server 2008 R2 client on any IC server system.
- If you are configuring IC with SQL Server 2012, you must install the SQL Server 2012 client on all the IC server system.

Detailed information about database client installation is beyond the scope of this manual. Therefore, for more information, see the documentation provided by your RDBMS vendor.

Requirements for database clients

Database clients require the following:

32-bit versions: For all supported databases, you must install the 32-bit version of the database client. Interaction Center does not support the use of 64-bit versions of database clients, even with 64-bit database server components.

Dedicated RAM: Reserve a dedicated amount of RAM to run the database. For more information, see the documentation for your database client.

Connection pool: Ensure there is a connection pool to the Data server. For example, if your Interaction Center includes an Oracle database, calculate the amount of memory required, in megabytes, by multiplying the connection pool size by 3.

Swap space: Reserve two to three times the amount of main memory as swap space, preferably on a raw disk.

Configuring binary sort order for Web Management

Web Management:

- Does not support binary sort order on any database platform.
- Cannot differentiate between employee accounts based on case.
- Can cause authentication problems in cases where, for example, **Agent1** is not the same user as **agent1**.

Binary sort order compares bit by bit and is case-sensitive. For example, in Web Management, the SQL command `select * from topic` would not return results from a table named `Topic` if binary sort order is turned on, because `Topic` does not match `topic`.

Note:
DB2 databases do not use binary by default. The sort order for DB2 is set in the configuration of the AIX operating system.

Microsoft SQL Server

All Interaction Center servers and client components support the following Microsoft SQL Server databases:

- Microsoft SQL Server 2008 R2 Standard Edition
- Microsoft SQL Server 2008 R2 Enterprise Edition
- Microsoft SQL Server 2012 Standard Edition
- Microsoft SQL Server 2012 Enterprise Edition
- Microsoft SQL Server 2014 Standard Edition
- Microsoft SQL Server 2014 Enterprise Edition

This section includes the following topics:

- Installing SQL Server 2008 on page 215
- Recommended configuration for SQL Server on page 218

Installing SQL Server 2008

You must install and configure SQL client on all computers that host your Interaction Center databases.

Important:
Do not configure your database to be case-sensitive.

The following table contains recommended values for certain options that you must select during an SQL Server installation. For more information about these options, and about the other options in the SQL Server installer, see the documentation provided with your SQL Server database.

Property	Value
Architecture of the SQL Server	Select **x64**. This option indicates that you are installing the 64-bit version of SQL Server.
Local Computer	Selection depends upon where you plan to deploy your OA Historical subsystem: • If Historical subsystem is on the same computer as Interaction Center and OA databases, select **Server and Client Tools**. • If Historical subsystem is a different computer than the Interaction Center and OA databases, select **Client Tools**.
Setup Role	Select **All Features with Defaults** option.
Feature Selection	Do not install the **Business Intelligence Development Studio** option.
Instance Configuration	Enter a name for the database instance that identifies the instance of the RDBMS system in which you create databases. **Tip:** You need the database instance name to install the OA Historical subsystem.
Service Accounts	• Select **Use the same account for all SQL Server service**s. • Enter the sa login ID (or a login ID with the same privileges) and the password for that account. **Tip:** You need this login and password when you configure Interaction Center and install the OA Historical subsystem.

Property	Value
Collation Settings	Select the default value. **Note:** AIC database uses SQL_Latin1_General_CP1_CI_AS Collation. If you want to use AIC with OA then AIC database collation must be set to SQL_Latin1_General_CP1_CI_AS Collation.
Account Provisioning	Authentication Mode: • Select **Mixed Mode**. • Enter and confirm the password for the `sa` login ID.
TCP/IP sockets	Enter the port number used to communicate with the database. The default port is 1433 for Interaction Center and OA. **Tip:** You need this port number when you configure Interaction Center and install the OA Historical subsystem.

Detailed instructions on the installation and configuration of SQL Server are beyond the scope of this manual. If you plan to use SQL Server with Interaction Center, but have not yet installed SQL Server, consult a qualified SQL Server DBA (Database Administrator) for assistance.

Installing SQL Server 2012 and SQL Server 2014

You must install and configure SQL client on all computers that host your Interaction Center databases.

Important:
Do not configure your database to be case-sensitive.

Software Prerequisites for SQL Server 2014:

- Microsoft SQL Server 2014 requires .Net Framework 3.5 Service Pack 1 to be installed on the server. If you run Setup and you do not have .NET 3.5 SP1, SQL Server Setup will require you to download and install .NET 3.5 SP1 before you can continue with the SQL Server installation. You can download Microsoft .NET Framework 3.5 Service Pack 1 from the following Microsoft website: https://www.microsoft.com/download/details.aspx?id=22.
- If you run Setup on a computer with Windows Server 2008 R2 SP1 or Windows 8, you must enable .NET Framework 3.5 SP1 before you install SQL Server 2014.

- .NET 4.0 is a requirement for SQL Server 2014.

The following table contains recommended values for certain options that you must select during an SQL Server installation. For more information about these options, and about the other options in the SQL Server installer, see the documentation provided with your SQL Server database.

Property	Value
Architecture of the SQL Server	Select **x64**. This option indicates that you are installing the 64-bit version of SQL Server.
Local Computer	Selection depends upon where you plan to deploy your OA Historical subsystem: • If Historical subsystem is on the same computer as Interaction Center and OA databases, select **Server and Client Tools**. • If Historical subsystem is a different computer than the Interaction Center and OA databases, select **Client Tools**.
Setup Role	Select **All Features with Defaults** option.
Instance Configuration	Enter a name for the database instance that identifies the instance of the RDBMS system in which you create databases. **Tip:** You need the database instance name to install the OA Historical subsystem.
Service Accounts	Select the default value.
Collation Settings	Select the default value. **Note:** AIC database uses SQL_Latin1_General_CP1_CI_AS Collation. If you want to use AIC with OA then AIC database collation must be set to SQL_Latin1_General_CP1_CI_AS Collation.

Property	Value
Server Configuration	Authentication Mode: • Select **Mixed Mode**. • Enter and confirm the password for the `sa` login ID.
TCP/IP sockets	Enter the port number used to communicate with the database. The default port is 1433 for Interaction Center and OA. **Tip:** You need this port number when you configure Interaction Center and install the OA Historical subsystem.

Detailed instructions on the installation and configuration of SQL Server are beyond the scope of this manual. If you plan to use SQL Server with Interaction Center, but have not yet installed SQL Server, consult a qualified SQL Server DBA (Database Administrator) for assistance.

Recommended configuration for SQL Server

Interaction Center does not have any required or recommended configuration settings for SQL Server.

However, OA has some recommended configuration settings that you need to set after you configure the Interaction Center databases in Database Designer. For more information, see OA *Installation Planning and Prerequisites*.

For information about international character set for SQL server, see http://msdn.microsoft.com/en-us/library/ms142795.aspx.

SQL server AlwaysOn Availability Groups

Avaya Interaction Center support SQL server **AlwaysOn Availability** feature from Avaya Interaction Center Release 7.3.6 with SQL server 2016 Enterprise Edition.

The **Always On Availability Groups** feature is a high-availability and disaster-recovery solution that provides an enterprise-level alternative to database mirroring. This feature maximizes the availability of a set of user databases. An availability group supports a set of read-write primary databases and one to eight sets of corresponding secondary databases

Note:

When secondary node is back into network after a long time, data synchronization takes more time. It depends on the size of Database delta, when the node is down and come back into cluster.

Network round-trip delay between SQL server nodes must not be more than 64 minutes. More delays causes database synchronization issue across the nodes.

Avaya Interaction Center supports only SQL server nodes configured with your local database storage. Databases of any node must be synchronized before becoming a primary node. Otherwise, this causes data lose for Avaya Interaction Center.

Failovers

The type of failovers include the following:

- Manual node failure from **AlwaysOn Availability** dashboard
- Network failure of active node
- Active node SQL server service
- Active node machine shutdown
- Node HA between two different networks

During a failover:

- New Agent login request fails and existing agents are connected without any impact.
- New contacts are not processed and the existing connected contacts are unaffected.
- IC email and poller server can have issue on reading message IDs for few of the contacts for existing emails in the Avaya IC system.
- Database server can have issues. For example, **QW_KEYS table is locked or not exists**.
- Voice workflow server might not receive customer records for few calls that are already routed.

The following alarms are raised during failover:

- Poller@@DBRefresh : Error in ReadAllMessageIDs.
- DB::MessageTbl::ReadAllMessageIDs failed to run database query.
- Exhausted Workflow servers available to analyze emails from [ICEmail_Email] server.
- Fetch Customer Record (ts.incomingcall.FetchCustomerData): Error 10079: Generic Exception
  DCO=customerDCO Error=Database Error: In <Select>
  State:08S01,Code:10054,Error:[SQL Server Native Client 11.0]TCP Provider: An existing connection was forcibly closed by the remote from method MTTBinaryDataComm::Select
- QW_KEYS table is locked or not exists.{? = call q_next_key (N'mediainteraction', 10, ?)}.State:08S01,Code:64,Error:[SQL Server Native Client 11.0]TCP Provider: The specified network name is no longer available.
- ReportServer : Database Connection is broken.
- CDBRecord::SaveDcoRetry failed to run database query, will retry again.
- ICEmail server [ICEmail_Email] failed to fetch data from database for msgid [17536], contact will not be processed. Check database connectivity.

- Problem accessing Database.
- EDUAdaptor::createEDU : Unable to Create EDU! [Timeout] [Check: 1) EDU Server status, 2) Network strength]
- ICEmail Analyzed (icemail.analyzenoca.ICEmailAnalyzed1): Error 1: Timeout.

After the failover and **Database is accessible** alarm is raised:

- All connected agents are still connected without any impact.
- All connected chat and voice contacts are connected as it is
- Email channel is not impaired.
- TS maintains assigned devices session as it is.
- AAWC/SDK servers maintains connected agents session as it is.
- Website/CSPortal can escalate new chat.
- TS can process new voice contacts.
- New agent login works without any issue.
- There is no server crash.
- Avaya IC server do not raise DB operational related alarm for processing contact.

Oracle

All Interaction Center servers and client components support the following releases of the Oracle database:

- Oracle 10g

  Note:
  From Release 7.3.5, Avaya Interaction Center is not supporting Oracle 10g.
- Oracle 11g
- Oracle 11g Release 2
- Oracle 12c supported on IC Release 7.3.3 and later

You must consider the needs of your contact center, the operating system of the computer that hosts your database, and the configuration of your Interaction Center system to determine whether you require the Enterprise Edition or Standard Edition of Oracle.

This section includes the following topics:

- Required version mode for Oracle Client on page 221
- Required patches for an Oracle database on page 221

- Installing Oracle Server on page 221
- Installing Oracle Client on page 225

Required version mode for Oracle Client

You must install Oracle client in 32-bit mode. The Interaction Center Data server for Oracle uses 32-bit Oracle libraries. The Interaction Center Data server does not function if you install Oracle clients in 64-bit mode.

Required patches for an Oracle database

The following table describes the patches that Interaction Center requires for an Oracle database:

Oracle version	Required patches
Oracle 10g	• Patch set 4 – Windows: patch set p4163362_10104_WINNT – Solaris: patch set 10.1.0.4
Oracle 11g	• Patch set 11.1.0.6.0 (Windows and solaris both) • Patch set 11.0.2.1.0 (Windows Server 2008 R2, 64-bit)
Oracle 11g Release 2	Patch set 11.2.0.1.0 Patch set 11.2.0.4

Installing Oracle Server

This section contains information you must use when you install and configure Oracle server for use with Interaction Center.

This section includes the following topics:

- Location of Oracle server on page 222
- Configuration settings for Oracle 10g server on page 222
- Recommended values for installing Oracle 11g, 11g R2, and 12.1c server on page 222
- Configuration settings for Oracle 11g, 11g R2, and 12.1c server on page 223

Location of Oracle server

You must install and configure the Oracle Server on all computers that host your Interaction Center databases.

Configuration settings for Oracle 10g server

When you create the database instance for Interaction Center, you must include the following configurations:

Configuration	Required settings
db_block_size	8192 or higher
Dedicated connections	A minimum of 115 concurrently dedicated connections
Logging Parameters	Checkpoint Timeout of 0
Tablespaces	Two tablespaces for each Interaction Center database: one for standard database tables, one for temporary tables. For example, IC Repository and CCQ databases require the following tablespaces: • IC Repository tables – **T_CI** • IC Repository temporary tables – **T_CI_TEMP** • CCQ tables – **T_CCQ** • CCQ temporary tables – **T_CCQ_TEMP**
Rollback segment tablespace size	4000-MB Oracle 10G provides automatic undo management. For more information please check Oracle documentation.
Temporary tablespace	2000-MB

For OA configuration requirements, see OA *Installation Planning and Prerequisites*.

Detailed instructions on installation and configuration of an Oracle Server are beyond the scope of this manual. If you plan to use Oracle Server with Interaction Center but have not yet installed the Oracle Server, consult a qualified Oracle DBA for assistance.

Recommended values for installing Oracle 11g, 11g R2, and 12.1c server

The following table contains recommended values for certain options that you must select during an Oracle 11g installation. For more information about the options in an Oracle installer, see the documentation provided with your Oracle database.

1. You can configure Oracle 11g database using the Database Configuration Assistant.

2. Once you run the configuration tool, in step 4 of 15: Management Options, select the **Configure Enterprise Manager** check box, and click the Configure Database Control for local Management option.
3. In step 10 of 14: Initialization Parameters,
   a. Under the **Memory** tab, click the **Typical** option (Recommended) and specify Memory Size (SGA and PGA) as 600-MB.

      To allow Oracle to manage memory allocation, select the **Typical** option.

   b. Click the **Custom** option, select **Automatic Shared Memory Management** from the **Memory Management** drop-down list and specify the following:

      - SGA size = 450-MB
      - PGA size = 150-MB

   c. Under the **Character sets** tab, click the **Use Unicode** (AL32UTF8) option and select AL16UTF16 from the **National Character Set** drop-down list.
   d. Under the **Sizing** tab, specify the block size as 8192 (default).
   e. Under **Connection Mode**, click the **Dedicated Server Mode** option.
4. In step 13 of 14: Database Storage, under Redo Log Groups, specify the Log file size as 50 MB (default)

Detailed instructions on installation and configuration of an Oracle Server are beyond the scope of this manual. If you plan to use Oracle Server with Interaction Center, but have not yet installed the Oracle Server, consult an Oracle DBA for assistance.

Configuration settings for Oracle 11g, 11g R2, and 12.1c server

When you create the database instance for Interaction Center, you must include the following configurations:

Configuration	Required settings
db_block_size	8192 or higher
Dedicated connections	A minimum of 115 concurrently dedicated connections
Logging Parameters	Checkpoint Timeout of 0

Configuration	Required settings
Tablespaces	Two tablespaces for each Interaction Center database: one for standard database tables, one for temporary tables. For example, IC Repository and CCQ databases require the following tablespaces: • IC Repository tables – **T_CI** • IC Repository temporary tables – **T_CI_TEMP** • CCQ tables – **T_CCQ** • CCQ temporary tables – **T_CCQ_TEMP**
Rollback segment tablespace size	4000-MB Oracle 11G provides automatic Rollback Segment configuration, and it is recommended to be used in the automatic mode. For more information please check Oracle documentation.
Temporary tablespace	2000-MB

For OA configuration requirements, see OA *Installation Planning and Prerequisites*.

Detailed instructions on installation and configuration of an Oracle Server are beyond the scope of this manual. If you plan to use Oracle Server with Interaction Center, but have not yet installed the Oracle Server, consult an Oracle DBA for assistance.

Installing Oracle Client

Important:
For all supported databases, you must install the 32-bit version of the database client. Interaction Center does not support the use of 64-bit versions of database clients, even with 64-bit database server components.

You must install the appropriate version of the Oracle client on every computer that hosts an Interaction Center component that requires access to the database. For more information, see Location for database clients on page 213.

You can view complete installation instructions for the Oracle client from the Oracle Technology Network website.

IBM DB2

Interaction Center servers and client components support IBM DB2 9.5.

Important:
The DB2 version and Fix Pack version on the DB2 Server must match the versions on the DB2 Client.

This section includes the following topics:

- Supported versions of DB2 on page 226
- Required version mode for IBM DB2 Client on page 226
- Location of IBM DB2 Server on page 226
- Configuring IBM DB2 server for Interaction Center on page 226
- Installing IBM DB2 Client on page 228
- Configuring IBM DB2 client for Interaction Center on page 228
- Troubleshooting DB2 SQL1131N DARI error for IBM DB 9.5 on AIX 6.1 on page 229

Supported versions of DB2

The following table lists the releases of the IBM DB2 database that are supported by Interaction Center servers and client components.

IBM DB2 version	Bit mode
DB2 9.5	32-bit only

Required version mode for IBM DB2 Client

You must install the DB2 client software in 32-bit mode. The Interaction Center Data server for DB2 uses 32-bit DB2 libraries. The Interaction Center Data server does not function if you install DB2 clients in 64-bit mode.

Location of IBM DB2 Server

Install and configure the IBM DB2 server on all AIX computers that host the database instance for Interaction Center databases.

Configuring IBM DB2 server for Interaction Center

This section includes the following topics which describe the configuration parameters for IBM DB2:

- DB2 registry variables on page 227
- Automatic configuration parameters on page 227
- Manual configuration parameters on page 227

DB2 registry variables

The following table includes the DB2 registry variables required for Interaction Center.

DB2 registry variable	Recommended entry	IBM DB2 9.5
DB2_INDEX_2BYTEVARLEN	yes	-
DB2_STRIPED_CONTAINERS	yes	
DB2_RR_TO_RS	YES_OVERRIDE_RI	
DB2COMM	tcpip	

Manual configuration parameters

The following table includes DB2 configuration parameters required for Interaction Center. You must configure these parameters manually. Database Designer does not automatically configure the DB2 configuration parameters.

Configuration parameter	Required minimum setting
APP_CTL_HEAP_SZ	256
MAXLOCKS	22
MAXAPPLS	500

Automatic configuration parameters

You should use the Database Designer to create and configure Interaction Center databases in DB2. Database Designer automatically sets the configuration parameters in the following table:

Configuration parameter	Required minimum setting
Database code set	UTF-8
Territory	US
pagesize	8KB
APPLHEAPSZ	512
bufferpool BUFFERPOOL8K	1000

Configuration parameter	Required minimum setting
tablespace USERSPACE8K	• pagesize: 8k • bufferpool: BUFFERPOOL8K
tablespace TEMPSPACE8K	• pagesize: 8k • bufferpool: BUFFERPOOL8K

Installing IBM DB2 Client

Important:
For all supported databases, you must install the 32-bit version of the database client. Interaction Center does not support the use of 64-bit versions of database clients, even with 64-bit database server components.

You must install the appropriate version of the IBM DB2 client on every computer that hosts an Interaction Center component that requires access to the client. For more information, see Location for database clients on page 213.

When you install IBM DB2 Client, select a typical install.

Configuring IBM DB2 client for Interaction Center

You must catalog the IBM DB2 client on every computer that hosts a secondary Interaction Center Data server.

You do not need to catalog the IBM DB2 client on the computer that hosts the primary Data server that you used to connect to the database computer to configure the Interaction Center databases. The IBM DB2 client on that computer is catalogued when Database Designer creates the databases.

If you did not use Database Designer to create the databases, you need to catalogue the nodes on all IBM DB2 clients.

For more information about how to catalog the databases on an IBM DB2 client, see the DB2 documentation.

Troubleshooting DB2 SQL1131N DARI error for IBM DB 9.5 on AIX 6.1

Problem: While configuring the DB2 database, updating the agent records or email accounts, the Alarm Monitor displays the ***SQL1131N DARI (Stored Procedure) process has been terminated abnormally. SQLSTATE=38503*** error message. Intermittently, you can observe this error while doing other operations.

Solution: In order to resolve the error, you must run the following commands on the DB2 CLI prompt.

1. db2 update dbm cfg using keep fenced no
2. db2stop force
3. db2start

Running these commands sets the `KEEPFENCED` parameter value to `NO` for the entire DB database. Setting this parameter might impact the performance. To improve the performance, you must turn the logging off by removing or commenting the logging related information in the `db2cli.ini` file. The `db2cli.ini` files looks as shown below:

```
[tstcli1x]
uid=userid
pwd=password
autocommit=0
TableType="'TABLE','VIEW','SYSTEM TABLE'"

[tstcli2x]
; Assuming dbalias2 is a database in DB2 for MVS.
SchemaList="'OWNER1','OWNER2',CURRENT SQLID"

[MyVeryLongDBALIASName]
dbalias=dbalias3
SysSchema=MYSCHEMA
```

You can observe that the `[Common]` section, which contains logging information, is not available in the file. You can also comment the logging options available in the `[Common]` section.

After settings these parameters, follow the steps mentioned in the *IC Installation Planning and Prerequisites Guide* to configure the DB database.

Chapter 10: Supported Telephony switches and software

This section includes the following topics:

- Exceptions for Telephony software and switches on page 231
- Avaya Aura® Communication Manager products on page 231

Interaction Center supports these telephony products over various protocols. The supported switches interface with Interaction Center in various ways. For example, a switch connects directly to the Interaction Center Telephony server. Avaya products use this interface.

Exceptions for Telephony software and switches

The following table contains exceptions for telephony support for certain Interaction Center components:

Interaction Center component	Supported Telephony software and switch
Business Advocate	Support for multiple announcements is only available with Avaya Aura® Communication Manager 5.x or later.

Avaya Aura® Communication Manager products

Interaction Center supports the following Avaya Aura® Communication Manager products:

- Communication Manager 5.x
- Communication Manager 6.x
- Communication Manager 7.x (supported from Release 7.3.4)

For more information about the definition of the supported versions and about subsequent updates or service packs of the software, see About the supported versions on page 286.

For more information about the interface between Avaya products and the Interaction Center Telephony server, see *IC Telephony Connectors Programmer Guide*.

This section includes the following topics:

- Supported components on page 232
- Requirements for Avaya Aura® Communication Manager products on page 233
- Downloading the Avaya Aura® Application Enablement Services - CVLAN client on page 234

Supported components

The following table describes the support for Interaction Center components and features with the supported Avaya Aura® Communication Manager products:

Switch	Supported operating systems for Telephony server	Multi-Site Heterogeneous Switch	Protocol
Communication Manager: • 5.x • 6.0.x • 6.2.x • 6.3.x • 7.0.x	• Microsoft Windows Server 2012 R2 (Standard and Datacenter edition) • Microsoft Windows Server 2008 R2 (Standard, Enterprise, and Datacenter edition) • Oracle Solaris 10 update 9 • AIX 6.1 (AIX 6.1 is not supported from Release 7.3.3 of AIC.)	Yes	ASAI

Requirements for Avaya Aura® Communication Manager products

Install the following for Avaya Aura® Communication Manager products. Consult the administrator responsible for the Avaya Aura® Communication Manager Call Center at your site for more detailed information about these requirements.

Important:
Interaction Center requires Call Center Elite. Call Center Elite includes Expert Agent Selection. Telephony in Interaction Center uses Expert Agent Selection to improve the synchronization between the agent desktop telephone and the Avaya Agent Softphone. These improvements were made available through tighter linkages with ASAI Agent States.

Install AES / CVLAN Client version 4.2 or later to use the Service Observer feature of your Avaya Aura® Communication Manager products. Do not use version 8.2.1 of the CVLAN Client. Version 8.2.1 can cause the Telephony server to fail under a moderate load.

For detailed information about the requirements for Avaya Aura® Communication Manager products, see Requirements for supported Avaya switches and software on page 293.

The following table shows the compatibility matrix for IC and AES:

IC 7.3	AES / Avaya Aura® Application Enablement Services - CVLAN client	AES Server
Windows	6.1,7.0.1	5.2.x, 6.1, 7.0.1
Oracle Solaris	3.1-25	5.2.x
		6.1
AIX	3.1-9	5.2.x
		6.1

For IC 7.3.3 release, AES CVLAN Client 6.3.3 is supported on Microsoft Windows Server 2008 R2 and Microsoft Windows Server 2012 R2 with AES Server 6.3.x.

Downloading the Avaya Aura® Application Enablement Services - CVLAN client

To download and install AES / CVLAN client refer to Avaya Aura® Application Enablement Services - CVLAN client Client installation on page 341.

Chapter 11: Supported Web servers

This section provides information about the supported Web servers. This section includes the following topics:

- Components that require a Web server on page 235
- Microsoft Internet Information Server on page 235
- Oracle iPlanet Web Server on page 237
- IBM HTTP Server on page 238
- Configuring Tomcat for Interaction Center Client SDK server and Web Services server (Optional) on page 240



Tip:
For information about the Web servers supported for each operating system, see Required software for Interaction Center servers on page 287.

Components that require a Web server

The following Avaya Interaction Center (Interaction Center) components require a Web server:

- Web Management external website with chat and ICM server.
- Web Management administration website.
- Email Management Template Administration.
- Web License Manager.
- Avaya Agent Web Client.

Microsoft Internet Information Server

If your system uses Windows Server to host the Interaction Center servers, you must use Microsoft IIS as your Web server.

- Microsoft IIS 7.5 is part of the Windows Server 2008 R2 operating system.
- Microsoft IIS 8 is part of the Windows Server 2012 R2 operating system.

For information on how to configure and use Microsoft IIS, see the documentation for the Windows Server operating system.

This section includes the following topics:

- Security patches and hot fixes for Microsoft IIS on page 236
- Configuring MIME types for Microsoft IIS on page 236

Security patches and hot fixes for Microsoft IIS

You need to check the Microsoft website for security bulletins and hot fixes for Microsoft IIS that describe the possible security issues and solutions. Review the security bulletins after you install Microsoft IIS, make any required configuration changes, and apply the required patches.

You can find a listing of current security bulletins, patches, and hot fixes for Microsoft IIS from the following website: http://www.microsoft.com/technet/security/current.aspx

Continue to monitor the Microsoft security bulletins and apply all future hot fixes when they are made available.

Configuring MIME types for Microsoft IIS

Configure the MIME types in the following table using **MIME Types** in the **Home** pane of the Default Website:

Extension	MIME type
.dll	application/x-msdownload
.ini	text/html
.imp	text/html
.txt	text/html

IIS Roles

For details on the IIS Web Server Role and the required services, refer to Roles on page 264.

Oracle iPlanet Web Server

The type of Web server required for Interaction Center servers depends upon the version of Oracle Solaris. This section provides information specific to Interaction Center that you need to install and configure a supported version of Oracle iPlanet Web Server.

This section includes the following topics:

- Supported versions of Oracle iPlanet Web server 7.0.13 on page 237
- Oracle iPlanet 7 Web Server configuration parameters on page 237

Supported versions of Oracle iPlanet Web server 7.0.13

Interaction Center supports Oracle iPlanet 7.0.13 Web Server on Oracle Solaris only. You can download the Oracle iPlanet 7.0.13 Web server from the Oracle website.

Oracle iPlanet 7 Web Server configuration parameters

A detailed guide to installing and configuring an Oracle iPlanet 7.0.13 Web Server is beyond the scope of this document. For more information about the Oracle iPlanet Web Servers, see the documentation provided by Oracle on the Oracle website.

The following table includes some recommended values when you install Oracle iPlanet Web server to use with Interaction Center.

Parameter	Value
Installation type	Typical installation
Installation components	• All • Server Core • Java Development Kit
Computer name	Default

Parameter	Value
System User / Group	Choose a UNIX user and group to represent the Oracle iPlanet Web Server in the user directory. The Web Server runs as this user. This user must have no privileges in the computer network system. The Administration Server gives this group some permissions in the server root to perform server-specific operations. If you have not yet created a user and group for the Web Server, create this user and group using your native UNIX system utilities.
Run Web Server Administration Server user	The Web Server Administration Server is different from other Web servers on the system. The Web Server Administration Server must run with a different user id than those used by the other Web servers on the computer. The Administration Server user is the only user able to write Web server configuration files. **Note:** If the Web Server Administration Server is run as "root", you can use the administration interface to start and stop the other Web servers.
Web Server Admin User Name/ Password	The Web Server Administration Server requires its own administrative user name and password for GUI access. When you access the Web Server Administration Server interface, it prompts you for the administrative user name and password. For example, select admin/admin
Web Server Admin Server Port	8989
Web Server Port	80
Web Server Content Root	Default

IBM HTTP Server

This section provides information specific to Interaction Center that you need to install and configure the supported version of IBM HTTP Server.

This section includes the following topics:

- Supported version of IBM HTTP server on page 239
- Restriction on the deployment of IBM HTTP Server on page 239

- IBM HTTP Server configuration parameters on page 239

You can obtain more information about IBM HTTP Server 7.0 from the IBM website.

Supported version of IBM HTTP server

If your system uses AIX 6.1 as the operating system for the Interaction Center servers, you must use IBM HTTP Server, release 7.0 as your Web server.

Restriction on the deployment of IBM HTTP Server

Install the WebConnector on a computer that is separate from the Interaction Center server and OA server. The HTTP Server can reside on the same computer as WebConnector, but this is not recommended. For more information about installing OA, see OA *Installation Planning and Prerequisites*.

IBM HTTP Server configuration parameters

A detailed guide to installing and configuring IBM HTTP Server is beyond the scope of this document. See the installation guide for IBM HTTP Server.

When you install and configure IBM HTTP Server, use the following parameters:

Parameter	Value
ServerName Property is in the following file: `<IBMHttPServer_installation_root>/conf/httpd.conf`	Fully-qualified domain name of the computer that hosts the IBM HTTP Server. **CAUTION:** Do not use `localhost` for the value. A value of `localhost` for `ServerName` causes an infinite redirection loop when you access the Administration website.

Configuring Tomcat for Interaction Center Client SDK server and Web Services server (Optional)

Interaction Center installs Tomcat with the Interaction Center core servers component. Tomcat is the servlet container of the Jakarta Project. Tomcat is developed in an open and participatory environment and released under the Apache Software License.

Important:
To obtain assistance from professional services with deploying load balancing, failover, or SSL for the Client SDK and Interaction Center Web Services, contact your Avaya representative.

This section includes the following topics:

- Installation location for Tomcat on page 240
- Default web application contexts on page 240
- Setting up load balancing or failover on page 241
- Using Jakarta Tomcat Connector to configure a stand-alone HTTP server on page 241

Installation location for Tomcat

Interaction Center installs the Tomcat server in the following directory for the Client SDK and Web Services:

IC_INSTALL_DIR\IC73\tomcat

Default web application contexts

The following table lists the default web application contexts configured by Interaction Center in Tomcat:

Server	Default web application context	Installation location
Client SDK server	icsdk	*IC_INSTALL_DIR*\IC73\sdk\server
Web services server	webservices	*IC_INSTALL_DIR*\IC73\sdk\webservices

Setting up load balancing or failover

To configure Tomcat to support load balancing or failover for the Client SDK server or Web Services server, see the Apache website.

Using Jakarta Tomcat Connector to configure a stand-alone HTTP server

Note:
Follow the instructions in this section only if you want to front Tomcat Server with a stand-alone HTTP server.

To use the Jakarta Tomcat Connector to configure a stand-alone HTTP Server with Tomcat:

1. Set up Tomcat, as described in the Tomcat documentation. For more information go to Apache website and search for Tomcat Load Balancer and Tomcat connectors.
2. If your Tomcat configuration includes the AJP 1.3 connector, you can uncomment the lines in the appropriate server configuration file:
   a. In a text editor, such as Notepad, open one of the following server configuration files:
      - For the Client SDK server:
        IC_INSTALL_DIR\IC73\tomcat\conf\server.icsdk.xml
      - For the Web Services server:
        IC_INSTALL_DIR\IC73\tomcat\conf\server.icwebservices.xml
   b. Search for the XML tag with the following attribute:

      ```
      protocol="AJP/1.3"
      ```

   c. Remove the comment tags surrounding that XML tag.
   d. Save the server configuration file.

Comments on this document? infodev@avaya.com

Chapter 12: Supported email servers

Certain components of Avaya Interaction Center require access to email servers that support the following protocols:

SMTP

- RFC 1893 Enhanced Mail System Status Codes
- RFC 2034 SMTP Service Extension for Returning Enhanced Error Codes
- RFC 1652 SMTP Service Extension for 8bit-MIMEtransport
- RFC 1869 SMTP Service Extensions
- RFC 1870 SMTP Service Extension for Message Size Declaration
- RFC 1891 SMTP Service Extension for Delivery Status Notifications
- RFC 2554 SMTP Service Extension for Authentication
- RFC 2821 Simple Mail Transfer Protocol
- RFC 3030 SMTP Service Extensions for Transmission of Large and Binary MIME Messages

POP3

- RFC 1939 Post Office Protocol - Version 3
- RFC 1734 POP3 AUTHentication command
- RFC 2449 POP3 Extension Mechanism
- RFC 2195 IMAP/POP AUTHorize Extension for Simple Challenge/Response

IMAP4

- RFC 3501 Internet Message Access Protocol - Version 4 rev 1
- RFC 1731 IMAP4 Authentication Mechanisms
- RFC 2195 IMAP/POP AUTHorize Extension for Simple Challenge/Response

Secure

Hunny Mail++ supports TLS (also known as SSL) through tunneling, alternate secure ports, and upward negotiation. The following RFCs are supported:

- RFC 2246 The TLS Protocol Version 1.0
- RFC 2595 Using TLS with IMAP, POP3, and ACAP
- RFC 2487 SMTP Service Extension for Secure SMTP over TLS

SMTP and POP3 / IMAP4 are standard Internet email protocols. Most common mail servers, such as Microsoft Exchange and Lotus Notes, support these protocols. You need to install or configure your enterprise email server to support SMTP and POP3 / IMAP4 services.

CAUTION:
Turn off Microsoft Word Autocorrect features if you use Word as the editor for Outlook. The Autocorrect features can cause application errors in the Interaction Center agent desktop.

Note:

- Microsoft Exchange 2003 and 2007 is supported from IC 7.3 onwards.
- Microsoft Exchange 2010 is supported from IC 7.3.1 onwards.
- Microsoft Exchange 2013 is supported from IC 7.3.4 onwards.
- IC 7.3 is certified with IBM Lotus Domino 7.
- Microsoft Exchange 2016 is supported from IC 7.3.5 onwards.

Configuring SMTP and POP3 / IMAP4 servers

Email Management works closely with other servers and applications on your Local Area Network.

To configure your email system:

1. Configure your mail server to allow POP3 / IMAP4 and SMTP access.

   The Avaya Email Server uses a POP3 / IMAP4 server to retrieve incoming messages, and uses an SMTP server to send outgoing messages.

2. Define an email address for your email system that matches the following configuration. You will set this configuration in the Notification server:

   - Email server name
   - Domain name
   - Default email sender name, for example user@xyzcorp.com

Note:
For IMAP4, specify the folder that is used for accessing emails.

3. Verify the email system on the computer, as described in the following table.

Operating system	Verification step
Windows	Notification server verifies the ability to send a simple email contact to the default email sender name. The Notification server does not start if the email address is invalid.

Oracle Solaris	You must verify that the default email sender name is accessible from the mail daemon on the computer that hosts the Notification server.
	Execute the following command from any directory to send a simple text message:
	`mail <email_address>`
	`test`
	`.`
	Where <*email_address*> is the default email sender name. For example, enter `user@xyzcorp.com`

AIX	You must verify that the default email sender name is accessible from the mail daemon on the computer that hosts the Notification server.
	Execute the following command from any directory to send a simple text message:
	`mail <email_address>`
	`test`
	`.`
	Where <*email_address*> is the default email sender name. For example, enter `user@xyzcorp.com`

4. Remove all aliases and distribution lists from the mail accounts that Email Management handles.

   To avoid potential mail loops, do not include mail accounts that are polled by Email Management in any distribution lists or aliases.

5. Configure your firewall for Email Management:
   - To send messages to the SMTP server on port 25.
   - To retrieve messages from the POP3 server on port 110 or on port 995 (If TLS is activated).
   - To retrieve messages form the IMAP4 server on port 143 or on port 993 (If TLS is activated).
   - To allow agent computers to communicate with the Email server on port 19113.
   - To allow administrators to communicate with Mail Template Administration on port 19114.

6. Enable SMTP relaying if Email Management sends replies to customers outside the local domain.

Configuring security certificates for TLS

Avaya IC 7.3.x supports SSL for Transport Layer Security (TLS) to secure email messages.

For securing email messages, use TLS option while configuring your email accounts. For more information about enabling TLS, see *IC Installation and Configuration* guide.

Before using TLS, ensure that you have the following certificates from a certifying authority.

- Server side certificate - generated for template Webserver
- Root certificate of the certifying authority

The certificates must be in PEM format.

If they are not in the required format you need to convert them using the OpenSSL utility. You can download the OpenSSL utility from the OpenSSL website.

For more information, see *IC Installation and Configuration* guide.

Chapter 13: Business Advocate

You must configure the operating system and database for Business Advocate before you install Avaya Interaction Center (Interaction Center). The configuration steps are different for each supported operating system and database.

This section describes the operating systems and databases supported by Business Advocate and the configuration steps for each supported platform. This section includes the following topics:

- Exceptions to platform support for Business Advocate on page 247
- Configuring Windows for Business Advocate on page 248
- Configuring SQL Server for Business Advocate on page 252
- Configuring Oracle for Business Advocate on page 254

Exceptions to platform support for Business Advocate

The following table describes the exceptions to platform support for Business Advocate for Interaction Center. For information about which platforms are supported by Business Advocate, see Required software for Business Advocate on page 299.

Platform	Exception
Operating system	Resource Manager servers support only Windows. No AIX or Oracle Solaris support for Resource Manager servers. Business Advocate does not function with the Resource Managers servers on AIX or Oracle Solaris.
Database	Advocate database supports only SQL Server or Oracle. No DB2 support for the Advocate database. Agent administration for Business Advocate does not function with the Advocate database on DB2. You can use DB2 for the other Interaction Center databases.

Configuring Windows for Business Advocate

If your Interaction Center system includes Business Advocate, you must install the Microsoft Message Queuing service (MSMQ) support on the computer that hosts the Resource Manager server. This computer serves as your MSMQ client for Business Advocate.

Tip:
You need a Windows CD-ROM for these steps.

This section includes the following topics:

- Business Advocate implementation modes on page 248
- Implementing Business Advocate in Workgroup mode on page 248
- Implementing Business Advocate in Active Directory mode on page 249
- Installing the Managing Message Queuing (MSMQ) service on page 250
- Configuring Windows for Thai (optional) on page 250

Business Advocate implementation modes

You can choose between the following implementation modes when you implement Business Advocate:

Active Directory mode: Use the Active Directory mode for a large, complex Business Advocate deployment. The Active Directory mode implements Windows Active Directory for user services.

Workgroup mode: Use the Workgroup mode for a less complex Business Advocate deployment or if you do not want to implement Windows Active Directory.

Implementing Business Advocate in Workgroup mode

For more information about how to install and configure the Workgroup mode for Windows Server, see the Microsoft documentation provided with the operating system software and the following Microsoft articles:

- http://support.microsoft.com/default.aspx?scid=kb;en-us;299909
- http://msdn.microsoft.com/library/default.asp?url=/library/en-us/rpc/rpc/rpc_security_essentials.asp

To implement Business Advocate in the Workgroup mode:

1. Configure all computers that host Business Advocate components in the Windows Workgroup mode.
2. To ensure that the Business Advocate processes on different computers can communicate, configure Windows RPC/DCOM/MTS and MSMQ security permissions for secure access on all computers that host the following Business Advocate components:
   - Business Advocate administrative tools on a computer that does not also host a Resource Manager server.
   - A standby Resource Manager server.

   You do not need to configure RPC/DCOM/MTS between the computers that host the primary Logical Resource Manager or an additional Logical Resource Manager.
3. Create an administrative user with the same loginID and password on all Windows computers that host Business Advocate components. Assign "Logon as Service" privileges to all of these administrative users.
4. Install the MSMQ service on all computers that host Business Advocate components, as described in Installing the Managing Message Queuing (MSMQ) service on page 250.

Implementing Business Advocate in Active Directory mode

For more information about how to install and configure Active Directory for Windows Server, see the Microsoft documentation provided with the operating system software.

Tip:
If the Business Advocate system includes Active Directory integration and the MSMQ service is already installed and configured, you have to re-install the service on that computer after you join the computer to the Active Directory domain.

To implement Business Advocate in Active Directory mode:

1. If your network does not include an Active Directory domain, create a new Active Directory domain.

   A computer that hosts one or more Business Advocate servers can serve as the Active Directory domain controller.
2. Join all Windows computers that host Business Advocate servers and Business Advocate administration to the same Active Directory Domain. If your Interaction Center system includes servers on Oracle Solaris or AIX, join all Windows computers that host Resource Manager servers to the same Active Directory domain.
3. Create an Active Directory user and assign the user the local administrator and "Logon as Service" privileges on all the Business Advocate servers.
4. Install the MSMQ service on all computers that host Business Advocate components, as described in Installing the Managing Message Queuing (MSMQ) service on page 250.

Configuring Business Advocate (BA) on the Windows Server 2019

To configure Business Advocate on the Windows Server 2019, the following steps need to be performed:

1. Switch off **Exploit Protection**.
   1.1. Open the **Exploit Protection.**
   1.2 Open the **System Settings.**
   1.3 Under the **System Settings** change the settings of the attributes mentioned in the following table:

Item	Change to
Control flow guard (CFG)	Off by default
Data Execution Prevention (DEP)	Off by default
Force randomization for images (Mandatory ASLR)	Off by default
Randomize memory allocations (Bottom-up ASLR)	Off by default
High-entropy ASLR	Use default (On)
Validate exception chains (SEHOP)	Off by default
Validate heap integrity	Off by default

2. Install **Avaya Interaction Center**.
3. Configure **Business Advocate**.
4. After **Business Advocate** configuration is complete, you need to check registry branch
5. `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\MMC\SnapIns\{20D604E0-6E00-11D2-A94C-00A0C985986D}`
6. This branch should exist for appropriate functioning of Advocate Component Manager.

Installing the Managing Message Queuing (MSMQ) service

To install MSMQ service for Microsoft Windows Server 2008 R2 and 2012 R2:

1. If you have not already done so, log in to the computer with an account that has local administrator privileges.
2. Select **Start** > **Administrative Tools > Server Manager**.
3. In Server Manager, click **Features**.
4. In the right-hand pane under **Features Summary**, click **Add Features**.
5. In the resulting window, expand **Message Queuing**.
6. Expand Message Queuing Services.
7. Click **Directory Services Integration** (for computers joined to a Domain), then click **HTTP Support**.
8. Click **Next**.
9. Click **Install**.

Note:
The MSMQ service cannot send or receive messages until a connection with a Message Queuing server is established.

Configuring Windows for Thai (optional)

If you install Windows with an English CD-ROM, and then configure for Thai, you must configure Windows to display the Thai characters. If you do not configure Windows correctly:

- Business Advocate Supervisor displays Thai characters as question marks when creating qualifiers.
- OA events for updating qualifiers do not function correctly.

Important:
You must configure Windows for Thai before you install the SQL Server database. You may encounter problems if either the database or Business Advocate is installed before the operating system is changed to Thai.

To retrieve and display Thai characters correctly in an English version of Windows:

1. Change the value of the **Default Locale** configuration parameter to Thai.
2. Change the value of the **System Locale** configuration parameter to Thai.

3. Change the value of the **User Locale** configuration parameter to Thai.

   After you configure the English version of Windows for Thai, install SQL Server on the computer.

Creating a user to configure the BA tool

Problem: You may get the following error message while starting the BA config tool.

```
Unable to start avaya business advocate component manager service
```

Solution:

1. Click **Start** > **Administrative Tools** > **Local Security Policies**.
2. In the **Local Security Policy** window, in the left-hand side pane, under **Local Policies** select **User Right Assignment**.
3. In the right -hand side pane, double-click **Log on as a Service**.
4. Add your BA user.

Configuring SQL Server for Business Advocate

Business Advocate does not use Database Designer to create and configure the Advocate database. You must create and configure the Advocate database before you install the Business Advocate components.

To configure SQL Server for Business Advocate, perform the steps in the following sections:

- Creating a database for Business Advocate on page 252
- Configuring the SQL Server client on page 252
- Configuring a user to run Business Advocate services on page 253
- Configuring SQL Server for Thai (optional) on page 254

Creating a database for Business Advocate

With SQL Server Enterprise Manager, create a database with the properties in the following table.

Property	Value
Database name	advocate **Note:** You can use a different name if desired. However, you should name this database "advocate" for easy identification.
Main schema size	10-MB or more
Log size	20-MB or more

Note:
For each additional Logical Resource Manager, you need to create a separate database with a different database name. For example, `advocate_lrm2`.

Configuring the SQL Server client

On every computer that hosts one or more Business Advocate servers, do the following:

1. Install the SQL Server Client, Microsoft Data Access Component.

2. Configure the Client to access the computer that hosts your Advocate databases with TCP/IP protocol, using the correct server port, as follows:
   a. Run the SQL Server Client Network Utility.

      If you installed the SQL Server Client in the default location, you can find the Client Network Utility in the following folder: `C:\Windows\SysWOW64\cliconfg.exe`

   b. On the **Alias** tab page, add an alias with the properties in the following table:

Property	Value
Server alias	Name of the computer that hosts SQL Server. **Note:** You can use a different name if desired. However, you should use this naming convention for easy identification.
Network libraries	TCP/IP.
Server name	Name of the computer that hosts your Advocate database.
Dynamically determine port	Do not select this check box.
Port number	Enter the port number that the client uses to communicate with the Advocate database.

Configuring a user to run Business Advocate services

Create and configure a user to run Business Advocate services:

1. Create a user account for Business Advocate.

   If your Business Advocate system includes the optional Active Directory integration, you must create an Active Directory user account for Business Advocate.

2. Configure the Business Advocate user account with the following rights and permissions:
   - Read, write, and execute permissions to the Nethome network share.
   - Create, delete, and access permissions for MSMQ queues.
   - Send and receive rights for MSMQ events.
   - Logon as a service permissions on every computer that hosts Business Advocate servers.
   - Local administrative rights on every computer that hosts Business Advocate servers.

   For information about how to assign these rights and permissions to the user account, see the documentation provided by Microsoft.

Configuring SQL Server for Thai (optional)

If you install Windows with an English CD-ROM, then configure for Thai, you must configure SQL Server to display the Thai characters. If you do not configure SQL Server correctly:

- Business Advocate Supervisor displays the Thai characters as question marks when creating qualifiers.
- OA events for updating qualifiers do not function correctly.

Important:
You must configure Windows for Thai before you install the SQL Server database. For more information, see Configuring Windows for Thai (optional) on page 250. You must configure SQL Server for Thai before you install Business Advocate.

To retrieve and display the Thai characters correctly for the SQL Server on an English version of Windows:

1. Open Enterprise Manager for SQL Server.
2. Verify that the value of the Collation parameter is Thai:
   a. Right-click on the Advocate database and click **Properties**.
   b. On the **General** tab, confirm that the value of the **Collation Name** field in the **Maintenance** group is Thai.

   After you complete this configuration, you can install Interaction Center and Business Advocate components.

Configuring Oracle for Business Advocate

Business Advocate supports Oracle 10g and Oracle 11g on Windows and Oracle Solaris. The steps to configure both versions of Oracle are almost identical.

If your Interaction Center system includes Business Advocate and an Oracle database, perform the steps in the following topics:

- Location of Oracle components for Business Advocate on page 255
- Creating tablespaces for the Business Advocate database on page 255
- Creating Oracle users for Business Advocate on page 256
- Installing the Oracle Client on page 257

Location of Oracle components for Business Advocate

The following table shows which Oracle components you need to install for Business Advocate. For more information, see the documentation provided with your Oracle database software.

Computer	Required Oracle components
Computer that hosts your Business Advocate database	Install the following components: Supported operating system: • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 R2 • Oracle Solaris 10 Supported Oracle database: • Oracle Enterprise Server 10g • Oracle 11g • Oracle 11g R2 • Oracle 11.2g • Oracle 12c
On every computer that hosts a Resource Manager server	Install the Oracle Client with all the required patches.

Creating tablespaces for the Business Advocate database

You must create a tablespace for every computer that hosts Business Advocate servers. Create these tablespaces on the computer that hosts your Business Advocate database.

To create a tablespace:

1. Open the Oracle DBA Studio standalone.
2. Create a tablespace with the properties described in the following table.

Window	Property	Recommended value
Database Connection Information	Username	Internal Note: Internal is the recommended value that means system predefined user account(SYSTEM, SYS, other internal user accounts). For more information, refer to *Oracle documentation.*
	Password	oracle

	Connect as	SYSOPER

Comments on this document? infodev@avaya.com

Window	Property	Recommended value
General tab of Create Tablespace	Name	Enter a name for the tablespace. For example, enter ADVOCATETBS.
	Drive used for directory	E If possible, use drive E for the Business Advocate tablespace, and use drive D for the system tablespace. This configuration reduces the I/O burden on the drive for the system tablespace.
	Size	Enter an appropriate size. The minimum tablespace size is 100 MB.

Creating Oracle users for Business Advocate

You must create a unique Oracle user for every Logical Resource Manager in the Business Advocate system. Create these Oracle users on the computer that hosts the Business Advocate database.

Important:
To ensure that Business Advocate can create the schema in Oracle, the user name must start with a letter, and can contain only letters, digits, and underscore characters.

To create an Oracle user:

1. Open the Oracle DBA Studio standalone.

2. Create a user with the properties described in the following table:

Window	Property	Recommended value
General tab of Create User	Name	Enter a name for the user. For example, enter advocate. Caution: To ensure that Business Advocate can create the schema in Oracle, the user name must: • Start with a letter. • Contain only letters, digits, and underscore characters.
	Password	Enter a password for the user. For example, enter advocatepw.
	Confirm	Re-enter the password.
	Tablespaces Default	Enter the name of the Business Advocate database. For example, enter ADVOCATEDB.
Role tab of Create User	Available roles	Select the following role and move to the **Granted** column: • DBA
System Privileges tab of Create User	Available system privileges	Select the following system privilege and move to the **Granted** column: • UNLIMITED TABLESPACE

Installing the Oracle Client

When you install the Oracle Client, install the Oracle ODBC connector on the computer that hosts your Oracle database server. Do not install the Microsoft Oracle ODBC connector.

Important:
For all supported databases, you must install the 32-bit version of the database client. Interaction Center does not support the use of 64-bit versions of database clients, even with 64-bit database server components.

Chapter 14: Network configuration

You need to configure your network for Avaya Interaction Center. To set up your network, perform the steps in the following sections:

- Enabling TCP/IP networking on page 259
- Verifying DNS resolution on page 259

For additional network information, see Network topology and configuration guidelines on page 38.

Enabling TCP/IP networking

All Interaction Center servers and client applications use TCP/IP to communicate. You need to enable TCP/IP networking on each computer in an Interaction Center system.

By default, Windows and UNIX operating systems include TCP/IP networking on all computers with network cards. Typically, Interaction Center uses the default TCP/IP settings applied during installation.

However, if you deploy Interaction Center on an existing Novell NetWare network, you may need to take additional steps to configure the TCP/IP networking protocol. You can obtain information on how to install and configure TCP/IP networking on a NetWare network from your IT professionals.

Verifying DNS resolution

Before you install software for Web Management or Email Management, you must verify the domain name system (DNS) resolution on each computer.

Each Web Management server and Email Management server must have a Fully Qualified Domain Name (FQDN) that:

- Has a minimum of three parts, separated with periods.

  For example, **`bsmith.com`** only has two parts and would not qualify. **`bsmith.domain.com`** has three parts and would qualify.
- Does not contain special characters, except the dash (**-**).
- Has forward and reverse DNS mapping in public DNS records.

To verify the DNS resolution on computers in your Interaction Center system, perform the steps in one of the following sections:

- Verifying DNS resolution in Windows on page 260
- Verifying DNS resolution on Oracle Solaris and AIX on page 261

Verifying DNS resolution in Windows

The following procedure verifies that DNS is configured properly for Windows. Perform this procedure on every Interaction Center server that has a Windows operating system.

To verify DNS resolution in Windows:

1. Open a command prompt window.
2. To find the computer's IP address, type **ipconfig** at the prompt.

   The system returns information about the computer's IP configuration, including the IP address (`254.24.167.211`), as shown in the following example:

   ```
   Windows NT IP Configuration

   Ethernet adapter El70x1:

   IP Address. . . . . . . . . . : 254.24.167.211
     Subnet Mask . . . . . . . . . : 255.255.255.0
     Default Gateway . . . . . . . :  254.24.167.1
   ```

3. To verify the "forward" DNS mapping, type the following command with the computer's FQDN at the prompt:

   nslookup <*computer_name*>.<*domain_name*>

   The system returns information about the computer's forward DNS mapping, including the computer's IP address and FQDN. The following example of forward DNS mapping indicates that the FQDN `bsmith.domain.com` is assigned to the IP address `254.24.167.211` in public DNS records.

   ```
   Server: ns3.domain.com
     Address:  254.24.167.23

   Name:    bsmith.domain.com
     Address:  254.24.167.211
   ```

4. To verify the “reverse” DNS mapping, type the following command with the computer’s IP address at the prompt:

   nslookup <*IP_address*>

   The system returns information about the computer’s reverse DNS mapping, as shown in the following example:

```
Server: ns3.domain.com
  Address:  254.24.167.23

Name:    bsmith.domain.com
  Address:  254.24.167.211
```

Verifying DNS resolution on Oracle Solaris and AIX

The following procedure verifies that DNS is configured properly for Oracle Solaris and AIX. Perform this procedure on every Interaction Center server with a UNIX operating system.

To verify DNS resolution on Oracle Solaris and AIX:

1. Open the **hosts** file and locate the information about the computer’s IP configuration, including the IP address (`254.24.167.211`).
2. To verify the “forward” DNS mapping, type the following command with the computer’s FQDN at the prompt:

   nslookup <*computer_name*>.<*domain_name*>

   The system returns information about the computer’s forward DNS mapping, including the computer’s IP address and FQDN. The following example of forward DNS mapping indicates that the FQDN `bsmith.domain.com` is assigned to the IP address `254.24.167.211` in public DNS records.

```
Server: ns3.domain.com
  Address:  254.24.167.23

Name:    bsmith.domain.com
  Address:  254.24.167.211
```

3. To verify the “reverse” DNS mapping, type the following command with the computer’s IP address at the prompt:

   nslookup <*IP_address*>

   The system returns information about the computer’s reverse DNS mapping, as shown in the following example:

```
Server: ns3.domain.com
  Address:  254.24.167.23

Name:    bsmith.domain.com
  Address:  254.24.167.211
```

Troubleshooting an unresolved DNS entry

If a DNS entry is not set up for a Web Management or Email Management computer, you can temporarily use local host entries.

Note:
This workaround is only temporary. You must establish true DNS resolution as quickly as possible for an easier implementation.

To add local host entries for Interaction Center servers:

1. Open the **hosts** file in a text editor.
   - Windows default location: `C:\WINDOWS\system32\drivers\etc`
   - Oracle Solaris default location: `/etc`
   - AIX default location: `/etc`
2. In the **hosts** file, locate the IP entry and name for **localhost**.

   For example, the **localhost** line in the file might read**:**

   ```
   127.0.0.1  localhost
   ```
3. Add an entry for each Web Management or Email Management computer:
   a. At the end of the **localhost** line, press **Enter** to get a new line.
   b. Type the computer's IP address.
   c. Press **Tab** or type a few spaces, and type the computer's FQDN.
   d. Press **Tab** or type a few more spaces, and type the computer name.

      The computer name and the FQDN resolve to the specified address, as shown in the following example:

      ```
      192.168.0.1  testbox.xyzcorp.com  comhub
      192.168.0.2  testbox.xyzcorp.com  sql
      ```
4. Save the file under its original name (hosts).

Note:
If the IP address changes, you must update the **hosts** file to reflect this change.

Chapter 15: Supported operating systems

This section includes the information about how to configure the operating system and install required prerequisite software on computers that host Avaya Interaction Center components. For information about supported software, see Required software components on page 285.

This section includes the following topics:

- Regional settings on page 263
- Microsoft Windows Server on page 263
- Microsoft Windows based desktop operating system on page 265
- Security for Unix platforms on page 270
- Oracle Solaris on page 270
- IBM AIX on page 274
- Citrix on page 278

Regional settings

If you need to change the regional system settings for a computer, make sure that you change the settings for all users, including the local system account.

Microsoft Windows Server

For list of supported Microsoft Windows Server see Unsupported features on page 30.

Note:

A minimum of 4 GB of extra temp space is required for the Interaction Center Installer to perform installation.

For more details about the definition of supported versions and about subsequent updates or service packs of the software, see About the supported versions on page 286.

Prerequisites for Windows Server

Microsoft Windows Server introduces a new concept of Roles/Features to make management of Servers easier and efficient. This section lists the roles and features required to successfully install/configure IC on Windows Server.

Note:
The roles are applicable for Microsoft Windows Server 2008 R2 and Microsoft Windows Server 2012 R2.

Roles

Web Server (IIS): This role is required for the servers that host the Avaya IC website.

The following Role Services are required for the Web Server (IIS) role:

- Common HTTP Features
- Application Development:
  - ISAPI Filters
  - ISAPI Extensions
- Health and Diagnostics (Optional)
- Management Tools:
  - IIS Management Console
  - IIS Management Scripts and Tools

Note:
Only the essential roles or services required for successfully configuring the website are listed in the previous list. Additional Roles or services are required for maintaining and running a website using IIS.

Application Server: This role is required for servers hosting Business Advocate.

The following Role Services are required for the Application Server role:

- .Net Framework 3.5.1
- TCP Port Sharing
- COM+ Network Access
- Incoming Remote Transactions under Distributed Transactions
- Outgoing Remote Transactions under Distributed Transactions
- Message Queuing Activation
- TCP Activation
- Named Pipes Activation

Features used in Windows Server

The following are the key features used in Windows Server:

- Message queuing for servers hosting Business Advocate
- .Net Framework 3.51 Features
- Role Administration - Webserver (IIS) Tools
- Windows PowerShell Integrated Scripting Environment
- Windows Process Activation Service

Note:
Only the essential features or services required for successfully configuring and running IC are listed in the previous list. Additional features or services may be required for a fully functional server running other software besides IC.

Microsoft Windows based desktop operating system

Note:
Before you install the Interaction Center agent applications, configure all agent workstations with restore points. The agent installer replaces some system files. Restore points allow easy rollback after you uninstall Interaction Center. See the Windows documentation or third-party guides for more information about the restore points.

To install and configure the following Windows components for Interaction Center, see the documentation provided by Microsoft and the information in the following sections:

- Setting up Microsoft Windows 7 on page 266
- Setting up Microsoft Windows Vista on page 266
- Setting up Microsoft Windows XP Professional on page 267
- Setting up Microsoft Internet Explorer on page 267

Setting up Microsoft Windows 8.1

Interaction Center Release 7.3.3 and later components support Microsoft Windows 8.1 Professional.

Setting up Microsoft Windows 7

Interaction Center components support Microsoft Windows 7 Professional. For more details about the definition of supported versions and about subsequent updates or service packs of the software, see About the supported versions on page 286.

Installing the required service packs for Microsoft Windows 7 Professional

Avaya supports Microsoft Windows 7 Professional with SP1. You must install one of these service packs on all computers that run Windows 7 Professional.

To install a service pack:

1. Go to the Microsoft website at http://www.microsoft.com
2. Go to the Downloads section for Windows 7 Professional, and follow the installation instructions provided by Microsoft.
3. Download the following:
   - Windows 7 SP1.
   - Readme and other deployment instructions.

Setting up Microsoft Windows Vista

Important:
Interaction Center supports only the 32-bit version of Microsoft Windows Vista. Microsoft Windows Vista operating system is only supported on IC 7.3, 7.3.1, and 7.3.2.

The Interaction Center components support the following versions of Windows Vista. For more details about the definition of supported versions and about the subsequent updates or service packs of the software, see About the supported versions on page 286.

- Windows Vista Enterprise Edition
- Windows Vista Ultimate Edition

Setting up Microsoft Windows XP Professional

Important:
Interaction Center does not support the 64-bit version of Microsoft Windows XP Professional. Interaction Center supports only the 32-bit version of Microsoft Windows XP Professional. Microsoft Windows XP is only supported on IC 7.3, 7.3.1, and 7.3.2.

Interaction Center components support Microsoft Windows XP Professional. For more details about the definition of supported versions and about subsequent updates or service packs of the software, see About the supported versions on page 286.

Installing required service packs for Microsoft Windows XP Professional

Avaya supports Microsoft Windows XP Professional with SP2 and SP3. You must install one of these service packs on all computers that run Microsoft Windows XP Professional.

To install a service pack:

1. Go to the Microsoft website at http://www.microsoft.com
2. Go to the Downloads section for Microsoft Windows XP Professional, and follow the installation instructions provided by Microsoft.
3. Download one of the following:
   - Microsoft Windows XP SP2 or SP3.
   - Readme and other deployment instructions.

Setting up Microsoft Internet Explorer

You must install Internet Explorer on every computer that hosts one or more of the following Interaction Center components:

- Avaya Agent
- Web Management
- Email Management
- Administration tools

All supported versions of Windows typically include Internet Explorer. However, you may need to upgrade to the current version.

This section includes the following topics:

- Downloading Internet Explorer on page 268

- Installing an Oracle Java Virtual Machine (32-bit) plug-in for Internet Explorer on page 268
- Configuring the JVM on page 268
- Configuring Internet Options for agent applications on page 269
- Configuring encoding for localized releases on page 270

Downloading Internet Explorer

You can download Microsoft Internet Explorer from the download center on the Microsoft website at http://www.microsoft.com.

Installing an Oracle Java Virtual Machine (32-bit) plug-in for Internet Explorer

The following Interaction Center components / features require a JVM (32-bit) to function correctly:

- Email Template Administration
- Avaya Agent Web Client
- Collaborative Form-filling (website customer).

Note: Collaborative Form-filling is only supported on Internet Explorer.

If you host these components on a computer with Microsoft Windows XP Professional, Windows Vista, Windows 7, or Windows 8.1, you must download and install a supported Oracle JVM, also referred to as JRE, on those computers. For list of supported JRE on IC release see Unsupported features on page 30. You can obtain a copy of the Oracle JRE from the following website:

http://java.com/en/download/index.jsp

Configuring the JVM

If you install the JVM plug-in, you must configure Microsoft Windows and Internet Explorer to use this plug-in.

Important:
You do not need to configure the JVM plug-in for Internet Explorer 9 and later.

To configure the JVM:

1. In the **Windows Control Panel**, click **Java**.
2. In the **Java Control Panel** dialog box:
   a. Click the **Advanced** tab.

b. Under **Default Java for browsers**, make sure that the **Microsoft Internet Explorer** check box is selected.

c. Click **OK**.

d. Close Control Panel.

3. In Internet Explorer, select **Tools** > **Internet Options**.
4. In the **Internet Options** dialog box:
   a. Click the **Advanced** tab.
   b. In the **Java (Sun)** section, select the **Use** JRE 1.x.x_xx ***for <applet>*** **(requires restart)** check box.

Note:
For details on the JRE version see Unsupported features on page 30.

   c. In the **Microsoft VM** section, clear the **JIT Compiler for virtual computer enabled** check box.
   d. Click **OK**.
5. Close all Internet Explorer Web browser sessions for the changes to take effect.

Configuring Internet Options for agent applications

The following table lists the required settings for Internet Options in Internet Explorer for all agents who will handle chat contacts:

Internet option	Required setting
Security level	Medium
ActiveX controls	Allow to run.
Trusted sites	• For Avaya Agent, add the URL of the website server to the Trusted Sites list. • For Avaya Agent Web Client, add the URL of the Avaya Agent Web Client to the Trusted Sites list.
Proxy server settings	If your Interaction Center system uses a proxy server, add the fully qualified domain name of the contact center to the proxy **Exceptions** field. For example, you can enter ***.company_name.com** or ***.*.company_name.com**. You can add multiple names. Check the documentation for your operating system for details.
Pop-up blockers	For Avaya Agent Web Client, disable or configure to allow pop-ups on the Avaya Agent Web Client URL.

Configuring encoding for localized releases

If your Interaction Center system includes Prompter in a supported language other than English, you must configure the encoding in Internet Explorer to match that locale.

For example, if an agent views Prompter scripts in Thai, you need to perform the following steps to configure the coding in Internet Explorer for Thai:

1. Turn off Auto select.
2. Configure the encoding for the Thai locale.

   To configure encoding, select **View** > **Encoding** in Internet Explorer.

Security for Unix platforms

Users must avoid running Avaya software as the root user, wherever possible, for security reasons. For more information, see User accounts for Oracle Solaris on page 273 and User accounts for AIX on page 277.

Oracle Solaris

Interaction Center servers support Oracle Solaris 10 update 9.

Important:
Solaris is only supported on SPARC platform.

Interaction Center Design & Administration Tools and client applications do not support Oracle Solaris.

This section includes information that you need to install and configure an Oracle Solaris operating system on computers that host Interaction Center servers or databases. This section includes the following topics:

- Browser requirements for Oracle Solaris on page 271
- Disk space requirements for Oracle Solaris on page 271
- Configuration requirements for Oracle Solaris on page 271
- User accounts for Oracle Solaris on page 273

Browser requirements for Oracle Solaris

Interaction Center does not support an internet browser for Oracle Solaris. However, you must have an Internet Explorer browser to install an Interaction Center license. If you host Interaction Center servers on Oracle Solaris, install the Interaction Center license from the computer that hosts the Design & Administration Tools or from another computer with a supported Windows operating system.

Disk space requirements for Oracle Solaris

An Oracle Solaris computer that hosts Interaction Center servers requires the following disk space:

- A minimum of 1 GB of disk space for the server files.
- A minimum of 30 GB disk space to store server log files.
- A minimum of 2 GB extra temp space in the /var/tmp directory for the Interaction Center installer to perform the Java Virtual Machine.

These requirements do not include disk space for the required third-party applications, such as Oracle Solaris, iPlanet Web Server, or the JDK.

Detailed information about how to partition individual Oracle Solaris computers is beyond the scope of this manual. The most efficient method to partition a computer depends on many factors, including, which Interaction Center servers you plan to host on the computer, and the volume of customer interactions in your contact center. You must consider all of these factors when you determine how to partition each computer in your Interaction Center system.

Configuration requirements for Oracle Solaris

This section includes the following topics which describe the recommended configuration parameters for Interaction Center on Oracle Solaris:

- Configuration settings for Oracle Solaris on page 272
- ULIMIT parameters on page 273

Configuration settings for Oracle Solaris

The following table describes the configuration settings required on an Oracle Solaris computer that hosts Interaction Center servers:

Configuration setting	Notes
DISPLAY	Enable the `DISPLAY` parameter. The Interaction Center installation and Configuration Tool cannot run if you have not enabled the `DISPLAY` parameter.
National character set	UTF8
Oracle Database character set	UTF8
Locale	Install the English locale: English: en_US.UTF-8 You can also install the appropriate locale for the language of your Interaction Center system: • Japanese: ja_JP.UTF-8 • Korean: ko_KR.UTF-8 • Simplified Chinese: zh_CN.UTF-8 • German: de_DE.UTF-8 • French: fr_FR.UTF-8 • Italian: it_IT.UTF-8 • Spanish: es_ES.UTF-8 • Portuguese: pt_BR.UTF-8 • Thai: th_TH.UTF-8 • Russian: ru_RU.UTF-8 **Note:** This setting is case-sensitive.
Port 9010	Oracle Solaris runs the HTT Input Method Server (htt_server) on port 9010 by default. This port assignment creates a conflict with any Interaction Center server that you configure to run on port 9010. To avoid the conflict, you can update htt_server to use a different port, or not assign an Interaction Center server to port 9010. In a typical installation, with the primary ORB server on port 9001, IC Manager automatically assigns port 9010 to the Report server.
Space requirements	Make sure that the server has sufficient space in the `/var/tmp` directory. For more information, see Disk space requirements for Oracle Solaris on page 271.
Windowing environment	Install a Windowing environment such as X Windows.

ULIMIT parameters

The following table describes the minimum required settings for ULIMIT parameters required on an Oracle Solaris computer that hosts the Interaction Center servers. The superuser must ensure that the hard limits for the ULIMIT parameters are not less than these minimum required settings. For more information, see the UNIX man pages provided by Oracle Solaris.

Parameter	Minimum required setting
data	512MB
stack	512MB
memory	512MB
core dump	1 GB
file descriptors	2000

User accounts for Oracle Solaris

You need the following Oracle Solaris user accounts when you install and configure Interaction Center:

- Root user on page 273
- Installation user on page 274

Root user

You need the root account when you:

- Install Interaction Center on a computer that hosts a Telephony server for an Avaya switch with Communication Manager software.
- Configure the Web applications with the Configuration Tool, including the website, Email Template Administration, and Web License Manager.

Installation user

Use this account to perform all the tasks to install and configure Interaction Center that do not require the root user. This account must own the Interaction Center installation directory.

Important:
If you do not use a root account to install Interaction Center servers on a computer, and need to configure that computer with a Telephony server for an Avaya switch with Communication Manager software, reinstall the Interaction Center servers under the root account.

Interaction Center does not have any specific requirements for the installation user account. However, you must:

- Create an installation group named **avaya**.
- Assign the avaya group as the primary group when you create the installation user account.
- Do not assign a secondary group membership to the installation user account.

IBM AIX

Interaction Center (Release 7.3, 7.3.1, and 7.3.2 only) servers support AIX 6.1. Interaction Center Design & Administration Tools and client applications do not support AIX.

Note:
IBM AIX and IBM DB2 are only supported on Interaction Center Release 7.3, 7.3.1, and 7.3.2. For more information see the Unsupported features on page 30. All the information related to IBM AIX and IBM DB2 is only applicable to Interaction Center Release 7.3, 7.3.1, and 7.3.2.

This section includes information that you need to install and configure an AIX operating system on computers that host Interaction Center servers or databases. This section includes the following topics:

- Browser requirements for AIX on page 275
- Disk space requirements for AIX on page 275
- Configuration requirements for AIX on page 276
- User accounts for AIX on page 277

Tip:
For information about IBM LPAR support, see IBM Logical Partition (LPAR) technology on page 192.

Browser requirements for AIX

Although, Interaction Center does not support an internet browser for AIX, you must have an internet browser to install an Interaction Center license. If you host Interaction Center servers on AIX, install the Interaction Center license from the computer that hosts the Design & Administration Tools or from another computer with a supported Windows operating system.

Disk space requirements for AIX

An AIX computer that hosts Interaction Center servers requires the following disk space:

- A minimum of 1 GB of disk space for the server files.
- A minimum of 30 GB disk space to store server log files.
- A minimum of 3 GB extra temp space in the `/tmp` directory for the Interaction Center installer to perform the Java Virtual Machine.

These requirements do not include disk space for required third-party applications, such as AIX or the JDK.

Detailed information about how to partition individual AIX computers is beyond the scope of this manual. The most efficient method to partition a computer depends on many factors, including which Interaction Center servers you plan to host on the computer and the volume of customer interactions in your contact center. Consider all of these factors when you determine how to partition each computer in your Interaction Center system.

Installing required locales

All installations on IBM AIX require that you install the following locales:

- EN_US locale

  AND

- If the Interaction Center system includes a supported language other than English, the locale for that language. For more information about the locale settings, see Configuration requirements for AIX on page 276.

Configuration requirements for AIX

The following table describes the configured settings required on an AIX computer that hosts Interaction Center servers.

Configuration setting	Notes
Locale	Install EN_US and any additional locales, as appropriate for the language of the Interaction Center system: • English: EN_US • Spanish: ES_CO • Portuguese: PT_BR • Italian: IT_IT • French: FR_FR • German: DE_DE • Simplified Chinese: ZH_CN • Korean: KO_KR • Japanese: JA_JP • Thai: TH_TH • Russian: RU_RU **Note:** EN_US does not have to be the primary locale.
DISPLAY	Enable the **DISPLAY** parameter. The Interaction Center installation and Configuration Tool cannot run if you have not enabled the **DISPLAY** parameter.
Space requirements	Make sure that the server has sufficient space in the `/tmp` directory. For more information, see Disk space requirements for AIX on page 275.
Windowing environment	Install a Windowing environment such as X Windows.

User accounts for AIX

You need the following AIX user accounts when you install and configure Interaction Center:

- Root user on page 277
- Installation user on page 277

Root user

Interaction Center requires that the root account be in the same group as the database administration login for the Interaction Center databases. For example, include the root user account in the db2admin group.

You need the root account when you:

- Install Interaction Center on a computer that hosts a Telephony server for an Avaya switch with Communication Manager software.
- Configure the Web applications with the Configuration Tool, including the website, Email Template Administration, and Web License Manager.

Installation user

Use this account to perform all tasks to install and configure Interaction Center that does not require the root user. This account must own the Interaction Center installation directory.

Important:
If you do not use a root account to install Interaction Center servers on a computer, and need to configure that computer with a Telephony server for an Avaya switch with Communication Manager software, reinstall the Interaction Center servers under the root account.

Interaction Center does not have any specific requirements for the installation user account. However, you must:

- Create an installation group named **avaya**.
- Assign the avaya group as the primary group when you create the installation user account.
- Do not assign a secondary group membership to the installation user account.

Citrix

Interaction Center provides support for Avaya Agent on Citrix servers for Windows. For information about which agent desktop applications are not supported, see Limitations on support for Citrix on page 280.

With Interaction Center agent desktop applications in a Citrix environment, the contact center can:

- Administer agent desktop applications from a central location.
- Remotely provide agents and supervisors with access to the agent desktop applications.
- Publish Avaya Agent or another supported agent desktop application on one or more Citrix servers.
- Use Web browser or Citrix client to access agent desktop applications from agent or admin computers.

For information about supported versions of Citrix, see Prerequisites for agent desktop applications on Citrix on page 310.

This section describes the support for Interaction Center components in Citrix. This section includes the following topics:

- Deploying of Interaction Center components in a Citrix environment on page 278
- Limitations on support for Citrix on page 280
- Licensing for Interaction Center in Citrix on page 281
- Citrix Web interface on page 281
- Citrix client interface on page 281
- Limitations of integration with Citrix on page 283

Deploying of Interaction Center components in a Citrix environment

This section provides information about where to deploy Interaction Center components in a Citrix environment, including information about how to deploy more than one configuration of the Interaction Center agent desktop applications.

This section includes the following topics:

- Location of Interaction Center components on page 279
- Multiple configurations of agent desktop applications on page 279

Location of Interaction Center components

When you install Interaction Center in a Citrix environment, deploy the Interaction Center components as follows:

Interaction Center servers: Locate the Interaction Center servers on the servers, following the appropriate deployment scenario for the components in the Interaction Center system. You do not need to change the deployment of Interaction Center servers if you host the agent desktop applications in a Citrix environment.

Design & Administration Tools: Locate the Design & Administration Tools on separate administration computers. You do not need to change the deployment of Design & Administration Tools if you host the agent desktop applications in a Citrix environment.

Web Management website: Locate the customer website on a separate computer in the DMZ of the network and the administration website on an administration computer inside the firewall. You do not need to change the deployment of the Web Management websites if you host the agent desktop applications in a Citrix environment.

Agent desktop applications: Locate the Interaction Center agent desktop applications on one or more Citrix servers. Do not install the agent desktop applications on the agent workstations.

Interaction Center Citrix connectors: Locate the Interaction Center Citrix connectors on the agent workstations. These connectors provide agents with access to the agent desktop applications on the Citrix servers, and ensure that the agent desktop applications resize correctly in the Citrix client.

Citrix clients: Locate the Citrix clients on the agent workstations.

Multiple configurations of agent desktop applications

With the agent desktop applications on Citrix, you can host different configurations of the agent desktop applications on different Citrix servers. For example, you can create a voice only configuration and a multi-channel configuration, as follows:

- Avaya Agent with voice only on ServerA.
- Avaya Agent with voice, chat, and email on ServerB.

Agents can easily switch from voice only work to multi-channel work by exiting from Server A and logging in to Server B.

Interaction Center components supported in Citrix

Interaction Center supports the Avaya Agent on Citrix with the following features:

- Inbound voice channel
- Email channel
- Chat channel

Interaction Center support for publishing applications in Citrix

Interaction Center supports both of the following methods of publishing applications in Citrix:

- Agent applications accessed as embedded applications in the Citrix Web interface.
- Agent applications accessed in a seamless window in the Citrix client interface.

Limitations on support for Citrix

Interaction Center Release 7.3.x does not support all operating systems that are supported by Citrix. Avaya also does not provide support for the hosting of OA components, Avaya Agent Web Client, or other Interaction Center components on the Citrix servers.

The limitations on support for components of Interaction Center and OA on Citrix servers, include the following:

- Agent workstation with an operating system that is not Windows 2008 R2 Server
- Interaction Center Design and Administration Tools, including IC Manager, Workflow Designer, and Database Designer
- Business Advocate administration tools, including Business Advocate Supervisor
- OA
- IP Softphone
- Windows Terminal Services (TSE) without Citrix
- Other Citrix servers, such as UNIX servers
- Wyse Terminals and other terminals, such as the COMPAQ T20

Licensing for Interaction Center in Citrix

If the Interaction Center system includes agent desktop applications in Citrix, the following licenses are required:

- The appropriate number and kind of Citrix licenses.
- An Interaction Center license for every agent and supervisor who will be concurrently logged in to Interaction Center.

If an Interaction Center system includes Citrix, there is no reduction in the number of Interaction Center licenses that are required. The Web License Manager monitors the number of agents who log in to Interaction Center. If the number of agents who attempt to log in to Interaction Center exceeds the number of licenses, the Web License Manager denies access to those login attempts that exceed the licensed number.

Citrix Web interface

The Citrix Web interface is also called “publish as desktop”. The Web interface uses an ActiveX control to exchange information about agent actions with the Interaction Center agent desktop applications published on Citrix server.

Access to agent desktop applications: With the Web interface, agents use a Web browser to log in to the agent desktop applications. After the agent logs in, the Web interface displays a Web page that includes Avaya Agent and other agent desktop applications published on Citrix server.

Configuration for Citrix: You do not have to perform any configuration in Citrix to ensure that agents can access the agent desktop applications through the Web interface.

Citrix client interface

The Citrix client interface is also called *publish as application*. The client interface uses the Independent Computing Architecture (ICA) protocol to exchange information about agent actions with the Interaction Center agent desktop applications published on Citrix server.

The Citrix client interface with the seamless window causes issues with the login behavior and the appearance of the Interaction Center agent desktop applications. Avaya provides two tools that prevent these potential issues. For example, these tools ensure that:

- Agents log in to the appropriate agent desktop applications.
- The Agent desktop applications, such as screen pops and Web Agent, size properly in the Web interface.
- Avaya Agent does not overlap the other agent desktop applications in the window.

This section includes the following topics:

- Configuring Citrix on page 282
- Configuring Citrix integration for seamless window applications on page 282
- Web browser tool for the client interface on page 282
- Executable tool for the client interface on page 283

Configuring Citrix

You do not have to perform any configuration in Citrix to ensure that agents can access the agent desktop applications through either the Web interface or the agent interface.

Depending upon the environment, you may need to adjust the size of the Avaya Agent framework. For more information about how to customize the framework size, see *Avaya Agent Integration*.

Configuring Citrix integration for seamless window applications

If the Interaction Center system includes access to Interaction Center agent desktop Applications through the Citrix client interface in a seamless window, the Citrix integration can be configured in the following ways:

- Configure and run the Web browser tool to access the agent desktop applications.
- Configure and run the Executable tool to access the agent desktop applications.

Both of these tools require that you install the Avaya Agent INI file (qui.ini). For more information, see *IC Installation and Configuration Guide*.

Web browser tool for the client interface

The Web interface tool appears as a Web page in Internet Explorer that agents use to log in to the agent desktop applications on Citrix. The Web interface tool ensures that:

- Agents log in to the appropriate agent desktop applications.
- Agent desktop applications size properly in the Web interface.

Configuring the Web browser tool: The only configuration required for this Web interface tool is to update the HTML file with the correct location for the Citrix server that hosts the agent desktop applications.

Customizing the Web browser tool: If desired, you can customize the appearance of the Web page for the Web interface tool.

For information about how to configure the Web browser tool to access a specific agent desktop application on a Citrix server, see *IC Installation and Configuration Guide*.

Executable tool for the client interface

The executable tool is intended for use only in the Interaction Center systems where the design precludes a Web browser application. This tool includes an executable and an INI file. This tool appears as a dialog box on the agent desktop.

Agents use the dialog box to access and log in to agent desktop applications published on Citrix server. After the agent logs in, the client interface opens a window that displays Avaya Agent and the other agent desktop applications published on the Citrix server.

Configuring the executable tool: The only configuration required for the executable tool is updating the INI file with the correct location for the Citrix server that hosts the agent desktop applications.

Customizing the executable tool: If desired, you can customize the text on the buttons in the dialog box to meet the needs of the contact center or the corporate style.

For information about how to configure the client interface tool to access a specific agent desktop application on a Citrix server, see *IC Installation and Configuration Guide*.

Limitations of integration with Citrix

With Citrix integration, you can install, publish, and access the agent desktop applications on the Citrix server. Only the interface to the agent desktop applications is installed on the agent workstations.

Before you deploy your Interaction Center agent desktop applications on a Citrix server, consider the following limitations:

- Do not host embedded applications and seamless window applications on the same Citrix server. To use both publishing methods in an Interaction Center system, host the embedded applications on a different Citrix server from seamless window applications.
- Do not use the Web browser tool, the Executable tool, or the Avaya Agent INI file (qui.ini) on a Citrix server that hosts embedded applications.
- Citrix cannot make agent desktop applications look as if they are on agent workstations.
- Citrix does not provide the ability to integrate applications across processor boundaries. For example, you cannot integrate the agent desktop applications on the Citrix server with an application on the agent workstation.
- If the Interaction Center system includes integration with another application, such as PeopleSoft or Siebel, you must integrate the applications on the Citrix server.

Chapter 16: Required software components

Before you plan or install an Interaction Center (IC) system, you must know:

- The servers are required by the components in the Interaction Center system.
- The third-party software is required for the components in the Interaction Center system.

This section includes the following topics:

- About the supported versions on page 286
- Exceptions to supported operating systems on page 286
- Required software for Interaction Center servers on page 287
- Required software for Interaction Center databases on page 289
- Required software for Telephony on page 291
- Required software for Web Management on page 293
- Required software for Email Management and Content Analyzer on page 296
- Required software for Business Advocate on page 299
- Required software for the Interaction Center Client SDK on page 305
- Required software for Interaction Center for Siebel on page 305
- Required software for Design & Administration Tools on page 306
- Required software for agent applications on page 307
- Upgrading Daylight Saving Time (DST) patches on page 311
- Upgrading Daylight Saving Time (DST) patches on page 311



Tip:
This section provides the summary of the prerequisites for the Interaction Center components. Further details about service packs, fix packs, maintenance levels, and patches are available in the appropriate chapters of this document.

These topics do not include information about the required software for OA. For more information about OA and its prerequisites, see Operational Analyst *Planning and Prerequisites*.

About the supported versions

Avaya supports use of the software versions documented in this manual with Release 7.3.x of Operational Analyst and Avaya Interaction Center. These software versions are the minimum versions required by Avaya.

Release 7.3.x does not support operating systems, databases, Web servers, switches, or other software platforms that are not documented in this manual.

Avaya supports subsequent updates and service packs that are released to provide corrections to a bug, defect, or problem for the software versions documented in this manual, so long as those updates and service packs:

- Are guaranteed by the manufacturer to be backwards compatible with the supported version.
- Do not include changes to core functionality or new features.

You must test all updates and service packs subsequent to the supported versions in a development environment before applying them to a production environment.

Exceptions to supported operating systems

The following table describes the exceptions to operating system support for Interaction Center. For information about limitations to support for Citrix, see Limitations on support for Citrix on page 280.

Interaction Center component	Exception to supported operating systems
Business Advocate	No AIX or Oracle Solaris support for Resource Manager servers. Business Advocate does not function with the Resource Manager servers on AIX or Oracle Solaris. Host the Resource Manager servers on Windows computers. For more information, see Exceptions to platform support for Business Advocate on page 247.

Required software for Interaction Center servers

The Interaction Center servers manage communication between internal and external components, and control the routing of contacts. Some servers are required by all Interaction Center systems. However, some servers, such as the DUStore server, are not required in all the Interaction Center systems.

The following table shows the software that you must install on computers that host one or more Interaction Center servers or on a computer that communicates with a server. For more details about the definition of supported versions and about subsequent updates or service packs of the software, see About the supported versions on page 286.

Required software	Location	Supported versions[1]			
		Microsoft Windows		Oracle Solaris	IBM AIX
Operating systems	All core servers	Windows Server 2012 R2	Windows Server 2008 R2	Oracle Solaris 10 update 9	AIX 6.1 update 3
Web server **Note:** You can co-locate with the WebLM application.	Computer that communicates with WebLM application	Microsoft IIS 8	Microsoft IIS 7.5	Oracle iPlanet Web Server 7.0.13	IBM HTTP Server 7.0
Time synchronization utility	All core servers	Third-party NTP application	Third-party NTP application	NTP application	NTP application
PDF reader for documentation	All core servers	Adobe Acrobat Reader	Adobe Acrobat Reader	Adobe Acrobat Reader	Adobe Acrobat Reader

Required software	Location	Supported versions[1]			
		Microsoft Windows		Oracle Solaris	IBM AIX
Email servers	Computer that communicates with Notification server	SMTP and POP3 / IMAP4 compliant email servers	SMTP and POP3 / IMAP4 compliant email servers	SMTP and POP3 / IMAP4 compliant email servers	SMTP and POP3 / IMAP4 compliant email servers
Web browser	Computer that hosts WebLM	Internet Explorer 11 (32-bit) Note: Internet Explorer 7 and 8 are no longer supported in IC 7.3.3. The Document Mode should not be set to Quirks mode or older Internet Explorer version standards.	Internet Explorer 11 (32-bit) Internet Explorer 10 (32-bit) Internet Explorer 9 (32-bit) Note: Internet Explorer 7 and 8 are no longer supported in IC 7.3.3. The Document Mode should not be set to Quirks mode or older Internet Explorer version standards.	Through Admin computer: Internet Explorer 11 (32-bit) Internet Explorer 10 (32-bit) Internet Explorer 9 (32-bit)	Through Admin computer: Internet Explorer 11 (32-bit) Internet Explorer 10 (32-bit) Internet Explorer 9 (32-bit)

1. Avaya IC 7.3.x supports VMWare ESX Server 4.1, VMWare ESXi Server 5.0, and VMWare ESXi Server 5.1. For information about IBM LPAR support, see IBM Logical Partition (LPAR) technology on page 192.

Required software for Interaction Center databases

The Interaction Center servers and client applications require access to the Interaction Center databases. These databases store system-level data, including information about customers and agents, and application-level data, including information about contacts with customers.

OA reports are based on the information that Interaction Center stores in its databases.

This section lists the prerequisite software required to support the Interaction Center databases. This section includes the following topics:

- Required Interaction Center databases on page 289
- Optional Interaction Center databases on page 289
- Prerequisites for the databases on page 290

Required Interaction Center databases

The following Interaction Center databases are required for all Interaction Center systems. For a brief description of these databases, see Interaction Center databases on page 46.

- Repository
- CCQ

Optional Interaction Center databases

The following table shows the Interaction Center databases that are only required for Interaction Center systems that include specific components. For a brief description of these databases, see Interaction Center databases on page 46.

Component	Databases
Business Advocate	• Business Advocate System Store • Business Advocate Resource Store
Interaction Center for Siebel	• Siebel 8.1.1.x, 8.2.2.x, and 15 • On AIX 6.1, IC 7.3 Siebel integration is only supported with Siebel 8.1.1.3 to 8.1.1.6 and from IC 7.3.4 and above, Siebel 15 is supported. • On Red Hat Enterprise Linux 6.5, IC 7.3.4 Siebel integration is only supported with Siebel 8.1.1.14 and Siebel 15

Prerequisites for the databases

All Interaction Center systems require a Relational Database Management System (RDBMS). Interaction Center supports each RDBMS only on certain supported operating systems.

For more details about the definition of supported versions and about the subsequent updates or service packs of the software, see About the supported versions on page 286.

Note:

Interaction Center provides limited support for databases that run on a different operating system than the Interaction Center servers. For more information, see Supported database management systems on page 209.
For information about exceptions to this RDBMS support for certain optional databases, such as Business Advocate databases, see Exceptions to supported database management systems on page 210.

The following table lists the required operating system for each supported RDBMS:

Database server operating system	Microsoft SQL Server Database			Oracle Database Server				IBM DB2 Database
	2008 R2	2012	2014	10g	11g	11g R2	12c	9.5
Windows Server 2008 R2	Y 64-bit only	Y 64-bit only	Y 64-bit only	Y	Y	Y[1]	N	N
Windows Server 2012 R2	Y 64-bit only	Y 64-bit only	Y 64-bit only	N	N	Y	Y	N
Oracle Solaris 10	N	N	N	Y 64-bit only	Y 64-bit only	Y	N	N
IBM AIX 6.1	N	N	N	N	N	N	N	Y 32-bit only
Red Hat Linux 6.3 and 6.4 (64-bit)[2] [3]	N	N	N	N	N	Y	Y	N

1. You must install Patch 9888297 for Oracle 11g R2 on Windows 2008 R2 Server.
2. You can install and configure IC with the remote instance of the Oracle Database Server, which is installed on the Red Hat Linux 64-bit operating system. For the Oracle database server, you must install the 32-bit client on IC server systems.
3. Oracle database on Red Hat Linux platform is supported from IC 7.3.2 release onwards.

Required software for Telephony

The Telephony components provide services that manage communication between switches and Interaction Center, and control the routing of voice contacts.

This section lists the servers that support Telephony for Interaction Center and the prerequisite software for the servers that support Telephony. This section includes the following topics:

- Telephony servers on page 291
- Prerequisites for Telephony servers on page 292

Telephony servers

The following table shows the servers that support Telephony:

Component	Servers
Required servers for Telephony	• Telephony server
Optional servers for Telephony	• Telephony Queue Statistics server • VOX server
Required core servers for Telephony	• ADU server • Alarm server • Blender server • Data server • Directory server • EDU server • License server • ORB server • Notification server • Report server • Workflow server
Optional core servers for Telephony	For systems with multiple servers, install additional core servers as described in the following sections: • Interaction Center single site deployment scenarios on page 79 • Interaction Center multi-site deployment scenarios on page 123

Prerequisites for Telephony servers

For more information about the definition of supported versions and about subsequent updates or service packs of the software, see About the supported versions on page 286.

Certain switches and software support only certain functions and components of Interaction Center. For more detailed information, see Supported Telephony switches and software on page 231.

Supported Telephony software

The following table shows the software that you must install on all computers that host one or more servers for Telephony:

Required software	Location	Supported operating system versions		
		Microsoft Windows	Oracle Solaris	IBM AIX
Operating systems	All core servers	Windows Server 2008 R2 Windows Server 2012 R2	Oracle Solaris 10 update 9	AIX 6.1
Time synchronization utility	All core servers	Third-party NTP application	NTP application	NTP application
Avaya switches and software	As required by switch or software	For more information about supported switches and switch software, see: • Requirements for supported Avaya switches and software on page 293 • Required software for Web Management on page 293		

Requirements for supported Avaya switches and software

The following table shows the software that Interaction Center Telephony requires for the supported Avaya switches and software:

Note:
If the Interaction Center system includes Business Advocate and Communication Manager 5.x or later, you must activate Increased Adjunct Route Capacity on the Communication Manager.

Connectivity method	Endpoint	Requirements	Applicable switch releases
Via AE Services	H.323	AE Services 5.x CVLAN Service TN799DP Clan board(s) in Communication Manager. ADJ-IP Adjunct Link (not asai link) configured on the switch. Order of an Avaya IC ACD connector configures the RFA file on switch appropriately. Call Center Elite with EAS for ASAI Agent States.	Communication Manager 5.x or later
	In IC 7.3.2 FP, following SIP endpoint models are supported: 9608 9611 9621 9641 **Note:** The IC 7.3.2 FP release supports the SIP endpoints only on Windows platform with AES version 6.3 or later.	AE Services 6.3 or later CVLAN Service. ADJ-IP Adjunct Link (not asai link) configured on the switch. Order of an Avaya IC ACD connector configures the RFA file on switch appropriately. Call Center Elite with EAS for ASAI Agent States. Session Manager Release 6.3 or later Avaya Aura System Manager 6.3 or later.	Communication Manager Release 6.3 SP3 or later connected to Session Manager using SIP Trunk.

Required software for Web Management

Web Management components provide services for the following Interaction Center features:

- Web Management
- Email Management

This section lists the servers that support Web Management and the prerequisite software for those servers. This section includes the following topics:

- Web Management servers on page 294
- Prerequisites for Web Management servers on page 295

Web Management servers

The following table shows the servers that support Web Management in Interaction Center:

Component	Servers
Required Web Management servers	• WebACD server • ComHub server • Paging server • Attribute server • Tomcat server for website • ICM server
Optional Web Management servers	• Central Internet Routing Service (CIRS)
Required servers for Web Scheduled Callback	• Required Web Management servers on page 294

Component	Servers
Required core servers for Web Management	• ADU server • Alarm server • Blender server • Data server • Directory server • EDU server • License server • ORB server • Notification server • Report server • Workflow server
Optional core servers for Web Management	For systems with multiple servers, install additional core servers as described in the following sections: • Interaction Center single site deployment scenarios on page 79 • Interaction Center multi-site deployment scenarios on page 123

Prerequisites for Web Management servers

The following table shows the software that you must install on computers that host one or more Web Management servers. For more details about the definition of supported versions and about subsequent updates or service packs of the software, see About the supported versions on page 286.

For information about the browsers supported for customers who access the website, see Upgrading Daylight Saving Time (DST) patches on page 311.

Required software	Location	Supported versions[1]			
		Microsoft Windows		Oracle Solaris	IBM AIX
Operating systems	All servers	Windows Server 2012 R2	Windows Server 2008 R2	Oracle Solaris 10 update 9	AIX 6.1
Web server **Note:** You can co-locate with the website application.	Computer that communicates with the website application	Microsoft IIS 8	Microsoft IIS 7.5	Oracle iPlanet Web Server 7.0.13	IBM HTTP Server 7.0

Required software	Location	Supported versions[1]			
		Microsoft Windows		Oracle Solaris	IBM AIX
Time synchronization utility	All servers	third-party NTP application	third-party NTP application	NTP application	NTP application
PDF reader for documentation	All servers	Adobe Acrobat Reader	Adobe Acrobat Reader	Adobe Acrobat Reader	Adobe Acrobat Reader
Web browser	Computer that hosts website	Internet Explorer 11 (32-bit)	Internet Explorer 11 (32-bit) Internet Explorer 10 (32-bit) Internet Explorer 9 (32-bit) Internet Explorer 8 Internet Explorer 7	Through Admin computer: Internet Explorer 11 (32-bit) Internet Explorer 10 (32-bit) Internet Explorer 9 (32-bit) Internet Explorer 8 Internet Explorer 7	Through Admin computer: Internet Explorer 11 (32-bit) Internet Explorer 10 (32-bit) Internet Explorer 9 (32-bit) Internet Explorer 8 Internet Explorer 7

1. Avaya IC 7.3.x supports VMWare ESXi Server 5.1 and VMWare ESXi Server 5.5. For information about IBM LPAR support, see IBM Logical Partition (LPAR) technology on page 192.

Required software for Email Management and Content Analyzer

Email Management and Content Analyzer components manage communication between email servers and Interaction Center, and control the routing of email contacts.

This section lists the servers that support Email Management and Content Analyzer for Interaction Center and the prerequisite software for those servers. This section includes the following topics:

- Email Management servers and Content Analyzer servers on page 297
- Prerequisites for Email Management servers and Content Analyzer servers on page 298

Email Management servers and Content Analyzer servers

The following table shows the servers that support Email Management and Content Analyzer:

Component	Servers
Required core servers for Email Management and Content Analyzer	• ADU server • Alarm server • Blender server • Data server • Directory server • EDU server • License server • ORB server • Notification server • Report server • Workflow server • DUStore server
Required Email Management servers	• ICEmail server • Poller server • Tomcat server for Email Template Administration
Required Web Management servers for email	• WebACD server • Paging server • ComHub server • Tomcat server for WebACD administration pages
Content Analyzer servers	• Required Email Management servers on page 297 • Required Web Management servers for email on page 297 • Content Analyzer administration server • Content Analyzer operation server
Optional core servers for Email Management and Content Analyzer	For systems with multiple servers, install additional core servers as described in the following sections: • Interaction Center single site deployment scenarios on page 79 • Interaction Center multi-site deployment scenarios on page 123

Prerequisites for Email Management servers and Content Analyzer servers

The following table shows the software that you must install on computers that host one or more servers for Email Management or Content Analyzer.

For more details about the definition of supported versions and about subsequent updates or service packs of the software, see About the supported versions on page 286.

Required software	Location	Supported versions[1]			
		Microsoft Windows		Oracle Solaris	AIX
Operating systems	All core servers	Windows Server 2012 R2	Windows Server 2008 R2	Oracle Solaris 10 update 9	AIX 6.1
Web server **Note:** You can co-locate with the Email Template Administration application	Computer that communicates with WebLM application	Microsoft IIS 8	Microsoft IIS 7.5	Oracle iPlanet Web Server 7.0.13	IBM HTTP Server 7.0
Time synchronization utility	All core servers	Third-party NTP application	Third-party NTP application	NTP application	NTP application
PDF reader for documentation	All core servers	Adobe Acrobat Reader	Adobe Acrobat Reader	Adobe Acrobat Reader	Adobe Acrobat Reader

Required software	Location	Supported versions[1]			
		Microsoft Windows		Oracle Solaris	AIX
Email servers	Computer that communicates with IC Email server computer	SMTP and POP3 / IMAP4 compliant email servers	SMTP and POP3 / IMAP4 compliant email servers	SMTP and POP3 / IMAP4 compliant email servers	SMTP and POP3 / IMAP4 compliant email servers
Web browser	Computer that hosts Email Template Administration application	Internet Explorer 11 (32-bit) Internet Explorer 10 (32-bit) Internet Explorer 9 (32-bit) Internet Explorer 8 Internet Explorer 7	Internet Explorer 11 (32-bit) Internet Explorer 10 (32-bit) Internet Explorer 9 (32-bit) Internet Explorer 8 Internet Explorer 7	Through Admin computer: Internet Explorer 11 (32-bit) Internet Explorer 10 (32-bit) Internet Explorer 9 (32-bit) Internet Explorer 8 Internet Explorer 7	Through Admin computer: Internet Explorer 11 (32-bit) Internet Explorer 10 (32-bit) Internet Explorer 9 (32-bit) Internet Explorer 8 Internet Explorer 7

1. Avaya IC 7.3.x supports VMWare ESX Server 4.1, VMWare ESXi Server 5.0, and VMWare ESXi Server 5.1. For information about IBM LPAR support, see IBM Logical Partition (LPAR) technology on page 192.

Required software for Business Advocate

Business Advocate for Interaction Center includes a set of servers that provide services to intelligently match agents with contacts in all supported media channels, and to manage communication with other Interaction Center servers.

This section lists the servers that support Business Advocate for Interaction Center and the prerequisite software for those servers. This section includes the following topics:

- Business Advocate servers on page 300
- Prerequisites for Business Advocate servers on page 301

Business Advocate servers

The following table shows the servers that support Business Advocate for Interaction Center:

Component	Servers
Required Business Advocate servers	• Resource Manager server
Required servers for Business Advocate with Telephony	• Telephony Services Adaptor server • Required servers for Telephony on page 291
Optional servers for Business Advocate with Telephony	• VOX server • HttpVOX server
Required servers for Business Advocate with Web Management	• Web Advocate Adaptor server • Required Web Management servers on page 294
Required servers for Business Advocate with Email Management	• Web Advocate Adaptor server • Required Email Management servers on page 297 • Required Web Management servers for email on page 297

Component	Servers
Required core servers	• ADU server • Alarm server • Blender server • Data server • Directory server • EDU server • License server • ORB server • Notification server • Report server • Workflow server • Secondary ADU servers on each computer with a Resource Manager server • Secondary EDU servers for contacts in supported media channels • DUStore server for Email Management
Optional core servers	For systems with multiple servers, install additional core servers as described in the following sections: • Interaction Center single site deployment scenarios on page 79 • Interaction Center multi-site deployment scenarios on page 123

Prerequisites for Business Advocate servers

The following table shows the software that you must install on a computer that host one or more Business Advocate servers. For more details about the definition of supported versions and about subsequent updates or service packs of the software, see About the supported versions on page 286.

You also need to configure Windows Server 2008 R2 to enable the Application Server role. For more information, see Enabling Application Server Role on page 301.

Enabling Application Server Role

For Business Advocate Servers you must activate the Application Server Role.

To configure Windows Server 2008 R2 with an Application Server role:

1. Select **Start** > **Administrative Tools > Server Manager**.
2. In the Server Manager window, in the left pane, select **Roles**.

3. In the right pane, under **Roles Summary** category, click **Add Roles**.
4. In the **Add Roles Wizard** window, in the **Before you Begin** screen, click **Next**.
5. In the **Select Server Roles** screen, under **Select one or more roles to install on this server, select Application. Roles:** select **Application Server**. A new window appears.
6. In the **Add role services required for Application Server?** window, click **Add Required Role Services**.
7. In the Select Server Roles screen, click **Next**.
8. In the **Application Server** screen, click **Next**.
9. In the **Select Role Services** screen, select the following**:**
   - Net Framework 3.5.1
   - TCP Port Sharing
   - COM+ Network Access
   - Incoming Remote Transactions under Distributed Transactions
   - Outgoing Remote Transactions under Distributed Transactions
   - Message Queuing Activation
   - TCP Activation
   - Named Pipes Activation
10. Click **Next.**
11. In the **Confirm Installation Selections** screen, click **Install**.
12. In the **Installation Results** screen, click **Close**.

Certain switches and software support only certain functions and components. For more detailed information, see Supported Telephony switches and software on page 231.

Required software	Location	Supported versions[1]		
		Microsoft Windows	Oracle Solaris	IBM AIX
Operating systems	All servers except Resource Manager server	Windows Server 2008 R2 or Windows 2012 R2	Oracle Solaris 10 update 9	AIX 6.1
	Computer that hosts Resource Manager server	Windows Server 2008 R2 or Windows 2012 R2	Not supported	Not supported
Windows Message Queuing services	Computer that hosts Resource Manager server	Provided with Windows	Not supported	Not supported
Time synchronization utility	All core servers	third-party NTP application	NTP application	NTP application
PDF reader for documentation	All core servers	Adobe Acrobat Reader	Adobe Acrobat Reader	Adobe Acrobat Reader
Microsoft Active Directory (optional)	Computer that hosts Resource Manager server and/or domain controller	Provided with Windows.	Not supported	Not supported
Telephony switches and software	As required by switch or software	For information about required software for Telephony, see Required software for Telephony on page 291. Business Advocate does not have any special requirements for Telephony.		
Web Management	As required by software	For information about required software for Web Management, see Required software for Web Management on page 293. Business Advocate does not have any special requirements for Web Management.		

Required software	Location	Supported versions[1]		
		Microsoft Windows	Oracle Solaris	IBM AIX
Email Management	As required by software	For information about supported software for Email Management, see Required software for Email Management and Content Analyzer on page 296. Business Advocate does not have any special requirements for Email Management.		
Content Analyzer	As required by software	For information about supported software for Content Analyzer, see Required software for Email Management and Content Analyzer on page 296. Business Advocate does not have any special requirements for Content Analyzer.		

1. Avaya IC 7.3.x supports VMWare ESX Server 4.1, VMWare ESXi Server 5.0, and VMWare ESXi Server 5.1. For information about IBM LPAR support, see IBM Logical Partition (LPAR) technology on page 192.

Required software for the Interaction Center Client SDK

The following table shows the software that you must install on computers that host one or more server-side components for the Interaction Center Client SDK. For more details about the definition of supported versions and about subsequent updates or service packs of the software, see About the supported versions on page 286.

Note:

IBM AIX and IBM DB2 is only supported on Interaction Center Release 7.3, 7.3.1, and 7.3.2. For more information see the Unsupported features on page 30. All the information related to IBM AIX and IBM DB2 is only applicable to Interaction Center Release 7.3, 7.3.1, and 7.3.2. For details on JRE/JDK see Unsupported features on page 30.

Required software	Location	Supported versions		
		Microsoft Windows	Oracle Solaris	IBM AIX
Operating systems	All Client SDK servers	Windows Server 2008 R2 or Windows 2012 R2	Oracle Solaris 10 update 9	AIX 6.1
Time synchronization utility	All Client SDK servers	third-party NTP application	NTP application	NTP application
PDF reader for documentation	All Client SDK computers	Adobe Acrobat Reader	Adobe Acrobat Reader	Adobe Acrobat Reader
Java Runtime Environment (32-bit)	Computer that hosts Java sample client	Oracle JDK	Oracle JDK	IBM J9 2.4 J2RE 1.6.0 SR15
.NET version	Computer that hosts .NET sample client	.NET version 3.5 and above	Not supported	Not supported

Required software for Interaction Center for Siebel

An Interaction Center for Siebel system requires the same software as an Interaction Center system. IC 7.3 supports the following:

- Integration with Siebel 8.1.1.x, 8.2.2.x, and 15.0.0.0.

- On AIX 6.1, IC 7.3 Siebel integration is only supported with Siebel 8.1.1.3 and later.
- If Siebel is installed on Windows Server, then the Siebel side IC integration components must be installed on the Windows Server. Other than this scenario, you must not install any of the IC components on Windows Server.
- On Red Hat Enterprise Linux 6.5, IC 7.3 Integration is only supported with Siebel Innovation Pack 14 and 15.
- If Siebel is installed on Red Hat Enterprise Linux Server 6.5, then the Siebel side IC integration components (ICSideLinux as Secondary ORB and SiebelSideLinux as AICD) must be installed on the Linux Server. The other IC Server components must be installed either on Windows or Solaris.

Note:

For detailed information about the components and prerequisites required for Interaction Center for Siebel, see *Avaya IC for Siebel Integration* guide. For information about the requirements for Siebel, see the documentation provided by Siebel.

Required software for Design & Administration Tools

The Design & Administration Tools for Interaction Center include the following components:

- IC Manager
- Database Designer
- Workflow Designer

The following table shows the software that you must install on computers that host one or more of the Design & Administration Tools. For more details about the definition of supported versions and about subsequent updates or service packs of the software, see About the supported versions on page 286.

Required software	Location	Supported versions
Operating systems	All computers	• Microsoft Windows Server 2012 R2 (IC Release 7.3.3 and later) • Windows Server 2008 R2 • Windows 10 Professional (IC Release 7.3.4 and later) • Windows 8.1 Professional (IC Release 7.3.3 and later) • Windows 7 (32-bit and 64-bit) • Windows Vista (32-bit) (IC Release 7.3, 7.3.1, and 7.3.2) • Windows XP Professional SP3 (32-bit) (IC Release 7.3, 7.3.1, and 7.3.2)
PDF reader for documentation	All computers	Adobe Acrobat Reader
Java Virtual Machine (32-bit)	Computer that runs the Web browser for Email Template Administration	For details see Unsupported features on page 30.
Web browser	All computers	Internet Explorer 11 (32-bit) Internet Explorer 10 (32-bit) Internet Explorer 9 (32-bit) Internet Explorer 8 Internet Explorer 7

Required software for agent applications

The agent applications for Interaction Center include the following:

- Avaya Agent
- Avaya Agent Web Client

This section describes the prerequisite software required to support the agent applications. This section includes the following topics:

- Prerequisites for Avaya Agent on page 308

- Requirements for Avaya Agent Web Client on page 309
- Prerequisites for agent desktop applications on Citrix on page 310

Prerequisites for Avaya Agent

The following table shows the software that you must install on computers that host Avaya Agent.

Required software	Supported versions
Operating systems	• Microsoft Windows 8.1 Professional (For IC 7.3.3 and later) • Microsoft Windows 7 (64-bit and 32-bit) • Microsoft Windows Vista (32 bit) (For IC 7.3, 7.3.1, and 7.3.2) • Microsoft Windows XP Professional SP3 (32 bit) (For IC 7.3, 7.3.1, and 7.3.2)
PDF reader for documentation	Adobe Acrobat Reader
Web browser	Internet Explorer 11 (32-bit) Internet Explorer 10 (32-bit) Internet Explorer 9 (32-bit) Internet Explorer 8 Internet Explorer 7
.NET version	Microsoft .NET Framework 3.5 and above

Requirements for Avaya Agent Web Client

The Avaya Agent Web Client software must be installed in addition to the software required by the Interaction Center servers. Avaya Agent Web Client is a browser-based application for the agents in your contact center.

This section includes the following topics:

- Required application server software on page 309
- Required software for Avaya Agent Web Client on page 309

Required application server software

The following table lists the software you must install on an application server to run Avaya Agent Web Client. This software is installed *in addition to* the software required by the Interaction Center servers.

Required software	Supported operating system versions		
	Windows	Oracle Solaris	AIX
Time synchronization utility	Third-party NTP application	NTP application	NTP application

Required software for Avaya Agent Web Client

The following table lists the software you must install on your agent desktop systems to access Avaya Agent Web Client:

Required software	Supported version
Operating system	• Microsoft Windows 8.1 Professional • Microsoft Windows 7 (64-bit and 32-bit) • Microsoft Windows Vista (32 bit) • Microsoft Windows XP Professional SP3 (32 bit)
Java J2RE plug-in	For details see Unsupported features on page 30. **Note:** J2RE installs with IC when you install agent desktop on Avaya Agent Rich Client. However, you must install J2RE on the machine that you use to access Avaya Agent Web Client
Web browser	Internet Explorer 11 (32-bit) in compatibility mode Internet Explorer 10 (32-bit) Internet Explorer 9 (32-bit) Internet Explorer 8 Internet Explorer 7

Prerequisites for agent desktop applications on Citrix

Interaction Center supports only Avaya Agent with certain features on Citrix. For detailed information about the limitations of support for Citrix, see Limitations on support for Citrix on page 280.

The following table shows the software that you must install on Citrix servers and on agent computers if you want to host a supported agent desktop application on Citrix.

Required software	Supported versions
Operating systems	• Windows Server 2012 R2 • Windows Server 2008 R2
Citrix XenApp	6.5 or 7.5

Required software	Supported versions
PDF reader for documentation	Adobe Acrobat Reader
Web browser	• Internet Explorer 10 (32-bit) • Internet Explorer 9 (32-bit) • Internet Explorer 8 • Internet Explorer 7

Upgrading Daylight Saving Time (DST) patches

IC 7.3.x is compliant with the Daylight Saving Time (DST) factor.

The major Operating System (OS) vendors have already released patches to support DST. IC customers must upgrade their operating system versions with the required DST patches from the websites of the respective operating system vendor.

The JRE can be updated using tools from the respective vendors. You can update JRE using the **TZUpdater** Tool on Windows and Oracle Solaris and **JTZU** tool on AIX:

To update JRE using the time zone updating Tool:

1. Stop all IC servers, services and log out Avaya Agent.
2. Update JRE that comes with IC.
3. For Windows and Oracle Solaris:
   - You can download the **TZUpdater** Tool from the Oracle website. For installation instructions see the documentation on the Oracle website.
4. For AIX:
   - You can download the **JTZU** Tool from the IBM website. For installation instructions see the documenation on the IBM website.

Note:

- JRE is located in the *IC_INSTALL_DIR*\IC73\Java directory.
- If you are changing the time zone after installing and configuring Avaya IC, update the adl query and regenerate the database.

Comments on this document? infodev@avaya.com

Chapter 17: Supported third-party applications

Interaction Center works with several third-party applications from other vendors. These applications support various functions within the product, such as database management and reports.

This section includes the following topics that describe third-party applications:

- Adobe Acrobat Reader on page 313
- Compilers for Interaction Center Server SDK on page 314

The following topics in other sections provide information about supported third-party applications and the requirements of Interaction Center:

- Required software components on page 285
- Operating systems, see Supported operating systems on page 263
- Database management systems, see Supported database management systems on page 209
- Telephone switches, see Supported Telephony switches and software on page 231
- Web servers, see Supported Web servers on page 235
- Email servers, see Supported email servers on page 243
- Tomcat, see Configuring Tomcat for Interaction Center Client SDK server and Web Services server (Optional) on page 240

For more information about OA and its prerequisites, see OA *Installation Planning and Prerequisites*. For detailed information about Interaction Center for Siebel, see *Avaya IC for Siebel Integration* guide.

Adobe Acrobat Reader

Interaction Center requires Adobe Acrobat Reader 5.0 (or later) to view and access the cross-document indexing and search capabilities of the Interaction Center documentation.

The PDF documents are available on the Avaya Support website at http://www.avaya.com/support.

You can download the free Acrobat Reader and the separate Search functionality from the Adobe website at http://www.adobe.com/

Compilers for Interaction Center Server SDK

If you build custom Interaction Center servers with the SDK, you must use the supported compiler for the Interaction Center server operating system. The following table lists the supported compilers:.

Server operating system	Supported SDK compiler
AIX	IBM XL C/C++ Enterprise Edition for AIX, V9.0
Oracle Solaris	Sun Studio 12
Windows	Microsoft Visual Studio .Net 2005

Compilers for Interaction Center SDK Sample Clients

You can use the sample clients provided by Avaya and need only runtimes. But if you wish to make your own custom SDK clients, you will need compilers and runtimes listed below.

Java Sample Client:

- Compiler / JDK:
  - Windows: Oracle JDK 1.8.0_40 (32-bit) (with target and source as 1.7)
  - Oracle Solaris: Oracle JDK 1.8.0_40 (32-bit) (with target and source as 1.7)
  - AIX: Java™ SE Runtime Environment (build pap3260sr3-20081106_07(SR3))
  - IBM J9 VM (build 2.4, J2RE 1.6.0 IBM J9 2.4 AIX ppc-32 jvmap3260-20081105_25433 (JIT activated, AOT activated)
- Java Runtime Environment (32-bit):
  - Windows: 1.8.0_40 (32-bit) (with target and source as 1.7)
  - Oracle Solaris: Oracle JRE 1.7.0 (32-bit)
  - AIX: Java™ SE Runtime Environment (build pap3260sr3-20081106_07(SR3))
  - IBM J9 VM (build 2.4, J2RE 1.6.0 IBM J9 2.4 AIX ppc-32 jvmap3260-20081105_25433 (JIT activated, AOT activated)

Note:
For more details see Unsupported features on page 30.

C# Sample Client

- IDE/Compiler:
  - Windows: Microsoft Visual Studio 2005
  - Oracle Solaris: Not Supported
  - AIX: Not Supported
- Runtime:
  - Windows: Microsoft .NET Framework 3.5.
  - Oracle Solaris: Not Supported
  - AIX: Not Supported

Comments on this document? infodev@avaya.com

Chapter 18: Server virtualization support

Avaya Interaction Center 7.3 supports virtualization of Windows Operating System as a guest operating system on VMware. In a virtualized environment, a single physical computer runs software that abstracts the physical computer's resources, so that they may be shared between multiple virtual computers. In virtualization, the term host server refers to the actual physical hardware server on which the virtualization takes place. The term guest refers to a virtual machine on the host server.

The benefits of using virtualization include the following:

- Decrease hardware, power, and cooling costs by running multiple operating systems on the same physical server.
- Lower management overhead costs by reducing the hardware footprint in Interaction Center.
- Guarantee high levels of performance for the most resource-intensive applications.
- Consolidate hardware resources with a production-proven and secure server virtualization platform.

Interaction Center supports the following virtualization:

- VMware vSphere Releases 4.1, 5.0, 5.1, 5.5, and 6.0 (ESXi and ESX versions) virtualization environment
- Microsoft Hypervisor Release 2012 and 2012 R2

Using virtualization in an Interaction Center enterprise solution requires careful up-front planning, engineering, and implementation. While the technical and business advantages are clear, virtualization imposes extra considerations when designing the Interaction Center solution architecture. Virtualization supports security and fault isolation. With environmental isolation, multiple operating systems can run on the same system. While virtualization offers these forms of isolation, virtualization environments do not really provide performance isolation. The behavior of one virtual machine can adversely affect the performance of another virtual machine on the same host. Most modern virtualization environments provide mechanisms that you can use to detect and reduce performance interference. You must carefully engineer your virtualized Interaction Center solution to avoid performance interference.

If you plan to install non-Interaction Center software applications on the other guests of a host server with Interaction Center installed, you must carefully analyze the impact of these applications on the Interaction Center solution and provide extra performance isolation to safeguard the functionality of Interaction Center.

Deploy Avaya Interaction Center on an enterprise-grade virtual environment with the most recent hardware that supports hardware-assisted virtualization. You must apply virtualization planning, engineering, and deployment with full organizational support for virtualization rather than organically growing a virtualization infrastructure.

This section provides information about engineering and commissioning Interaction Center using virtualization.

VMWare support

VMware vSphere Release 4.1 and later. All Interaction Center components supported on the Windows platform are supported on VMware. VMware vSphere allows multiple copies of the same operating system or several different operating systems to run as guests on a large x86-based host hardware server. The design of a virtualized system must follow the same guidelines for sizing and design as a normal physical deployment. Analyze your Interaction Center agent and call flow requirements and determine the specification and number of Interaction Center servers required. You must ensure that each guest (virtual machine) on which you plan to install Interaction Center software satisfies the capacity requirements and specifications for your Interaction Center. You must verify which Interaction Center applications can be installed co-resident on a virtual machine, while simultaneously considering your agent count and call rate.

This section includes the following topics:

- VMware vSphere Host considerations on page 319
- VMware Interaction Center Guest Operating Systems on page 321
- Overview of commissioning Interaction Center with VMware on page 321
- Performance monitoring and management on page 323
- VMware Snapshot considerations on page 324
- Time synchronization considerations on page 325
- Troubleshooting VMware on page 330

The following diagram shows a typical Interaction Center solution using virtualization. The diagram shows Interaction Center on a standalone virtual machine:

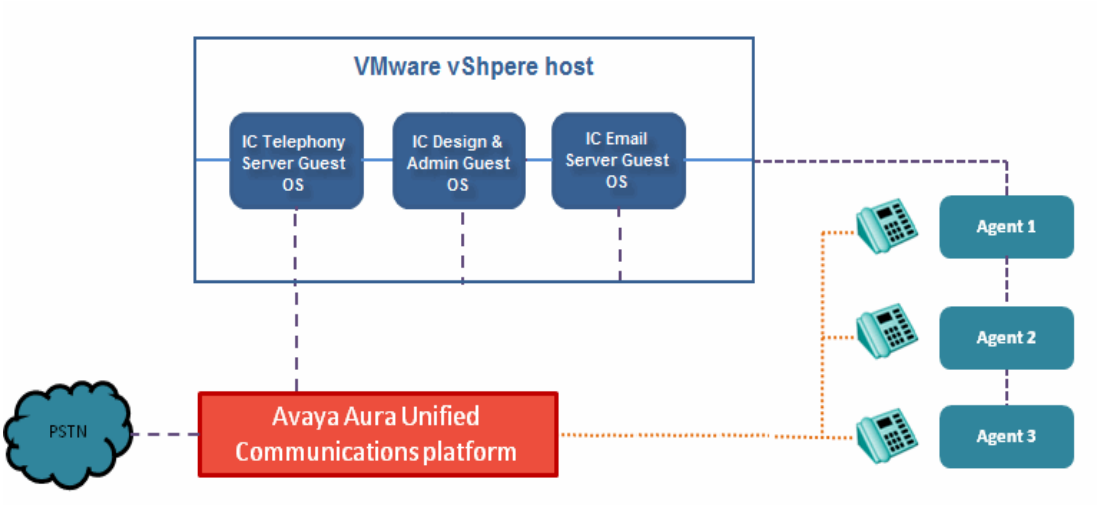


Figure 1: A sample multimedia Interaction Center solution using virtualization

Interaction Center does not support the following:

- VMware High Availability
- VMware Suspend and Resume

VMware vSphere Host considerations

When configuring virtual machines (guests) on your host system, the total resources needed by the virtual machines running on the host server must not exceed the total capacity of the host. It is good practice to under-commit CPU and memory resources on the host. If the host CPU capacity is overloaded, Interaction Center does not function correctly.

Important:
Interaction Center is not supported on an over-committed host where the total virtual resources from all the hosted virtual machines exceed the physical resources of the host.

This section includes the following topics:

- Hardware-Assisted Virtualization on page 320
- Hardware-Assisted CPU Virtualization (Intel VT-x and AMD-V) on page 320
- Hardware-Assisted MMU Virtualization (Intel EPT and AMD RVI) on page 320
- Storage Area Network (SAN) on page 320
- Disk drive provisioning on page 320

Hardware-Assisted Virtualization

Most recent enterprise-level processors from Intel and AMD support virtualization. There are two generations of virtualization support:

- The first generation introduced CPU virtualization
- The second generation included CPU virtualization and the memory management unit (MMU) virtualization.

For the best performance, make sure your system uses processors with at least the second-generation hardware-assist features.

Hardware-Assisted CPU Virtualization (Intel VT-x and AMD-V)

The first generation of hardware virtualization assistance includes technologies, such as VT-x from Intel and AMD-V from AMD. These technologies automatically trap sensitive interrupts, eliminating the overhead required to do so in software. This allows the use of a Hardware Virtualization (HV) Virtual Machine Monitor (VMM).

Hardware-Assisted MMU Virtualization (Intel EPT and AMD RVI)

More recent enterprise-level processors also include a feature that addresses the overheads due to MMU virtualization by providing the hardware support to virtualize the MMU. VMware vSphere supports this feature both in AMD processors, where it is called Rapid Virtualization Indexing (RVI) or nested page tables (NPT), and in Intel processors, where it is called Extended Page Tables (EPT).

Storage Area Network (SAN)

A Storage Area Network (SAN) is a dedicated storage network that provides access to consolidated block level storage. SANs are used to make storage devices, such as disk arrays, accessible to servers so that the devices appear as locally attached to the operating system. You must monitor the Interaction Center demand on the SAN storage device. Adhere to your vendor-specific SAN configuration recommendations to ensure that the SAN storage device meets the demands of Interaction Center. When Interaction Center is installed on virtual machines, it supports a SAN.

Disk drive provisioning

Provision sufficient hard disk drive space on the host server to support all the guest virtual machines, an ISO library, and provision additional space for snapshot image storage.

VMware Interaction Center Guest Operating Systems

Provision each Interaction Center virtual machine with at least the same specification as is listed for the physical server. For improved disk performance, configure the virtual hard disk to use the pre-allocated mode. The networking requirements of each virtual machine are the same as the networking requirements of an equivalent physical server.

If any of the following is true, an in-depth technical assessment is recommended:

- Guest CPU: Minimum accessible capacity is under 4 CPUs or minimum guaranteed capacity is under 1 CPUs.
- Memory: Minimum guaranteed capacity is under 2 GB.
- Disk: Free space is under 100 GB capacity.
- If the minimum guaranteed capacity does not exceed the busy-hour resource consumption of the guest.

Important:
You must review the Guest OS performance during the peak hours and determine the minimum guaranteed capacity and fine tune the VMware settings for the optimal performance of Interaction Center. For fine tuning the host OS/guest OS, contact VMware.

Install the most recent version of VMware Tools on each guest operating system.

For improved performance, follow these recommendations:

- Disable screen savers and Window animations on the virtual machines. Screen savers and animations consume extra physical CPU resources, potentially affecting the consolidation ratios and the performance of other virtual machines.
- Schedule backups and virus scanning programs in virtual machines to run at the off-peak hours and do not schedule them to run simultaneously in multiple virtual machines on the same VMware host.

Overview of commissioning Interaction Center with VMware

This section outlines how to engineer and install a virtualized environment to support Interaction Center.

1. Read VMware Performance Best Practices for VMware.

2. To determine the exact hardware requirement based on your Contact Center requirements/capacity, contact Avaya Professional Services or Avaya Business Partner. For more information about the IC hardware requirements, refer to Interaction Center hardware requirements on page 189. Each required Interaction Center server equates to one guest virtual machine. The specification of each virtual machine must be at least the same as the specification of an equivalent physical Interaction Center server.
3. Read the documents of your hardware provider covering virtualization support.
4. Combine the individual Interaction Center virtual machine specifications to determine the minimum specification for the Interaction Center VMware vSphere host server hardware.
5. Obtain a server hardware that meets the Interaction Center host hardware specification and that supports VMware vSphere.
6. Install the most recent BIOS available for your host server.
7. On the host server, disconnect or disable unused or unnecessary physical hardware devices, such as COM ports, LPT ports, USB controllers, Network interfaces, and Storage controllers.
8. On the host server, enable all available Virtualization Technology options in the hardware BIOS:
   - For Intel-based hosts enable Intel virtualization (VT-x), and if available, enable Extended Page Tables (EPT).
   - For AMD-based hosts enable AMD virtualization (AMD-V), and if available, enable Rapid Virtualization Indexing (RVI).
9. If the host hardware and BIOS support hyper-threading, vSphere automatically makes use of it. For the best performance, enable hyper-threading on the host server.
10. Install VMware vSphere software on the host server.
11. Using the vSphere client, configure each Interaction Center guest virtual machine with the CPU, memory, and disk space.
12. On each Interaction Center guest virtual machine, completely disable time synchronization to the host time.
13. Add the Interaction Center DVD image to the vSphere ISO library.
14. Prepare each guest virtual machine for Interaction Center. Configure disk partitions and install guest Windows Server operating system.
15. On each Interaction Center guest virtual machine, perform the Interaction Center server preparation procedures.
16. Install Interaction Center software on the guest operating system.
17. You must set the Network adapter setting to 1 Gbps Full Duplex in the VMware host server and in each Interaction Center guest virtual machine.
18. Commission and deploy each Interaction Center virtual machine as normal.
19. Capture the initial CPU and memory usage, as baseline performance metrics.

20. Continue to monitor the CPU and memory of each Interaction Center guest virtual machine.
21. Continue to monitor all the resources of the vSphere host server, focusing on CPU, memory, and disk drive resources.

Note:

The above points are only guidelines to install/deploy Interaction Center on VMware. Based on the guest OS resource requirement, determine the Host VMware capacity/hardware by contacting your IT support or VMware.

Performance monitoring and management

You must continuously monitor and measure the performance of the Interaction Center host server. You can use VMware vSphere vCenter to measure the critical host performance metrics in real-time. VMware vCenter aggregates and archives performance data so that data can be visualized and reported on.

Configure VMware vCenter statistics collection to collect 5 minute and 30 minute Interval Duration data for the host at Statistics Level 3. Retain the 5 minute Interval Duration data for three days and retain the 30 minute Interval Duration for one week. Generate performance reports using vCenter Report Performance and archive these reports to provide a baseline performance reference.

Generate and store 1-day and 1-week reports. Store the associated vCenter Report Summary with the performance reports. You must analyze performance reports after changes to the host to assess the impact of the change on the host.

Monitor, acknowledge, and resolve VMware vCenter alarms. In particular, you must immediately investigate and resolve host CPU usage and host memory usage alarms.

In addition, the command-line tools “esxtop” and “resxtop” (available only for VMware ESX) are available to provide a fine grained look at real-time metrics. There are a number of critical CPU-related counters to watch out for:

- If the load average listed on the first line of the CPU Panel is equal to or greater than the number of physical processors in the system, this indicates that the system is overloaded.
- The usage percentage of physical CPUs on the PCPU line can indicate an overloaded condition. In general, 80 percent usage is a reasonable ceiling in production environments. Use 90 percent to alert the VMware administrator that the CPUs are approaching an overloaded condition and must be addressed.
- **%RDY**: The percentage of time a schedulable entity was ready to run, but is not scheduled to a core. If %RDY is greater than 10 percent, then this can indicate resource contention.
- **%CSTP**: The percentage of time a schedulable entity is stopped from running to allow other vCPUs in the virtual machine to catch up. If %CSTP is greater than 5 percent, this usually means the virtual machine workload is not using VCPUs in a balanced fashion.

For more information about using esxtop or resextop, see the VMware Resource Management Guide.

Memory Reservations

Use VMware Reservations to specify the minimum amount of memory for an Interaction Center virtual machine. VMware Reservations maintain sufficient host memory to fulfill all reservation guarantees. ESX does not power-on a virtual machine if doing so reduces the amount of available memory to less than the amount reserved. Using reservations may reduce the total number of virtual machines that can be hosted on a VMware host server. After all resource reservations have been met, ESX allocates the remaining resources based on the number of shares and the resource limits configured for your virtual machine.

The recommended reservations value for an Interaction Center virtual machine is 75% of the memory requirement.

VMware Snapshot considerations

VMware snapshots save the current state of the virtual machine, so you can return to it at any time. Snapshots are useful when you need to revert a virtual machine repeatedly to the same state, but you do not want to create multiple virtual machines.

Important:
VMware snapshots are not a replacement for Interaction Center database backup (and restore) procedures and practices. You must continue to perform regular and frequent Interaction Center backups.

The following considerations apply when using snapshots with Interaction Center on VMware:

- Snapshots must be taken during an Interaction Center maintenance window. Do not take a snapshot of an Interaction Center virtual machine while Interaction Center is running.
- Create a snapshot for the Interaction Center virtual machines all at the same time. Likewise, when you restore a snapshot, restore all snapshots to ensure the data is consistent across the Interaction Center suite.
- Snapshots have a negative impact on the performance of a virtual machine over time. The amount of disk space used increases with the number of snapshots taken and stored. Snapshots must be consolidated within 25 days.
- When restoring snapshots, carefully consider the possible impact from out-of-date antivirus definitions, missed OS and security updates, and lapsed domain accounts on the Interaction Center. Isolate the restored virtual machine until these issues are resolved.

Time synchronization considerations

VMware time synchronization controls whether the virtual machine time is periodically re-synchronized with the host server while it is running. Even if you did not select the VMware time synchronization check, VMware Tools by default synchronizes the virtual machine's time after a few specific events that are likely to leave the time incorrect, and this might cause discrepancy in the Interaction Center reports. Follow the VMware instructions (KB 1189) to completely disable host time synchronization on the virtual machine running Interaction Center. Install compliant time synchronization software as per the IC 7.3 Installation Planning and Prerequisites Guide.

VMware Horizon View

Horizon is a family of desktop and application virtualization solutions, which provide a streamlined approach to deliver, protect, and manage Windows desktops and applications to the user. This approach helps the user work anytime, anywhere, on any device.

VMware Horizon View is a desktop virtualization solution that delivers virtual desktop services. You can use Horizon View to simplify and automate the management of desktops and securely deliver desktops as a service to users from a central location.

A single administration console provides granular levels of control, so that you can customize the user experience, access, and personalization to support corporate policy. Users get a familiar, personalized environment that the users can access from any number of devices anywhere throughout the enterprise or from remote locations. And as an Administrator, you have centralized control, efficiency, and security by having desktop data in the data center.
For more information about VMware Horizon view, see http://www.vmware.com.
AIC rich client and thin client is supported using Horizon desktop virtualization solutions, user can connect to horizon desktop using VMWare Horizon with standalone client. AIC rich client and thin client not tested with VMWare Horizon with web/mobile clients.

This section contains the following:

- Installing the agent applications on the Horizon view desktop on page 325
- Configuring the Avaya Agent INI file on page 326
- Configuring the Web Client URL pre-requisite on VMware Horizon View Master Image on page 327

Installing the agent applications on the Horizon view desktop

To install the agent desktop applications on a Horizon view desktop, follow the procedures in Testing the agent installer on page 369. Do not perform any more steps during the installation.

To work AIC rich client application successfully with horizon view desktop virtualization solution, the following steps are mandatory:

1. Install Avaya Rich Client application under **C:\Program Files (x86)** on Horizon view master desktop image.
2. Give full access windows permissions to **C:\Program Files (x86)\Avaya** directory for all AD domain users who are accessing horizon view desktops remotely to use AARC.

Depending on the environment, you might need to adjust the size of the Avaya Agent-framework then recreate the agent installer. For more information about how to customize the framework size, see *Avaya Agent Integration*.

Configuring the Avaya Agent INI file

If the IC system includes agents accessing the Horizon view client interface with the seamless window, you must configure the Avaya Agent INI file on Horizon view master desktop system. You must configure the Avaya Agent INI file on the Horizon view master desktop system from where horizon view desktop virtualization solution is configured.

The parameter needed for the seamless window can cause undesirable formatting and sizing of the Avaya Agent in other deployments.

Note:
Avaya IC agent is supported with Horizon View 5.3 release with Microsoft Windows 7 desktop virtualization solution.

To configure the Avaya Agent INI file:

1. In Notepad or another text editor, open a new document.
2. Type the following information into the document:

   ```
   [QConsole]

   ResizeDesktop=FALSE
   ```

3. Save the file with the following name: `qui.ini`
4. Install the file in the Windows installation directory on Horizon view desktop master image that hosts IC agent desktop applications.

   For example, the Windows installation directory is usually `C:\Windows`
5. If qui.ini file already exist user can just edit the file and append above step 2 parameters and save the file.

Configuring the Web Client URL pre-requisite on VMware Horizon View Master Image

Avaya IC 7.3.3 and later versions, supports access to web client for the agents who are logged in through VMware Horizon View solution.

The following procedure provides details on how to login to thin client agent on all published Horizon View desktop clients.

To configure web client URL pre-requisite on Horizon View master image before publishing for desktop creation, do the following:

1. Horizon View master image must have the supported version of Internet explorer.
2. Ensure that the latest JRE 8, 32 bit is installed on master image and the Internet Explorer browser is using JRE 8 to login to Avaya Agent Web Client.
3. Launch the Internet Explorer.
4. Access Avaya Agent Web Client URL.

   http://<WebConnectorServerIP>:<TomcatPort>/avaya/agent
5. Accept and install Active X Control installation options, if any.
6. Choose to allow access to all required controls.
7. Verify if IC agent is logged in successfully on the thin client.
8. Logout of Avaya Agent Web Client.

Note:

Avaya Agent Web Client is tested and supported with Horizon view Virtual solution on Internet Explorer 10 and 11 of Microsoft Windows 7 Operating System. Avaya Agent Web Client is supported using Horizon desktop virtualization solutions, you can connect to horizon desktop using VMWare Horizon with standalone client. Thin client is not tested with VMWare Horizon with web or mobile clients. Avaya Agent Web Client is not supported in VMWare ThinApp mode.

About VMware vSphere vMotion

VMware vSphere vMotion enables the live migration of running virtual machines from one physical server to another with zero downtime, continuous service availability, and complete transaction integrity. vMotion is key enabling technology for creating the dynamic, automated, and self-optimizing data center. VMware vMotion is supported in IC from IC 7.3.3 onwards.

vMotion is a VMware feature that migrates a running virtual machine from one physical server to another with minimal downtime or impact to end users. vMotion cannot be used to move virtual machines from one data center to another. Only the CPU and memory instances on ESXi host gets migrated, virtual machine files on datastore are not migrated. There might be live contacts drop, agent disconnect, or connection timeout on the IC server when using vMotion.

Storage vMotion is a VMware feature that migrates files on a running virtual machine files from the current datastore to a new datastore. When you use Storage vMotion the ESXi host is not changed, only the datastore file location is changed from the current datastore to the new datastore.

Note:

IC does not support VMware vSphere Storage vMotion.

Configuring Hosts for vMotion and Migrating Powered-On Virtual Machines

This scenario demonstrates how to configure vCenter Server and ESX/ESXi hosts so that you can migrate powered-on virtual machines without downtime. vMotion is a prerequisite for advanced vSphere features such as vSphere Distributed Resource Scheduler (DRS) and vSphere High Availability (HA), however AIC does not support with DRS and HA features of vSphere, AIC supports vMotion and Migrate Powered-On Virtual Machines from ESXi host to host with below Prerequisites.

Prerequisites

- Verify that you have at least two ESXi hosts that are licensed for vMotion.
- Verify that you have running instances of vCenter Server and the vSphere Web Client.
- Verify that hosts have access to shared storage of a supported type, such as Fibre Channel, iSCSI, or NAS.
- Verify that the source and destination hosts have compatible CPUs.
- Verify that hosts have access to the same physical networks.
- Verify that you have at least one active Gigabit Ethernet adapter on each host.
- Virtual machine files must be on shared storage visible by the hosts.
- Virtual machines must run a supported operating system.
- Virtual machines must not have a connection to a virtual media device with a mounted local image.
- Virtual machines must not have a connection to an internal vSwitch that is not connected to a physical network.
- Virtual machines must have access to the same subnets.

- Virtual machines must not have CPU affinity configured.

Migrating with vMotion

Migration with vMotion allows virtual machine working processes to continue throughout a migration. User has to do this migration of virtual machine with vMotion manually.

The entire state of the virtual machine, as well as its configuration file, if necessary, is moved to the new host, while the associated virtual disk remains in the same location on storage that is shared between the two hosts. After the virtual machine state is migrated to the alternate host, the virtual machine runs on the new host.

The state information includes the current memory content and all the information that defines and identifies the virtual machine. The memory content includes transaction data and whatever bits of the operating system and applications are in the memory. The defining and identification information stored in the state includes all the data that maps to the virtual machine hardware elements, such as BIOS, devices, CPU, MAC addresses for the Ethernet cards, chip set states, registers, and so forth.

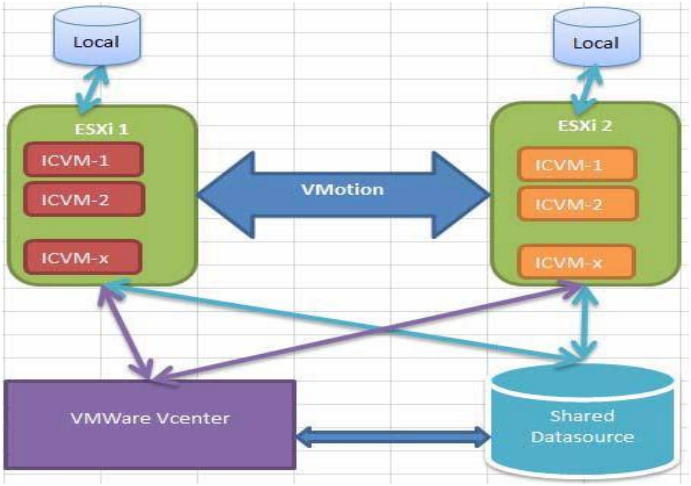
When you migrate a virtual machine with vMotion, the new host for the virtual machine must meet compatibility requirements in order for the migration to proceed as per above prerequisites.

Migration with vMotion happens in three stages:

1. When the migration with vMotion is requested, vCenter Server verifies that the existing virtual machine is in a stable state with its current host.
2. The virtual machine state information (memory, registers, and network connections) is copied to the target host.
3. The virtual machine resumes its activities on the new host.

If any error occurs during migration, the virtual machines revert to their original states and locations.

Avaya Interaction Center Deployment for VMotion



As shown in above diagram, two ESXi servers which having similar hardware configuration going to share common data storage, so that virtual machines can migrate from ESXi host to host, managing these two ESXi servers and VMotion activities we are going to use VMware VCenter.

Troubleshooting VMware

Virtualization platform performance issues can result in Interaction Center performance problems. The virtualization platform includes the host and the running virtual machines on the host. The Interaction Center performance problems can include, but are not limited to, high CPU usage, link instability, defaulted or abandoned calls.

You must logically and systematically investigate any Interaction Center performance issues to rule out virtualization performance problems. Rigidly follow the troubleshooting flows described in "Performance Troubleshooting for VMware vSphere" document on the VMware site at:

http://www.vmware.com

All deviations from the published specifications must be investigated and resolved before the Interaction Center software investigation is initiated.

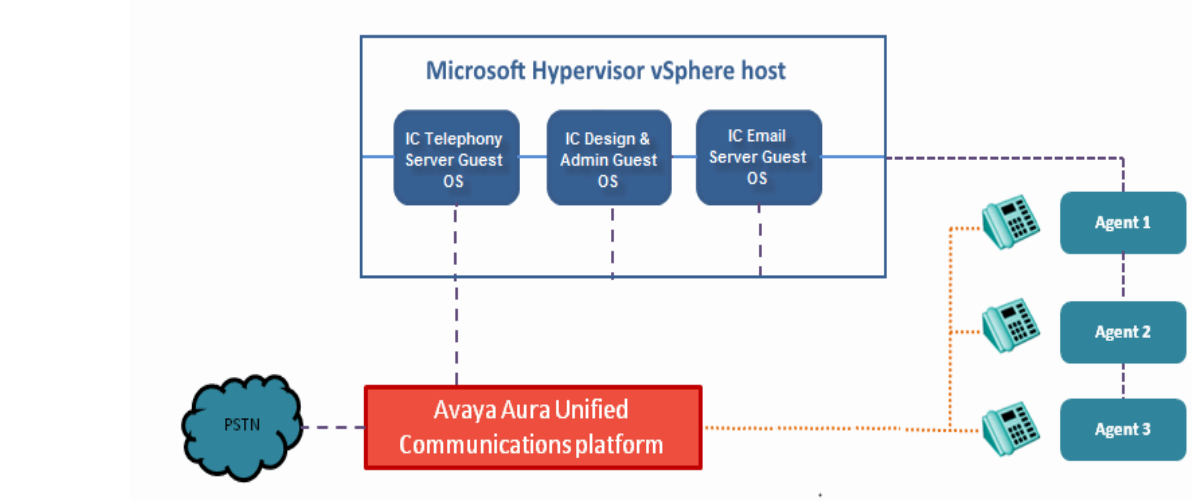
Microsoft Hypervisor support

All Interaction Center components supported on Windows platform are supported on Microsoft Hypervisor 2012 and 2012 R2. Microsoft Hypervisor allows multiple copies of the same operating system or several different operating systems to run as guests. The design of a virtualized system must follow the same guidelines for sizing and design as a normal physical deployment. Analyze your Interaction Center agent and call flow requirements and determine the specification and number of Interaction Center servers required. You must ensure that each guest (virtual machine) on which you plan to install Interaction Center software satisfies the capacity requirements and specifications for your Interaction Center. You must verify which Interaction Center applications can be installed co-resident on a virtual machine, while simultaneously considering your agent count and call rate.

This section includes the following topics:

- Microsoft Hypervisor Host considerations on page 332
- Using Hypervisor for Interaction Center Guest Operating Systems on page 332
- Overview of commissioning Interaction Center with Microsoft Hypervisor on page 333
- Microsoft Hypervisor Checkpoint considerations on page 335

The following diagram shows a typical Interaction Center solution using virtualization. The diagram shows Interaction Center on a standalone virtual machine:



Microsoft Hypervisor Host considerations

When configuring virtual machines (guests) on your host system, the total resources needed by the virtual machines running on the host server must not exceed the total capacity of the host. It is good practice to under-commit CPU and memory resources on the host. If the host CPU capacity is overloaded, Interaction Center will not function correctly.

Important:
Interaction Center is not supported on an over-committed host where the total virtual resources from all virtual machines hosted exceeds the physical resources of the host.

This section includes the following topics:

- Storage Area Network (SAN) on page 320
- Disk drive provisioning on page 320

Storage Area Network (SAN)

A Storage Area Network (SAN) is a dedicated storage network that provides access to consolidated block level storage. SANs are used to make storage devices such as disk arrays, accessible to servers so that the devices appear as locally attached to the operating system. You must monitor the Interaction Center demand on the SAN storage device. Adhere to your vendor-specific SAN configuration recommendations to ensure the SAN storage device meets the demands of Interaction Center. When Interaction Center is installed on virtual machines it supports a SAN.

Disk drive provisioning

Provision sufficient hard disk drive space on the host server to support all the guest virtual machines, an ISO library, and provision additional space for snapshot image storage.

Using Hypervisor for Interaction Center Guest Operating Systems

Provision each Interaction Center virtual machine with at least the same specification as is listed for the physical server. For improved disk performance, configure the virtual hard disk to use the pre-allocated mode. The networking requirements of each virtual machine are the same as the networking requirements of an equivalent physical server.

If any of the following is true, an in-depth technical assessment is recommended:

- Guest CPU: Minimum accessible capacity is under 4 CPUs or minimum guaranteed capacity is under 1 CPUs.

- Memory: Minimum guaranteed capacity is under 2 GB.
- Disk: Free space is under 100 GB capacity.
- If the minimum guaranteed capacity does not exceed the busy-hour resource consumption of the guest.

Important:
You must review the Guest OS performance during peak hours and determine the minimum guaranteed capacity and fine-tune the Microsoft Hypervisor settings for optimal performance of Interaction Center. For fine tuning the Host OS/Guest OS contact Microsoft.

For improved performance, follow these recommendations:

- Disable screen savers and Window animations on the virtual machines. Screen savers and animations all consume extra physical CPU resources, potentially affecting consolidation ratios and the performance of other virtual machines.
- Schedule backups and virus scanning programs in virtual machines to run at off-peak hours and do not schedule them to run simultaneously in multiple virtual machines on the same VMware host.

Overview of commissioning Interaction Center with Microsoft Hypervisor

This section outlines how to engineer and install a virtualized environment to support Interaction Center.

1. Read Best Practices for Microsoft Hypervisor.
2. To determine the exact hardware requirement based on your Contact Center requirements/capacity, contact Avaya Professional Services or Avaya Business Partner. For more information about IC hardware, see Interaction Center hardware requirements on page 189. Each Interaction Center server required equates to one guest virtual machine. The specification of each virtual machine must be at least the same as the specification of an equivalent physical Interaction Center server.
3. Read the documents of your hardware provider covering virtualization support.
4. Combine the individual Interaction Center virtual machine specifications to determine the minimum specification for the Interaction Center Microsoft Hypervisor host server hardware.
5. Obtain server hardware that meets the Interaction Center host hardware specification and supports Microsoft Hypervisor.
6. Install the most recent BIOS available for your host server.

7. On the host server, disconnect or disable unused or unnecessary physical hardware devices such as: COM ports, LPT ports, USB controllers, Network interfaces, Storage controllers.
8. On the host server, enable all available Virtualization Technology options in the hardware BIOS:
   - For Intel based hosts: Enable Intel virtualization (VT-x) and if available enable Extended Page Tables (EPT).
   - For AMD based hosts: Enable AMD virtualization (AMD-V) and if available enable Rapid Virtualization Indexing (RVI).
9. If the host hardware and BIOS support hyper-threading, Microsoft Hypervisor automatically makes use of it. For the best performance enable hyper-threading on the host server.
10. Install Microsoft Hypervisor software on the host server.
11. Using the Microsoft Hypervisor terminal, configure each Interaction Center guest virtual machine with the CPU, memory, and disk space.
12. On each Interaction Center guest virtual machine, completely disable time synchronization to the host time.
13. Add the Interaction Center DVD image to the ISO library.
14. Prepare each guest virtual machine for Interaction Center; configure disk partitions and install guest Windows Server 2008 R2 or Windows Server 2012 R2 Server operating system.
15. On each Interaction Center guest virtual machine, perform the Interaction Center server preparation procedures.
16. Install Interaction Center software on the guest operating system.
17. You must set the Network adapter setting to 1 Gbps Full Duplex in the Microsoft Hypervisor server and in each Interaction Center guest virtual machine.
18. Commission and deploy each Interaction Center virtual machine as normal.
19. Capture the initial CPU and memory usage, as baseline performance metrics.
20. Continue to monitor the CPU and memory of each Interaction Center guest virtual machine.
21. Continue to monitor all the resources of the Microsoft Hypervisor host server, focusing on CPU, memory, and disk drive resources.

Note:

The above points are only guidelines to install/deploy Interaction Center on Microsoft Hypervisor. Based on the Guest OS resource requirement, determine the Host Microsoft Hypervisor capacity/hardware by contacting your IT support or Microsoft.

Microsoft Hypervisor Checkpoint considerations

A checkpoint saves the state of each virtual hard disk that is attached to a virtual machine and all contents of the hard disk, including application data files. For virtual machines on Hyper-V host, a checkpoint also saves the hardware configuration information. By creating checkpoints for a virtual machine, you can restore the virtual machine to a previous state.

A typical use of checkpoints is to create a temporary backup before you update the operating system or an application, or make a configuration change on the virtual machine. A checkpoint gives access to you to restore the virtual machine to the previous state if the operation fails or adversely affects the virtual machine. For virtual machines on Hyper-V and ESX Server hosts, checkpoints are also useful in a test environment where to use multiple hardware configurations on a virtual machine.

Important:
Microsoft Hypervisor Checkpoint are not a replacement for Interaction Center database backup (and restore) procedures and practices. You must continue to perform regular and frequent Interaction Center backups.

This section includes the following topics:

- Creating Checkpoints on page 335
- Managing Checkpoints on page 335

Creating Checkpoints

You can create checkpoints only for a virtual machine that is deployed on a virtual machine host. You cannot create checkpoints for a virtual machine that is stored in the library.

For a virtual machine that is running on a Hyper-V, you can create a checkpoint without stopping the virtual machine.

You can create multiple checkpoints for a virtual machine. However, checkpoints use hard disk space and, when you proliferate, the checkpoints can affect the performance of a virtual machine when the machine is running. The performance is also affected during such virtual machine operations as migrating a virtual machine or storing it to the library. A best practice is to remove unneeded checkpoints.

Managing Checkpoints

After you create checkpoints, you can perform additional actions to manage the checkpoints.

Use the Restore action to restore a virtual machine to the state when a checkpoint was created.

When you no longer need to restore a virtual machine to a checkpoint, you can remove the checkpoint.

For Hyper-V checkpoints are portable. When you migrate, store, or deploy a virtual machine, any existing checkpoints move with the virtual machine.

Checkpoints are not intended for Backup

Checkpoints are intended to provide a temporary backup when you must restore a virtual machine to a previous state after a change. For example a system or an application update. However, you must not use checkpoints for the permanent backup of the operating system, applications, or files.

Checkpoints are stored with the virtual machine on the host. Therefore, if the host fails while the virtual machine is deployed, the checkpoints are lost. To provide data protection for your virtual machines, you must instead use the Volume Shadow Copy Service (VSS) writer for Virtual Server or a backup application. For example System Center Data Protection Manager (DPM), to back up your virtual machines to external storage.

If your virtual machines store user data files, you must back up the data files on a virtual machine before you restore the virtual machine to a checkpoint. When you restore the virtual machine, user data files on the virtual hard disks are returned to the previous state.

Memory management in Microsoft Hyper-V 2012

Microsoft Hyper-V 2012 has dynamic memory management. Since then you can enable dynamic memory on VM-level. After enabling the dynamic memory for a VM you can set a so called *Startup RAM*. *Startup RAM* is the amount of memory which is assigned to the VM during startup. Because Windows needs more memory during startup than the steady state, that is, Source. It must be set to the amount of memory which is needed to run the server and application with the level of performance required. You can also configure a *Minimum RAM*. *Minimum RAM* is the amount of memory up to which the hypervisor can reclaim memory using a ballooning technique. Because you can configure a *Minimum RAM*, you can also configure a *Maximum RAM*. *Maximum RAM* is the amount of memory up to which the hypervisor can add memory to the VM. And now comes the interesting part. The hypervisor adds memory to the VM using memory hot-add. If the VM needs more memory, the memory is added using hot-add to the VM. This explains why the OS inside the VM has to support memory hot-add in the case you use dynamic memory. And adding hot-add explains also why some applications are not supported with Hyper-V dynamic memory.

For AIC server VM you must have Minimum RAM at least 2 GB and Maximum RAM must be greater than or equal to 6 GB.

Important:
When installing or upgrading the operating system of a virtual machine, the amount of memory that is available to the virtual machine during the installation and upgrade process is the value specified as **Startup RAM**. Even if Dynamic Memory is configured for the virtual machine, the virtual machine only uses the amount of memory as configured in the **Startup RAM** setting. Ensure the **Startup-RAM** value meets the minimum memory requirements of the operating system during the install or upgrade procedure.

For more information about Microsoft hypervisor memory overview, see http://technet.microsoft.com/en-us/library/hh831766.aspx link.

Comments on this document? infodev@avaya.com

Appendix A: AES administration

This appendix provides configuration and administration information for Avaya Application Enablement Services (AES) supported by the Avaya CM Telephony Server (TS) in IC 7.3.x.

This section includes the following topics:

- Avaya Aura® Application Enablement Services administration on page 340
- Avaya Aura® Application Enablement Services - CVLAN client Client installation on page 341
- Telephony Server support with AES GRHA on page 342

Avaya Aura® Application Enablement Services administration

This section describes how to configure Avaya Aura® Application Enablement Services for use with the IC Telephony Server. Refer to the appropriate AES documentation for more details on administering the AES with an Avaya switch to accommodate the goals of this section.

AES Configuration for IC 7.3.x

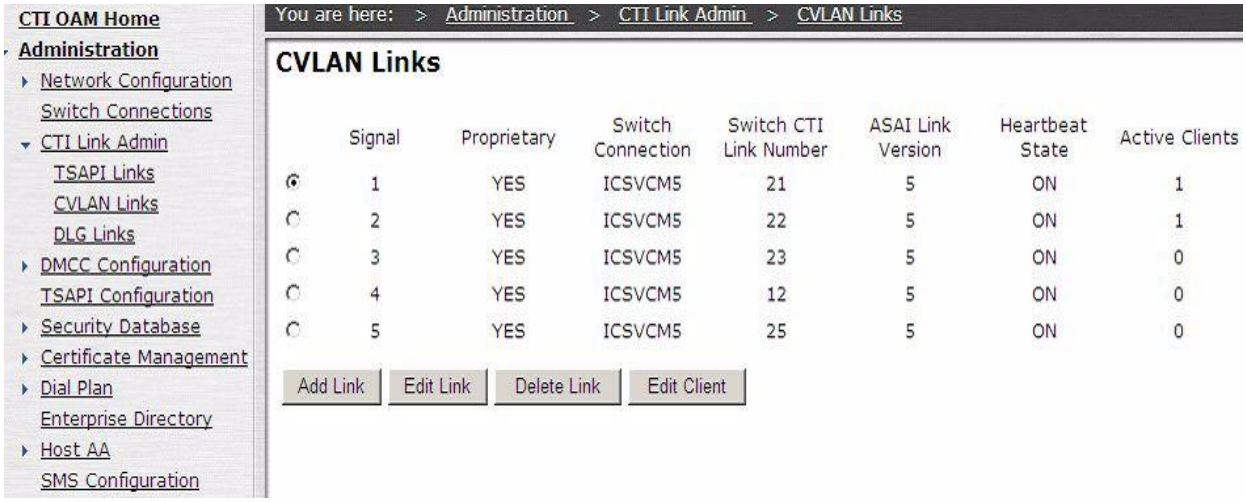
The Avaya AES must be configured with a license file that activates the ASAI Link Manager, CVLAN Service and Transport Layer Service.

CVLAN links must be configured with CTI link of Avaya Aura® Communication Manager and AES signal's ASAI Link Version should be set and active. For Avaya Aura® Communication Manager 8.0 support for 16 digit numbers, if the system uses 16 digital dial plan, then the ASAI Link version must be set to 8.

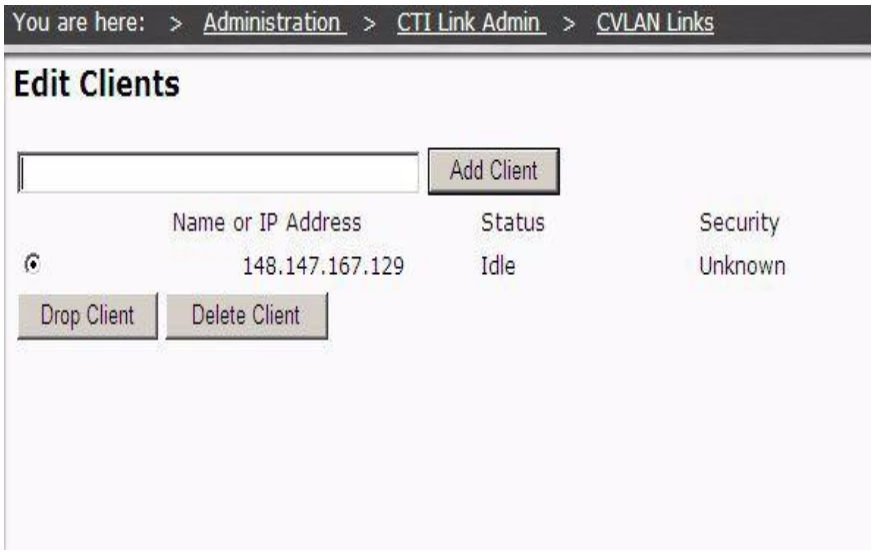
AES client must be added with CVLAN signal on AES.

To add an AES client:

1. Login to AES using **https://<ipaddress>/MVAP/index.jsp**
2. Go to the **CTI OAM Administration > Administration > CTI Link Admin > CVLAN Links**.



3. Click **Add Link t**o add a CVLAN Link.



4. Select the Switch CTI Link Number created by Communication Manager. For more information, see Defining link numbers (on 1.1 or later) on page 347.
5. On the **CVLAN Links** page, select the Signal (link) that you want to administer and click **Edit Client**.
6. In the **Add Client** field, type the <IP Address> or the <Host Name> of the CVLAN client, and click **Add Client**. Repeat this step for each client that you want to add.

Avaya Aura® Application Enablement Services - CVLAN client Client installation

Download the supported version of the Avaya Aura® Application Enablement Services - CVLAN Client from Avaya support web site. For details, refer to the compatibility matrix AES / Avaya Aura® Application Enablement Services - CVLAN client on page 233

To download the current version of the Avaya Aura® Application Enablement Services - CVLAN client:

1. Navigate to the Avaya Support website at http://www.avaya.com/support/
2. Under Resource Library, click the **Downloads** link.
3. Under DOWNLOAD BY PRODUCT NAME, click the **Avaya Aura® Application Enablement Services** link.
4. Select the supported version of CVLAN / AES Client from the drop-down list.

5. Follow the instructions provided on the Web page, and select the appropriate CVLAN / AES Client for your environment.
6. Download and Install the CVLAN / AES Client version on an Avaya CM TS server.

   Refer to the appropriate AES documentation for information on installing the AES Client.

Telephony Server support with AES GRHA

AIC 7.3.4 TS is supported with AES Geo Redundant High Availability (GRHA) option from AES release 7.0. GRHA option allows active and standby AE Services servers to be located in two different datacenters. GRHA allows two AE Services Virtual Machines (VMs) to be placed in two datacenters that are separated by a LAN/WAN with round trip time within 100 milliseconds. To ensure AE Services server does not failover due to hardware failure.

AES GRHA is not a state preserving HA. When a controlled failover occurs, AE Services are stopped on the current active VM and AE Services are started on the new active VM (previously the standby VM). In case of an uncontrolled failover, AE Services are started on new active (previously standby) VM. Depending on the reason for the uncontrolled failover, the previous active VM could be in an isolated network or it could be in the shutdown state.

- During the period when AES GRHA failover occurs, the AIC TS does not route any calls, voice agent login requests, and VDN registration requests. All the ongoing calls with AIC agent are connected from the stations and all the AIC agents are logged out from the voice channel.
- When the AE Services are started on the new active virtual machine (which was previously the standby virtual machine), the AIC agent must disconnect/wrap old ongoing voice calls first from station and then re-login to the voice channel using the retry option.

Note:

When the AES standby virtual machine becomes an active virtual machine, it takes three to five minutes for the AIC TS to become fully operational.

Advantages of AES GRHA

- Protects against datacenter failures.
- Protects against network failures (if configured).
- Only one set of AE Services licenses is needed for both AE Services servers (active and standby).
- Allows the AE Services VM in each datacenter to be in different networks or subnets.

Appendix B: Switch administration

This appendix provides configuration and administration information for each of the switches supported by the Avaya Telephony server (TS) in Avaya IC 7.3.x.

This section includes the following topics:

- Avaya Aura® Communication Manager administration on page 343

Important:
You must configure the switch to provide an ANI, to display the calling party's number on the Softphone when an agent receives a call. If there is no ANI, the Softphone displays the agent ID.

Avaya Aura® Communication Manager administration

This section describes how to configure the Avaya Aura® Communication Manager for use with the Avaya TS. Refer to the appropriate Avaya Aura® Communication Manager documentation for more details on administering the switch to accommodate the goals of this section.

Avaya IC supports the Redirect on No Answer (RONA) switch feature that redirects calls that are not answered by an agent. The agent must be configured on the switch for RONA. Refer to the administration documentation for your switch for RONA configuration instructions.

Important:
The Avaya Aura® Communication Manager switch sends the default reason code value 0 when it puts an agent on AUX work when a switch generated RONA occurs. This precludes the Avaya Agent from issuing a TS.BusyWithReason because the agent has already been placed into AUX work by the switch.

This section contains:

- Configuration for IC 7.3.x on page 344
- Best Services Routing (BSR) option on page 344
- Timed ACW on page 345
- Call vectoring adjunct routing request on page 345
- Configuring AES server software on page 353
- Configuring redundant CTI links on page 353
- Configuring the switch in an ACD environment on page 355

- Suppressing logout event when CMS moves agents across skills on page 355
- Service Observing on page 356
- Call Coverage on page 357
- Universal Call ID on page 359

Configuration for IC 7.3.x

You must configure the Avaya Aura® Communication Manager with a license file that activates the following Call Center Deluxe features.

- Call Vectoring (Basic).
- Call Vectoring (Prompting).
- Call Center Elite package (provides Expert Agent Selection “skills”, and Reason Codes).
- Computer Telephony Adjunct Links.
- Agent States.

The Co-Res Communication Manager LAN Gateway is required for the Avaya Media Servers. IC can interface with Communication Manager using a C-LAN board and a separate server running AEServices. The ASAI links must be configured either as ADJLK or ADJ-IP (for co-resident DLG or C-LAN connectivity). The ASAI links must also have IC Adjunct Routing active (with Communication Manager configured on the CTI Link form) to support multiple announcement/wait/loop back goto commands following the adjunct routing command.

Important:
When the switch administrator makes a change to be sent to an agent’s station on the switch while that agent is being monitored by the TS, the TS receives a C_PROV_ABT packet with a cause value of 19. When the TS receives this event, it assumes the CTI Link is down and the TS shuts itself down.

Do not make changes that cause a C_PROV_ABT packet with a cause value of 19 to an agent’s station on the switch while the agent is being monitored by the TS.

Best Services Routing (BSR) option

If you are using the Best Services Routing (BSR) option on your Avaya Aura® Communication Manager switch to transfer IC related calls, you must ensure that you have ISDN trunk lines configured between each switch and that you are passing UUI (User to User Information) on the D Channel to the remote switch. Avaya IC uses the UUI field to send and receive the EDUID of the call at each endpoint.

See the *Telephony Connectors Programmer Guide* for more information.

Timed ACW

Timed After Call Work (TimedACW) is a switch based feature supported by the Avaya Agent on the Avaya Aura® Communication Manager switch. With TimedACW, when an ACD call or queue is disconnected, the agent is placed into Wrapup (After Call Work) for a pre-defined period of time, which is configured on the switch. Once this period of time elapses, the agent is made available to receive the next call. TimedACW requires agents to use Auto-In functionality, not Manual-In.

Limitations

The following table lists the limitations to Timed ACW support:

Not supported with...	Not supported when...	Call types are...
Avaya Agent Wrapup	PBX TimedACW set to FALSE on the switch.	Outbound calls.
Selective Wrapup (customized by Avaya Professional Services)	Client TimedACW set to N in the VTel.ini file.	Direct calls dialed by equipment.
VTel standalone	Client Wrapup property in IC Manager set to TRUE.	Calls that are added in a conference or transferred.
Agent events turned off at the switch	-	Calls that are received by an agent that were previously RONA'd.
-	-	RONA or RONA'd calls.
-	-	Abandoned calls.

Call vectoring adjunct routing request

Adjunct routing is the process by which an ACD informs the Avaya TS that a call has arrived and the Avaya TS informs the ACD that the call should be routed to a particular destination.

There are several steps involved in adjunct routing, as outlined below. Each step is explained in the following sections.

1. Incoming call is identified by Dialed Number Identification Service (DNIS).

2. DNIS is mapped to a Vector Directory Number (VDN).
3. VDN identifies the vector to be executed.
4. Vector identifies the ASAI link to which the call is to be routed using an adjunct routing vector command.
5. Vector executes an adjunct route request on the ASAI link and waits for a return.
6. Avaya TS responds with a route select.

The following sections trace a call from its arrival at the switch to its eventual transfer to an agent.

Note:

The interaction of the Avaya TS and the Avaya Aura® Communication Manager can be affected by many switch parameter settings that are not described in this chapter. For example, when configuring the switch for outbound dialing, you may have to set the “Answer Supervision by Call Class” parameter to Y. Refer to your Avaya Aura® Communication Manager documentation for a complete description of switch parameters.

Defining Vector Directory Numbers (VDNs)

When a call arrives at the switch, the Dialed Number Identification Service (DNIS) is mapped to a Vector Directory Number (VDN).

The VDN table associates each VDN with a vector (script) to be executed when a call arrives on that VDN. The following example illustrates a VDN table. In this example, a call arriving on VDN 26001 would cause Vector 1 to be executed.

```
Allow VDN                Vec       Orig     Event     Skills
Ext Name                 Override  COR TN   Num Meas  Annc   Notif Adj   1st

26001 route to ASAI      n         1   1    1    none
26002 Route to LAN       n         1   1    2    none
26003 Rt LAN thn ASAI    n         1   1    3    none
```

Defining vectors

Vectors are scripts that contain a series of steps to be executed when the vector is run.

The following illustrates the definition of vector 1 (which, following the previous example, is the vector executed when a call arrives on VDN 26001). In this example, vector 1 causes calls to be adjunct routed to a link defined by extension 24961.

For information on defining link numbers on Avaya Aura® Communication Manager on release 1.1 or later, refer to Defining link numbers (on 1.1 or later) on page 347.

Avaya Aura® Communication Manager executes step 02, and then pauses as specified below in step 3 until one of the following occurs:

- Avaya TS requests a route (response to route request). The Avaya Aura® Communication Manager would then leave the vector and make the route to an available agent or wait treatment VDN.
- More than 10 seconds pass. The Avaya Aura® Communication Manager would then execute the next command in the vector, in this case, routing to the failover VDN defined by extension 24183.
- If the ASAI link is not operational, the Avaya Aura® Communication Manager automatically proceeds to step 4 in the vector without waiting the 10 seconds.

```
CALL VECTOR

    Number: 1               Name VECTOR 1
Multimedia? n
     Basic? y    EAS? y    G3V4 Enhanced? n    ANI/II-Digits? y    ASAI
Routing? y
 Prompting? y    LAI? y   G3V4 Adv Route? n    CINFO? n    BSR? y   Holidays? y

01 wait-time 0 secs hearing ringback
02 adjunct     routing link 24961
03 wait-time 10 secs hearing ringback
04 route-to number 24183 with cov n if unconditionally
```

Step 01 starts ringback and introduces a slight delay to prevent timing issues.

Blind transfer

When an agent initiates a blind transfer to the queue of a second agent, the call is connected to the second agent but it is not disconnected from the first agent. The call goes into the Hold state.

This happens because the call was moved from the VDN before the call merge could be completed. When the call is moved from the VDN and when the call merge takes place are operations controlled by the switch.

To correct this problem, you need to allow for enough time for the call merge to be completed before starting the adjunct route. To accomplish this, set a "wait-time 1 sec" step at the start of the vector.

Defining link numbers (on 1.1 or later)

This section describes how to define link numbers on a release version of Avaya Aura® Communication Manager of 1.1 or later.

A new CTI link form was added on Avaya Aura® Communication Manager 1.1 to define ASAI links. This new CTI link form replaces use of the "add station" form for assignment of station extensions to define ASAI links. This new form captures the same information that was administered on the station form for ASAI with the exception that a port number is no longer needed for a co-resident DLG link, an ADJ-IP link, or an ASAI-IP link. The port number is still required for a traditional ASAI link. When adding a link using this new form, a CTI link number is assigned. It is also necessary to enter an extension for the new link on the form.

The extension on the CTI link form is a station extension. An extension is still required because the switch architecture is based on extensions. Therefore, station extensions are used throughout the code for the internal ASAI implementation. However, externally on the SAT screens, ASAI links are referenced by their CTI link numbers. The CTI link number (between 1 and 16) is now used, instead of the ASAI extension, in the "adjunct routing link" vector step to define the link. Upgrades from an earlier release automatically add the new CTI link form and move the existing ASAI link assignments to the CTI Link form and the station extension numbers are converted to link numbers in all references to ASAI links in existing vectors.

Each ASAI link for use with IC is defined using two pages. The following screens illustrate page 1 for different links.

For earlier Communication Manager CSI/SI/R and the S8700 Media Servers (link type ADJLK):

```
add cti-link next                                                Page   1 of 2
LINK
   CTI Link: 01
   Extension: 40001                                               BCC: 0
        Type: ADJLK                                                TN: 1
        Port: 1C0501                                              COR: 1
        Name: ADJLK CTI Link 1                                    COS: 1
                                          Hunt-to Station

   STATION OPTIONS
                Loss Group: 3


   BRI OPTIONS
                XID? y     Fixed TEI? n
         MIM Support? n
                          CRV Length: 2
```

For S8100 or S8300 Media Servers

```
add cti-link next                                                Page   1 of 2
LINK
   CTI Link: 01
   Extension: 40001                                               BCC: 0
        Type: AD-IP                                                TN: 1
                                                                  COR: 1
        Name: ADJLK CTI Link 1                                    COS: 1
                                          Hunt-to Station

   STATION OPTIONS
                Loss Group: 3
```

The following is assigned to page 2 for all types of links:

```
add cti-link next                                                Page   2 of 2
LINK
   FEATURE OPTIONS

        Event Minimization? n


                                  Special Character for Restricted Number? N
```

For Communication Manager 5.x (link type ADJ-IP):

```
add cti-link next                                                Page   1 of 2
                                CTI LINK
   CTI Link: 4
   Extension: 77004
        Type: ADJ-IP
                                                                  COR: 1
        Name: CM100 (7.0 CI Windows)




--- ADJLK link, p. 1 ---

add cti-link next                                                Page   1 of 2
                                CTI LINK
   CTI Link: 5
   Extension: 77005
        Type: ADJLK
        Port: 1C1105                                              COR: 1
        Name: CM101 (7.0 CI Windows)

   BRI OPTIONS
                XID? n      Fixed TEI? y      TEI: 3
         MIM Support? n
                         CRV Length: 2

--- ADJLK, ADJ-IP link, p. 2 ---
```

The following is assigned to page 2 for all types of links:

```
add cti-link next                                                Page   2 of 2
                                CTI LINK
   FEATURE OPTIONS

        Event Minimization? n      Special Character for Restricted Number? N
        IC Adjunct Routing? y      Send Disconnect Event for Bridged Appearance? n
                                  Two-Digit Aux Work Reason Codes? y
                                  Block CMS Move Agent Events n
```

The following tables illustrate the valid link numbers for the various Avaya Aura® Communication Manager switch configurations:

Switch Configuration	Valid Link Numbers
Avaya Aura® Communication Manager R, S8700, and S8300	1 to 16

Involvement of the telephony server

Continuing with the above example:

1. The Avaya TS is notified of a new call arrival and requests that an EDU be created by the EDU server.
2. The Avaya TS passes the call to the Workflow server to determine the call's final destination.
3. The Workflow server requests the Avaya TS (TS.Route) to route the call to a station or queue.
4. When the Avaya TS gets the request, it sends the commands to the Avaya Aura® Communication Manager over the ASAI link to route the call.

Defining hunt and skill groups

The Avaya Aura® Communication Manager supports two environments for defining agents and assigning them to queues: EAS (Expert Agent Selection) and non-EAS.

Both non-EAS and EAS have agents defined in hunt groups and the AAS parameter should be set to N (for no). The AAS setting is only used for IVR ports, not live agents.

With non-EAS, the hunt group is defined as an ACD split. In this case each agent is pre-assigned (when administered) to the hunt group (split) to which the agent is a member. If an agent is to be a member of more than one split, the agent needs a separate set of work buttons for each of the splits because the agent must log into each split individually.

With EAS, the hunt group is defined as a skill and the agent becomes a member of the skill when they log in, not when they are administered. Each EAS agent has a LoginID form assigned, which lists the skills they become members of when they log in. An agent only needs one set of work buttons because once the agent logs in, the system automatically makes them a member of all their assigned skills (hunt groups). The agent LoginID form also has an AAS field (for use as an IVR port), which also should be set to N (for no) for live agents.

In both an EAS and non-EAS environment, agents are defined in hunt groups. When agents log in, they must identify the queue with which they are associated. The agents are not affiliated with a specific skill. The Auto Available Split (AAS) parameter in the Hunt Group must be set to N, for no.

EAS agents are associated with skill groups. If a caller must speak with an agent that has a specific skill, such as understanding a foreign language or having knowledge of a specific procedure, the caller is routed to a queue associated with the required skill. The next available agent with the appropriate skill takes the call and IC Telephony is notified that the call was transferred to an agent.

Depending on your environment, you must identify agents by either skill groups or hunt groups.

```
Grp  Grp          Grp  ACD/              Que   No.  Cov   Notif/   Dom   Message
No.  Ext.  Name   Typ  MEAS  Vec  MCH    Size  Mem  Path  Ctg Adj  Ctrl  Center

1    24301 Skill   1  ucd   y/N  SK     none   5     0       n             n

2    24302 Skill   2  ucd   y/N  SK     none   5     0       n             n

16   24316 Skill  16  ucd   y/N  SK     none   5     0       n             n

17   24317 Skill  17  ucd   y/N  SK     none   5     0       n             n
```

Summary of adjunct routing requirements

The following summarizes the items that must be configured for adjunct routing to take place. Refer to Configuration for IC 7.3.x on page 344 for more details.

1. Stations - phones connected and configured, ASAI Link or ASAI LAN gateway configured to a station extension. For MultiVantage 1.1 or later, a specific link number between 1 and 16.
2. Network DNIS mapped to a VDN on the switch.
3. VDN assigned to a vector number.
4. Vector script performing adjunct route to the ASAI ink extension or link number.
5. Agent logins defined with associated skills.
6. Skill queues (hunt groups) defined to route calls from Avaya Computer Telephony.
7. In the definition of the ASAI link, event minimization must be set to N.
8. To allow calls to be sent to an “agentid”, the “Direct Agent Calling” parameter of the “Class of Restriction” for both the sending and receiving parties, that is the Agent ID and the incoming VDN, must be set to “Y”. If not set to “Y” the call could be delivered to the agent as a personal call rather than an ACD call.

Note:

An agent's profile can be set to either Auto In mode or Manual In mode. This setting affects VTel’s ability to control the agent's availability. Refer to the *VTel Programmer’s Guide* for additional information on this setting.

Configuring AES server software

You must configure the AES server software to enable Avaya IC 7.3.x special features over the adjunct link. Before you begin, ensure the link you intend to use is set as Adjunct Links on both the switch and on AES.

- Check the station type for each of the clients assigned to the switch. The station type must be set to ADJLK.
- Contact your switch administrator to determine if your AES is configured as Adjunct. If your AES is configured for ASAI only, contact Avaya Technical Support for assistance.

Note:

The **Copy ASAI UUI During Conference/Transfer** parameter must be set to **Yes** in the system-parameters.

Once you determine the station types are set to ADJLK, you can configure AES. For information on administering AES, see *Application Enablement Services Administration and Maintenance* guide.

Configuring redundant CTI links

Installing two or more Avaya telephony servers allows failover in the event of a malfunction of the server or ISDN line.

There are two approaches available for configuring redundant ASAI links:

- Configure each link to connect with a different physical computer, each with its own Avaya TS.
- Configure each link to connect with a single computer running multiple Avaya TS processes on that computer. You must set the “Signal Number” configuration parameter to specify signal numbers for the ASAI links.

Avaya Aura® Communication Manager setup

Regardless of whether the primary and backup Avaya TSes are installed on either the same or different hardware, two separate VDNs and vectors are required in the Avaya Aura® Communication Manager, one for each Avaya TS. The division of work between ASAI links, and thus servers, is determined by the number of calls that are processed by each vector.

The following figure illustrates vectors that are configured to fail over to alternate ASAI links and finally, if both links fail, to a default routing. If either Avaya TS is disabled or the ISDN connection is broken, subsequent calls to the corresponding vector are immediately channeled through the alternate ASAI link to the working Avaya TS. When the Avaya TS is re-enabled or the ISDN connection is restored subsequent calls to that vector are processed via their usual path with no operator intervention.

```
display vector 7
Page   1 of 2
CALL VECTOR

    Number: 7              Name Troy Link 1
Multimedia? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? n  G3V4 Adv Route? y   CINFO? n   BSR? y  Holidays? y

01 wait-time  0 secs hearing ringback
02 adjunct    routing link extension 5100
03 wait-time  4 secs hearing ringback
04 adjunct    routing link extension 5113
05 wait-time  4 secs hearing ringback
06 route-to number 4000 if unconditionally

display vector 13
Page   1 of 2
CALL VECTOR

    Number: 13              Name Troy Link 2
Multimedia? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? n   BSR? y  Holidays? y

01 wait-time  0 secs hearing ringback
02 adjunct    routing link extension 5113
03 wait-time  4 secs hearing ringback
04 adjunct    routing link extension 5100
05 wait-time  4 secs hearing ringback
06 route-to number 4000 if unconditionally
```

The wait time in steps 03 and 05 of the sample vectors should be configured to allow adequate time for the adjunct route to process normally when the link is functioning properly. If the link fails because the physical link, the Avaya TS or the Workflow server fails, the vector skips the “wait” and immediately execute the next step in the vector. The time-out occurs only if the link, Avaya TS and the Workflow server are up and assigned, but network traffic or database access is so slow that the route does not reach the switch in time.

Configuring the switch in an ACD environment

When configuring the switch for non-EAS agents, certain parameters must be set. Note that the default setting of these parameters, and even whether or not they are displayed, varies depending on whether the switch was ever set up for EAS use.

The following notes are specific to the menus displayed by the Avaya Aura® Communication Manager G3V6 or higher. The wording and location of these parameters may vary slightly for other versions.

1. Log on to the **Avaya Aura® Communication Manager** console using an account with appropriate security, such as the unit account.
2. Enter the **Change System Customer Options** command.
3. On page 6 of the menu, set the BCMS/VuStats service level to Y and the EAS parameter must be set to Y. Note that, in some circumstances, the BCMS parameter can be set to Y. The switch displays a message indicating if it must be changed.
4. Log off for the changes to take effect.
5. Log on again (using the init account is optional for the following command).
6. Enter the **Change System Parameter Features** command.
7. On page 11 of the menu, the **EAS Enabled** parameter must be set to **Y**.
8. On page 14 of the menu, set **Auxwork Reason Code** to forced and **Logout Reason Code** to requested.

When defining hunt groups, note that the Auto Available Split (AAS) parameter must be set to “N” and the skill for the hunt group (if this option is displayed) must also be set to “N”. Agent phone extensions must be included in the hunt group as group members.

Suppressing logout event when CMS moves agents across skills

Until IC 7.3.3, TS supported a configuration suppress_logout_event. If turned on, it would suppress the C_logout event it receives from the CM and would not sent a TS.Logout.event to its clients. By default the suppress_logout_event parameter was turned off.

This configuration was a temporary arrangement to overcome a bug on the CM, when agents are moved across skills.

This configuration has been removed from IC 7.3.4 and the CM parameter to suppress the event has to be enabled.

To enable Block CMS Move Agent Events on CM:

1. Log on to the **Avaya Aura® Communication Manager** console using an account with appropriate security, such as the unit account.

2. Type `change cti-link 1` and press Enter. Here, `cti-link 1` corresponds to the link the telephony server is configured.
3. Go to page 2.
4. Set **Block CMS Move Agent Events** must be set to **y**.

Note:
You must busyout and release the CTI link before and after changing the Block CMS Move Agent Events value. Perform this procedure on all the CTI links that are using in IC's telephony server.

Service Observing

Service Observing is an Avaya Aura® Communication Manager feature that allows a specified user on Avaya IC, such as a customer service supervisor or a calling group supervisor, to observe the calls of another user (an agent) on Avaya IC. This gives the contact center the capability to ensure their customers are receiving quality service from their agents. Service Observing allows an observer with a hardphone to listen to calls at extensions within a Service Observing group. Observing means that the service observer can only listen and cannot be heard by either party on the call.

Important:
Avaya IC supports Service Observing activation through the hardphone only. The service observer must use a hardphone to observe the call of another user on Avaya IC.

The following scenario illustrates service observing on Avaya IC:

1. A call comes into the agent triggering a TS.IncomingCall and a TS.Connect event.
2. The recording application that is monitoring the station is notified about the service observing audio connection to this call with the TS.ObserverConnect event.
3. When the agent puts the call on hold, a TS.Hold event is triggered for the agent and a TS.ObserverDropped event is generated to the recording application, indicating that the audio connection is no longer active.
4. When the agent reconnects a held call, a TS.HoldReconnect event is triggered for the agent and a TS.ObserverConnect event is generated on the recording application, indicating that the audio connection is again active.
5. When the agent ends a call, a TS.ObserverDropped event is triggered for the agent and a TS.Disconnect is sent to the client application.

Call Coverage

Call Coverage provides automatic redirection of calls to a designated destination (VDN or extension number) in a Call Coverage path. Call Coverage enables you to:

- Establish coverage paths with multiple answering options.
- Establish redirection criteria that govern when a call redirects.
- Redirect calls to a local switch station.

In Avaya IC 7.3.x, the following Call Coverage functions are supported on the Avaya Aura® Communication Manager switch:

- Coverage Path
- Call Forward All Calls (Call Forward/All)
- Call Forward Busy/Don’t Answer (Call Forward Busy/DA)

The Avaya Aura® Communication Manager switch can be configured to leave a Bridged Call Appearance for the call following the Coverage Path or Call Forward. This option is not supported by Avaya IC because the Avaya TS does not support Bridged Call Appearance.

Important:
Call Coverage functionality is not supported on IC systems using Avaya Business Advocate. A conflict would exist because Advocate must control where the calls are routed and Call Coverage allows the switch to make call routing decisions.

Coverage Path

Coverage Path is a list of alternate answering options that are accessed, in sequence, when the dialed agent is not available to answer the call. Switch system administrators can configure Coverage Paths in one of the following ways:

- On stations (hardphones)
- By ACD Agent IDs (agent IDs)

The Coverage Path setup cannot be modified by agents. The switch routes the call based on the configuration set for the Dialed Number (DN).

For example:

- If the hardphone extension number is dialed, the call follows the "station" call coverage information.
- If the dialed number is the agent ID (in an EAS environment), the call follows the "agent ID" call coverage information.

If the agent does not have a Coverage Path configured, direct agent calls are queued to the agent on the agent's primary queue with a higher priority than any other call.

Note:
If Coverage Path is routed to a VDN by the Workflow server, additional routing hints should be defined on the queue that is used to route the call.

Call Forwarding

Call Forwarding allows agents to specify a destination to redirect calls when they are not available to take calls. These destinations can be either a VDN or an extension number. Call forwarding is set up by the agent before logging into Avaya IC.

Avaya IC 7.3.x supports the following Call Forwarding functions:

- Call Forward All Calls (Call Forward/All) - Limited support.
- Call Forward Busy/Don't Answer (Call Forward Busy/DA) - Limited support.

With either of these Call Forwarding functions, the TS does not receive information from the switch until the call is answered and the agent does not see the Softphone ring.

Before logging into Avaya Agent, the agent must manually perform call forwarding on the hardphone to initiate call forwarding functionality for the session.

Call Forward All

Only hardphones can forward calls with the Call Forward/All (CFA) function. If an agent logs into a hardphone with Call Forward/All activated, calls made to that hardphone are automatically forwarded to the designated destination. The agent is not notified about these calls.

Calls made to the agent ID either:

- follow the agent configuration if the agent's Class of Restriction (COR) allows Direct Agent Calls (DAC).
- or are forwarded to the designated destination if the agent's COR does not allow DAC.

Limitation:

Calls made to the agent through the queue are delivered to the agent as usual.

Call Forward Busy/DA

Only hardphones can set the Call Forward Busy/DA (CFN B/A) function. The hardphone must be authorized to allow Call Forward Busy/DA in its Class of Service (COS) before it can be set up for Call Forward Busy/DA.

The following scenario illustrates a call to a hardphone with Call Forward Busy/DA:

1. The phone rings a number of times, based on the configuration setting in System-Parameters Coverage-Forwarding.
2. The call is re-routed to the designated call forward destination.

3. When the calls rings on the hardphone, the TS is not notified by the switch that the hardphone is ringing and one of the following occurs:
   a. If the call is not answered, the TS is unaware the call was ever there, so the Report server and OA do not report this step of the call.
   b. If the call is answered, the TS tries to "catch up" and send the appropriate alerting and connecting events to the client assigned to the hardphone.

Calls made to the agent ID follow the same rules as Call Forward All.

Calls that are made to the agent ID that are not allowed to receive DAC are forwarded to the call forwarding destination without ringing.

Universal Call ID

The Universal Call ID (UCID) is a unique 8-byte binary tag assigned by Communication Manager ECS MultiVantage to each call upon call origination or upon entry into Communication Manager, if the call is not already associated with a UCID. UCID allows tracking of calls from cradle to grave within a private network of Communication Manager systems when they are connected via ISDN trunks.

Products such as Call Management System (CMS), Avaya IVR, and CentreVu Computer Telephony support UCID. For more information on using UCID in custom applications, please refer to *CallVisor ASAI Protocol Reference.*

Index

Symbols

.NET libraries 28

A

Active Directory mode
about 248
implementing 249
adapting
adding servers 80
co-locating servers 81
deployment scenarios 79
multi-processor machines 81
servers and domains 80
Adjunct Route Capacity 293
adjunct routing requirements, summarized 352
ADU persistence 56
ADU server 55, 63
Advanced Reporting Tools
see Operational Analyst
Advocate
see Business Advocate
AES 28
agent desktop applications
about 24
Avaya Agent 24
browsers 307
operating systems 307
prerequisites 307
agents, remote 40
AIX
browser 275
configuration requirements 271, 276
configuration settings 276
disk space requirements 275
IBM HTTP Server 238
installation user 277
locales 275
physical address 201
root user 277

Server SDK compiler 314
support 274
time synchronization 54
user accounts 277
verifying DNS resolution 261
Visual Age compiler 314
web server 238
windowing environment 276
AJP 1.3 connector 241
Alarm server
guidelines 56
APP_CTL_HEAP_SZ 227
APPLHEAPSZ 227
applications, time zones 49
asynchronous communication, AES 28
Attribute server 61
Avaya Agent
about 24
Citrix 279
Citrix interfaces 281
desktop 24
hardware requirements 196
Internet Explorer 269
internet options 269
Web Scheduled Callback 66
Avaya Agent Web Client
about 24
agent configuration guidelines 179
deployment guidelines 178
deployment scenarios 177
hardware requirements 197
Internet Explorer 269
internet options 269
NAT 45
pop-up blockers 269
proxy server settings 269
required software 309
Web Scheduled Callback 66
Avaya Communication Manager
configuring redundant CTI links 353
configuring the switch in an ACD environment 355
switch configuration 343
switch setup 354
Avaya Computer Telephony 25
Avaya IC for Siebel
required software 305
Avaya OA
see Operational Analyst
Avaya switches, prerequisites 293

B

bandwidth, remote agents 41
binary sort order 214
browsers

agent desktop applications 307
AIX 275
Design & Administration Tools 306
Internet Explorer 267
Solaris 271
bufferpool, DB2 227
Business Advocate
about 26
Active Directory mode 248
configuring SQL Server for Thai 254
configuring Windows for Thai 250
data center 170
databases 46, 64
deployment
high volume voice 92
multi-channel 112
multi-site 145, 152, 170
voice only 88
Event Collector server 74
Logical Resource Manager 63
multi-instance 152
Oracle
client 257
components 255
tablespaces 255
user 256
prerequisites 301, 305
requirements 301, 305
Resource Manager server 64
resource store 47
servers 63, 300
setting up Active Directory 249
setting up MSMQ 248
setting up Workgroup mode 248
single instance 145
supported exceptions 247
system store 46
TSA server 64
user 253
WAA server 65
Workflow server 59
Workgroup mode 248

C

C for AIX compiler 314
calendar, Web Scheduled Callback 66
cataloguing DB2 client 228
CCQ database 46
changing
adding servers 80
co-locating servers 81
deployment scenarios 79
multi-processor machines 81
servers and domains 80
channels
email 26
telephony 25
web 25
chat
co-locating servers 81
DUStore server 61
server guidelines 61
single site 117
Checkpoint 57
CIRS server 62
Citrix
Avaya Agent 279
clients 279
deployment 278
Design & Administration Tools 279
exceptions 280
integration limitations 283
interfaces
about 281
Web 281
licensing 281
limitations 21
multiple applications 279
support 278
Website 279
client applications 53
Client SDK
about 27
configuring Tomcat 240
default web application context 240
failover 241
features 28
Jakarta Tomcat Connector 241
load balancing 241
Tomcat installation 240
Web Scheduled Callback 66
Client to connection ratio 48
co-locating servers 81
Communication Manager
CVLAN client 234
prerequisites 293
requirements 233
Service Observing 356
compiler
AIX 314
Server SDK 314
components
about 22
agent desktop applications 24
Avaya Agent 24
Business Advocate 26
Client SDK 27
Computer Telephony for IC 25
Content Analyzer 27

core servers 22
Database Designer 24
deployment on Citrix 278
Design & Administration Tools 23
Email Management 26
IC Manager 23
optional databases 289
Oracle, Business Advocate 255
performance 36
required databases 289
Telephony 25
time zones 49
Web Management 25
Workflow Designer 23
Computer Telephony 25
configuration parameters
IBM HTTP server 239
Oracle iPlanet Web Server 237
configuration parameters, DB2 227
configuration, network 259
configuring
binary sort order 214
database machine 46
DB2 226
network 38
POP3 servers 244
SMTP servers 244
configuring SQL Server for Thai 254
configuring Windows for Thai 250
connections
network 39
VPN 40
contacts, volume 37
Content Analyzer
about 27
prerequisites 298
required software 296
servers 297
supported languages 27
core servers 22, 287
Customer Interaction Repository 210
customization, workflows 58
CVLAN client 234

D

data center 160, 170
Data server 56
database tables 48
location 47
database clients, requirements 213
Database Designer
about 24
prerequisites 306
database machine 47
databases
about 46, 210
Business Advocate 46, 64
CCQ 46
client location 213
connection pool 48
DB2 client 226, 228
DB2 server 226
IC Repository 46
login requirements 211
machine 46
Operational Analyst historical 47
Operational Analyst real-time 47
optional 289
Oracle 220
Oracle client 221, 225
Oracle server 222
prerequisites 290
required 289
servers 46, 211
setting up 209
Siebel 47
SQL Server 214
date/time 49
DB2
bufferpool 227
cataloguing client 228
client 226, 228
configuration parameters 227
configuring 226
fix pack level 226
patches 226
registry variables 227
server 226
tablespace 228
DB2_INDEX_2BYTEVARLEN 227
DB2_RR_TO_RS 227
DB2_STRIPED_CONTAINERS 227
DB2COMM 227
DBMS 209
default gateway 260
deployment
adapting scenarios 79
adding servers 80
additional servers and domains 80
Business Advocate
high volume voice 92
multi-channel 112
multi-site 145, 152, 170
voice only 88
Citrix 278
co-locating servers 81
components 22, 36
concurrent users 37
Data server 56

database servers 47
Email Management 62
Event Collector server 76
examples 79, 123
multi-processor machines 81
multi-site
multi-channel 133
multi-channel data center 160
voice only 124
network
connections 39
firewall 44
multiple cards 43
remote agents 40
security 39
network configuration 38
performance factors 36
planning 35
server performance 190
servers 50
single site
chat and email 117
multi-channel 96, 104
voice only 82
Telephony 60
volume of contacts 37
Web Management 62
deployment scenarios
Avaya Agent Web Client 177
basic 180
clustered 182
multiple cell 187
Design & Administration Tools
about 23
browsers 306
Citrix 279
Database Designer 24
hardware requirements 193, 195
IC Manager 23
operating systems 306
other software 306
Workflow Designer 23
Directory server
guidelines 56
disk space
AIX 275
servers 192
Solaris 271
distribution, servers 191
DMZ 44
DNS
unresolved 262
verifying on AIX 261
verifying on Solaris 261
verifying on Windows 260
verifying resolution 259
documentation
Readme file 21
domain name system 259
domains
agent 55, 76
DNS 44
Event Collector server 73
logical partitioning 52
naming convention 53
DUStore server
chat 61
email 62
voice 61

E

EDU persistence 57
EDU server 56, 57
email
co-locating servers 81
Content Analyzer 27
DUStore server 62
EDU server 57
single site 117
Workflow server 59
Email Management
about 26
configuring firewall 245
deployment 62
email servers 243
POP3 servers 244
prerequisites 298
required software 296
server guidelines 62
servers 297
SMTP servers 244
Email server 62
enabling TCP/IP networking 259
encryption 28
ephemeral ports 67
Event Collector Bridge 75
Event Collector server 73
examples
Business Advocate
high volume voice 92
multi-channel 112
multi-site 145, 152, 170
voice only 88
deployment scenarios 79, 123
multi-site
multi-channel 133
multi-channel data center 160
voice 124
single site

Comments on this document? infodev@avaya.com

chat and email ... 117
multi-channel ... 96, 104
voice ... 82
exceptions
Business Advocate ... 247
Citrix ... 280
supported operating systems ... 286
experience ... 31

F

factors, performance ... 36
failover
ADU server ... 55
capacity ... 80
CTI ... 353
Event Collector server ... 76
Operational Analyst ... 76
Resource Manager server ... 64
servers ... 191
Tomcat ... 241
TSA server ... 65
failure, server guidelines ... 55
features, Client SDK ... 28
finding IP address ... 260
firewall ... 44
Client SDK ... 28
communication through ... 45
deployment outside ... 44
DNS domains ... 44
Email Management ... 245
NAT ... 45
FQDN ... 259
fully qualified domain name ... 259

G

guidelines
ADU server ... 55
AIX configuration ... 271, 276
AIX disk space ... 275
Alarm server ... 56
Attribute server ... 61
Avaya Agent Web Client ... 178, 179
Business Advocate databases ... 64
Business Advocate servers ... 63
Business Advocate workflows ... 66
chat channel servers ... 61
CIRS server ... 62
client applications ... 53
components ... 36
concurrent users ... 37
core servers ... 55
database files ... 48
database server ... 47
database tables ... 48
Directory server ... 56
DUStore server ... 61, 62
EDU server ... 56, 57
email channel servers ... 62
Email server ... 62
Event Collector Bridge ... 75
Event Collector server ... 73
firewall ... 44
ICM server ... 62
licensing ... 53
logical partitioning ... 52
Logical Resource Manager ... 63
machine speed ... 191
NAT ... 45
network
connections ... 39
multiple cards ... 43
remote agents ... 40
security ... 39
Notification server ... 57
Operational Analyst failover ... 76
Operational Analyst servers ... 72
ORB server ... 57
physical partitioning ... 52
Report server ... 58
Resource Manager server ... 64
server failure ... 55
server naming ... 51
server partitioning ... 52
servers ... 50
Solaris configuration ... 272
Solaris disk space ... 271
Telephony server ... 60
time synchronization ... 54
TSA server ... 64
TSQS server ... 60
voice channel servers ... 60
volume of contacts ... 37
WAA server ... 65
Web License Manager ... 53
Web Management servers ... 62
Web Scheduled Callback ... 50, 66
Workflow server ... 58

H

hardware ... 195
Avaya Agent ... 196
Avaya Agent Web Client ... 197
Design & Administration Tools ... 193, 195
machine speed ... 191
requirements ... 189
servers ... 191
Host ID

See physical address
host/local 49
Hosts file 262
http
//www.vmware.com 325
hunt groups, defining 351

I

IBM HTTP Server
about 238
configuration parameters 239
IBM Logical Partition technology 192
IC Manager
about 23
Citrix 279
multi-processor machines 81
prerequisites 306
time zones 49
IC Repository 46, 210
ICM server 62
icsdk 240
IIS
security patches 236
implementation roles 31
installation user 274, 277
installing
database servers 211
DB2 client 228
DB2 server 226
DB2 version 226
IIS security patches 236
Internet Explorer 267
license file 199
Oracle client 225
Oracle server 222
SQL Server 215, 216
Windows XP Professional service packs 266, 267
integrations, Client SDK 28
Interaction 280
interaction
ADU server 55
CIRS server 62
DUStore server 61, 62
EDU server 56, 57
ICM server 62
time synchronization 54
TSQS server 60
interfaces, Citrix 281
internationalization 28
Internet Explorer
about 267
configuring Oracle JVM 268
downloading 268
encoding 270
internet options 269
JVM plugin 268
Trusted Sites 269
Internet Information Server 235
IP address 260

J

Jakarta Tomcat Connector 241
Java 28
Java Virtual Machine
configuring 268
installing plugin 268

L

LAN 39
languages
limitations 20, 21
supported 20
languages, Content Analyzer 27
latency, remote agents 42
license file
obtaining 199
prerequisites 199
replacing 204
requesting 202
updating 203
licensing
Citrix 281
guidelines 53
limitations
ADU data collection 74
ADU server 55
Business Advocate databases 64
Citrix 21, 280
Citrix integration 283
EDU 57
Resource Manager server 64
Thai 21
Traditional Chinese 20
load balancing. Tomcat 241
local 49
Locale
AIX 275, 276
Solaris 272
localhost 262
location
Alarm server 56
Attribute server 61
client applications 53
core servers 55
Data server 47
database client 213
database files 48

Comments on this document? infodev@avaya.com

Directory server 56
Email server 62
Event Collector server 73
Notification server 57
ORB server 57
Report server. 58
Resource Manager server 64
servers 60, 61, 62
Telephony server 60
WAA server 65
Web License Manager 53
Web Management servers 62
Workflow server 58
log file allocations 192
logical partitioning 52
Logical Resource Manager
ADU server 63
guidelines 63
LPAR 192

M

machine speed 191
MAXAPPLS 227
MAXLOCKS 227
media
email 26
telephony 25
web 25
Message Queuing services
see MSMQ
Microsoft
Internet Explorer 267
SQL Server 214
Visual Studio 314
Windows 265
minimum hardware requirements 195
MSMQ
Active Directory 249
setting up 248
Workgroup mode 248
multi-channel
multi-site 133
multi-site data center 160
single site 96, 104
multi-instance, Business Advocate 152
multiple network cards 43
multi-processor machines 81
multi-site
Business Advocate
data center 170
multi-instance 152
single instance 145
deployment scenarios 123
multi-channel 133
multi-channel data center 160
voice 124

N

naming, domains 53
naming, servers 51
NAT 28, 45
NetWare 259
network 62
bandwidth for remote agents 41
configuration 38, 259
connections 39
data server location 56
firewall 44
multiple cards 43
multiple network cards 43
Novell Netware 259
security 39
VPN 40
network cards, multiple 43
network configuration, database machine 46
Network Interface Cards 43
networks
TCP/IP 259
topology 38
NICs 43
Notification server 57
Novell NetWare 259
nslookup 261
number, concurrent users 37

O

obtaining, license file 199
ODBC, database tables 48
operating systems
AIX 274
Citrix 278
exceptions 286
setting up 247, 263
Solaris 270
supported 247, 263
Windows 265
Operational Analyst
about 29
Event Collector 73
Event Collector Bridge 75
failover 76
historical database 47
real-time database 47
server guidelines 72
optional databases 289
Oracle
Business Advocate

client 257
components 255
tablespaces 255
user 256
client 221, 225
patches 221
server 222
setting up 220
Oracle iPlanet Web Server
configuration parameters 237
Oracle IPlanet Web Server 7.0.13 Web Server
download 237
Oracle Java System Web Server
setting up 237
Oracle JVM plugin
about 268
configuring Internet Explorer 268
ORB server
guidelines 57
overview 19

P

partitioning, servers 52
patches
DB2 226
Oracle 221
performance
components 36
dependencies 190
factors 36
volume of contacts 37
physical address, identifying 200
physical partitioning 52
physical redundancy 80
planning
components 36
concurrent users 37
deployment 35
experience 31
network
connections 39
firewall 44
multiple cards 43
remote agents 40
security 39
network configuration 38
performance factors 36
servers 50
volume of contacts 37
POP3 ..... 62, 243, 244
pop-up blockers, Avaya Agent Web Client 269
ports
ephemeral 67
prerequisites
about 285
agent desktop applications 307
Avaya IC for Siebel 305
Business Advocate 301, 305
Communication Manager 233
Content Analyzer 298
core servers 287
databases 290
Design & Administration Tools 306
Email Management 298
experience 31
license file 199
Telephony servers 292
Web Management 295
proxy server
Avaya Agent Web Client 269
Client SDK 28

R

RAM, database clients 213
RDBMS 49, 209
Readme file 21
registry variables, DB2 227
remote agents
bandwidth 41
latency 42
VPN 40
replacing, license file 204
Report server 58
requesting
license file 202
replacement license file 204
required databases 289
required experience 31
required hardware 195
required software
agent desktop applications 307
Avaya Agent Web Client 309
Avaya IC for Siebel 305
requirements
about 285
Avaya IC for Siebel 305
Content Analyzer 298
core servers 287
database clients 213
database login 211
databases 290
Design & Administration Tools 306
Email Management 298
hardware 189
Telephony 292
Web Management 295
Resource Manager server 64
resource store 47

roles, implementation 31
root user 273, 277

S

scalability 28
Scheduled Call, servers 294
security
  Client SDK 28
  databases 211
  firewall 44
  license file 199
  network 39
  patches, IIS 236
  server location 55
  server partitioning 52
  validation 192
Server SDK compiler
  AIX 314
  Solaris 314
  Windows 314
servers
  about 22
  ADU 55
  Alarm 56
  Attribute 61
  Business Advocate 300
    guidelines 63
    Logical Resource Manager 63
    Resource Manager 64
    TSA 64
    WAA 65
  chat channel 61
  CIRS 62
  Content Analyzer 297
  core 287
  core server guidelines 55
  database guidelines 47
  Directory 56
  distribution 191
  DUStore 61, 62
  EDU 56, 57
  Email 62, 243
  email channel 62
  Email Management 297
  failover 191
  failure 55
  guidelines 50
  hardware requirements 191
  ICM 62
  interaction
    ADU server 55
    CIRS server 62
    DUStore server 61, 62
    EDU server 56, 57
    ICM server 62
    TSQS server 60
  location 47, 60, 61, 62
    Alarm server 56
    Attribute server 61
    client applications 53
    Directory server 56
    Email server 62
    Notification server 57
    ORB server 57
    Report server 58
    Telephony server 60
    Web License Manager 53
    Web Management 62
    Workflow server 58
  machine speed 191
  Microsoft Internet Information 235
  naming 51
  Notification 57
  Operational Analyst 72
    Event Collector 73
    Event Collector Bridge 75
  ORB 57
  partitioning
    guidelines 52
    logical 52
    physical 52
  performance 190
  platform considerations 190
  POP3 244
  prerequisites 287, 292
  Report 58
  Scheduled Call 294
  Server SDK compilers 314
  SMTP 244
  Telephony 60, 291
  time synchronization 54
  time zones 49
  TSQS 60
  voice channel 60
  web 235
  Web License Manager 53
  Web Management 62, 294, 297
  Workflow 58
Service Observing 356
service packs
  Windows XP Professional 266, 267
setting up
  databases 209
  email servers 243
  Oracle 220
  third party applications 313
  web servers 235
  Windows 265
Siebel database 47

Siebel, Avaya IC for 305
single instance, Business Advocate 145
single site
Business Advocate
high volume voice 92
multi-channel 112
voice only 88
chat and email 117
deployment scenarios 79
multi-channel 96, 104
voice 82
Sizing Tool 81
skill groups, defining 351
SMTP 62
SMTP servers 244
software
databases 209
Design & Administration Tools 306
email servers 243
exceptions 231
Internet Explorer 267
Oracle 220
Server SDK compilers 314
SQL Server 214
telephony 231
web servers 235
Windows 265
Solaris
browser 271
configuration requirements 272
disk space requirements 271
installation user 274
physical address 201
root user 273
Server SDK compiler 314
support 270
time synchronization 54
ulimit parameters 273
user accounts 273
verifying DNS resolution 261
web server 237
windowing environment 272
SQL Server
database tables 48
installing 215, 216
setting up 214
SSL
Client SDK 28
subnet mask 260
Sun Studio 314
support limitations
Citrix 21
Thai 21
Traditional Chinese 20
supported
languages 20
operating systems 247, 263
third party applications 313
switches
Communication Manager 231
exceptions 231
TSA server 65
synchronous communication, SSL 28
system store 46

T

tablespace, DB2 228
Tardis 2000 54
TCP/IP
communication protocol 39
networking 259
technologies 28
Telephony
about 25
Avaya switches 293
deployment 60
Event Collector server 74
exceptions 231
multi-site 124
prerequisites 292
required software 291
servers 291
single site 82
switches 231
TSA server 65
Telephony Queue Statistics server 60
Telephony server 60
Telephony Services Adaptor server 64
Thai
configuring SQL Server 254
configuring Windows 250
limitations 21
third party applications 313
time synchronization 54
time zones
host/local 49
local 49
methods 49
RDBMS 49
UTC 49
Web Scheduled Callback 50, 66
Tomcat
about 240
AJP 1.3 connector 241
default web application contexts 240
failover 241
installation location 240
Jakarta Tomcat Connector 241
load balancing 241

Traditional Chinese, limitations 20
troubleshooting
Event Collector server 76
license files 200
unresolved DNS 262
Trusted Sites 269
TSA server 64
TSQS server 60

U

ulimit parameters, Solaris 273
uname 201
Universal Call ID (UCID) 359
updating, license file 203
user accounts
AIX 277
installation 274, 277
root 273, 277
Solaris 273
users, concurrent 37
UTC 49

V

validation 192
Vector Directory Numbers (VDNs), defining 346
vectors, defining 346
verifying DNS resolution
AIX 261
Solaris 261
Windows 260
version mode
DB2 client 226
Oracle client 221
Visual Studio 314
voice
adding server machines 80
DUStore server 61
multi-site 124
single site 82
volume of contacts 37
VPN 40

W

WAA server 65
WAN 39
Web Advocate Adaptor server 65
Web interface, Citrix 281
Web License Manager 53, 202, 203, 204
Web Management
about 25
binary sort order 214
Citrix 279
deployment 62
prerequisites 295
required software 293
Scheduled Call 294
server guidelines 61
servers 62, 294, 297
web servers 235
Web Scheduled Callback
agent desktop applications 66
calendar 66
guidelines 50, 66
time zones 50, 66
Web Self-Service about 25
web servers
AIX 238
IBM HTTP Server 238
Oracle Java System Web Server 237
Solaris 237
Tomcat 240
Windows Server 2008 R2 235
W ɜb Services
configuring Tomcat 240
default web application context 240
failover 241
Jakarta Tomcat Connector 241
load balancing 241
Tomcat installation 240
WebLM 53
webservices 240
Website, Citrix 279
Windowing environment 272, 276
Windows
Active Directory mode 248
physical address 201
Server SDK compiler 314
setting up 265
time synchronization 54
verifying DNS resolution 260
Workgroup mode 248
Windows Server 2003
Active Directory 249
JVM 268
MSMQ 248
Workgroup mode 248
Windows Server 2008 R2
web server 235
Windows XP Professional
JVM 268
service packs 266, 267
Workflow Designer
about 23
prerequisites 306
Workflow server 37, 58
Business Advocate 59

email qualification....59
workflows
Business Advocate....66
customization....58
Workgroup mode
about....248
implementing....248

X

X-Windows....272, 276