Deploying Avaya Oceana®

Release 3.10.0.1
Issue 4
February 2026

Notices

© 2026 Avaya LLC. All Rights Reserved.

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

© 2016-2026, Avaya LLC
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

License types

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H 3 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.



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

Java is a registered trademark of Oracle and/or its affiliates.



Contents

Chapter 1: Introduction 22
Purpose 22
Change history 22
Chapter 2: Overview 23
Avaya Oceana® overview 23
Architecture 24
Chapter 3: Security Considerations for Avaya Oceana® and Avaya Analytics™ deployments 26
Introduction 26
SAL Policy Manager 27
Secure Communications using Transport Layer Security 27
Overview 27
Certificate Authority (CA) 29
Operating Systems 30
Surround Applications and Client Security 30
EASG-based authentication of Web Administrative Interfaces for Avaya Oceana® 31
Beyond the Enterprise Applications Security 33
Secure Solution Deployment 33
How to replace Default Breeze Node Identity Certificates 34
Avaya Oceana® Cluster Identity Certificate requirements 34
Modifying the End Entity Profile to support Avaya Oceana® 36
Creating and replacing default Identity Certificates for Avaya Oceana® Cluster 1 37
Creating and replacing default Identity Certificates for Avaya Oceana® Cluster 2 38
Creating and replacing default Identity Certificates for Avaya Oceana® Cluster 3 39
Viewing Breeze Identity Certificate details 40
User's Client Software and Platform requirements for secure connections 41
Chapter 4: Deployment process 42
Work flow 42
Chapter 5: Planning and preconfiguration 45
Planning and preconfiguration 45
Capacity specifications 46
Hardware and software specifications 49
Avaya Oceana® hardware requirements 51
Virtual Machine requirements 55
Inputs for Omnichannel Windows Server 61
VMware configuration 63
Upgrading ESXi hosts running Avaya Oceana® or Avaya Analytics™ virtual machines 67
Thin provisioning of disk storage in VMware 67
Avaya Oceana® virtualized deployment checklist 68

Create the database for External Data Mart 68
Planning tasks 69
Configuring the TLS version 69
Configuration and deployment details 70
Configuring LDAP server integration 74
Avaya Workspaces single sign-on 76
Adding Avaya Contact Recorder or Avaya Contact Recorder Advanced to Avaya Oceana® 77
Route Points configuration 77
Chapter 6: Deploy Avaya Breeze® nodes 79
Deploy Avaya Breeze® platform nodes overview 79
Avaya Breeze® platform nodes deployment checklist 80
Verifying the Avaya Breeze® platform deployment using System Manager 81
CylancePROTECT deployment on Avaya Breeze® 82
Installing CylancePROTECT 82
Verifying CylanceProtect running status 84
Disabling CylancePROTECT before the upgrade 84
Re-enabling CylancePROTECT post upgrade 84
Chapter 7: Configure certificates 86
Exporting root, intermediate, and LDAP certificates 86
Configuring server certificates for Avaya Breeze® platform nodes 87
Importing the authorization certificate 88
Exporting the Avaya Breeze® platform Authorization Identity Certificate 89
Chapter 8: Configure Session Manager routing 90
Configuration overview 90
Creating a routing location 90
Creating a Session Initiation Protocol (SIP) entity for Session Manager 91
Creating a SIP entity for Communication Manager 91
Creating a SIP entity for Avaya Breeze® platform 92
Creating a SIP entity for Experience Portal Media Processing Platform 92
Creating an entity link from Session Manager to Experience Portal Media Processing Platform 93
Creating an entity link from Session Manager to Communication Manager 93
Creating a routing policy for the Experience Portal Media Processing Platform entity link 93
Creating a routing policy for the Communication Manager entity link 94
Creating Dial Patterns for Experience Portal Media Processing Platform Routing Policy 94
Creating Dial Patterns for Communication Manager Routing Policy 95
Chapter 9: Deploy Avaya Oceana® clusters 97
Deploy Avaya Oceana® clusters 97
Verifying the host name resolution for Avaya Breeze® platform nodes 98
Loading license files in System Manager 99
Installation of Avaya Oceana® snap-ins 99
Viewing Oceana Monitor Service pages 140
Oceana Dashboard overview 141

Viewing Oceana Dashboard..... 142
Viewing Oceana Manager..... 143
Viewing Stuck Contact Tool..... 143
Chapter 10: Deploying External Data Mart..... 145
Deploy External Data Mart overview..... 145
Deploy External Data Mart on Avaya Control Manager SQL Server..... 146
Deploy External Data Mart on standalone SQL Server..... 163
Setting attributes to enable connection from Context Store to EDM..... 180
Transparent Data Encryption (TDE) on External Data Mart..... 182
Configuring automated SQL Server Agent jobs..... 189
Chapter 11: Deploy Engagement Designer tasks and workflows..... 191
Deploying Engagement Designer tasks..... 191
Verifying Engagement Designer tasks..... 192
Deploy Engagement Designer workflows..... 192
Exporting multiple workflows..... 193
Importing multiple workflows..... 194
Searching an instance in Engagement Designer Admin console..... 194
Deleting instances in Engagement Designer Admin console..... 195
Chapter 12: Deploy Omnichannel Windows Server..... 197
Deploy Omnichannel Windows Server overview..... 197
Creating a VMware virtual machine..... 197
Installing Microsoft Windows Server 2022..... 198
Installing the most recent supported operating system service packs..... 199
Adding the server to a domain..... 200
Disabling unused network adapters..... 201
Enabling Microsoft Remote Desktop connection..... 201
Disabling Admin Approval Mode for Omnichannel Windows Server administrators..... 202
Enabling or disabling a scheduled computer maintenance in Windows 2019..... 203
Installing the Omnichannel server software..... 203
Removing Server Message Block (SMB) from Omnichannel Server..... 204
Removing the IIS Default page..... 205
Manage Security and TLS certificates..... 205
Certificate Profiles..... 207
Creating end entities..... 208
Creating a Certificate Signing Request..... 208
Creating a certificate from a CSR..... 209
Creating a keystore to identify users..... 210
Configuring Caché to use TLS..... 210
Changing the Omnichannel Database password..... 212
Database encryption..... 213
Chapter 13: Commission Avaya Control Manager..... 219
Commission Avaya Control Manager overview..... 219
Creating a Communication Manager user for Avaya Control Manager..... 219

Logging in to Avaya Control Manager 220
Creating a location for Avaya Oceana® 221
Adding Communication Manager to Avaya Control Manager 221
Adding Communication Manager to the location 222
Adding a site, department, and team to Avaya Control Manager 222
Synchronizing Avaya Control Manager and Communication Manager 223
Creating a Manager Server for Unified Collaboration Administration 224
Adding an Avaya Oceana® server to a location 226
Synchronizing Avaya Oceana® Server 226
Adding connectors to Provisioning Server 227
Configuring token-based access between Control Manager and Avaya Oceana®, Avaya Analytics™, or Avaya Workspaces for Call Center Elite 228
Assigning a location to the UCA proxy server 235
Assigning location to Application Server 235
Assigning location to Synchronizer Service Server 236
Testing the UCA REST connection 236
Categories, Attributes, and Attribute Sets 237
Users, Accounts, and Providers 238
Adding Attribute Categories to Avaya Control Manager 238
Adding Attributes to Avaya Control Manager 239
Adding services to Avaya Control Manager 240
Configuring Properties in Avaya Control Manager 241
Configuring Avaya Oceana® system properties using Control Manager 242
Configuring access to Omnichannel Administration Utility 246
Starting Omnichannel Administration Utility 250
Starting Oceana Customer Management Tool 250
Chapter 14: Configure Communication Manager and Call Center Elite for Avaya Oceana 251
Configure Communication Manager and Call Center Elite overview 251
Configure Communication Manager resources for Avaya Oceana® 251
Logging on to Communication Manager 253
Configuring System Features and Customer Options 253
Configuring Signaling and Trunk Groups 254
Configuring a Route Pattern 255
Adding a Route Pattern to the Locations table 256
Configuring CTI-Link to Application Enablement Services 256
Configuring Direct Agent Calling 257
Configuring a Hunt Group 257
Configuring Agent Login ID using Communication Manager 258
Configuring Agent Phone-sets 259
Chapter 15: Configure Application Enablement Services 260
Configure Application Enablement Services overview 260
Configuring Communication Manager Link to Application Enablement Services 260

Configuring AES certificates ... 262
Creating an end entity ... 262
Creating the server certificate ... 263
Downloading the CA certificate ... 263
Importing the CA certificate to Application Enablement Services ... 263
Importing the server certificate to Application Enablement Services ... 264
Creating Application Enablement Services user for Call Server Connector communication ... 264
Verifying Application Enablement Services connection with Call Server Connector service ... 265
Chapter 16: Configure wait treatments for Voice contacts ... 267
Configure wait treatments for Voice contacts overview ... 267
Logging on to Communication Manager ... 268
Configuring the prompting timeout ... 268
Creating variables using Communication Manager ... 269
Configuring Avaya Aura® Media Server media files for Voice ... 272
Adding announcements ... 273
Creating the Fallback Vector Directory Number ... 274
Configuring a vector for the Fallback VDN ... 275
Creating the Ingress Vector Directory Number ... 276
Configuring a vector for the Ingress VDN ... 277
Creating the Treatment Vector Directory Number ... 278
Configuring a vector for the Treatment VDN ... 279
Creating the Routing Vector Directory Number ... 281
Configuring a vector for the Routing VDN ... 282
Creating the RONA Vector Directory Number ... 284
Configuring a vector for the RONA VDN ... 285
Creating the Coverage Vector Directory Number ... 287
Configuring a vector for the Coverage VDN ... 288
Creating a Transfer Vector Directory Number ... 290
Configuring a vector for the Transfer to Service VDN ... 292
Configuring a vector for the Transfer to User VDN ... 293
Chapter 17: Deploy the sample workflows for Voice ... 295
Deploying the sample Voice workflow ... 295
Modifying the sample Voice workflow ... 297
Adding a rule to the sample Voice workflow for priority, rank, and service ... 298
Sample Voice workflow ... 299
Deploying the sample Transfer to Service workflow for Voice ... 301
Chapter 18: Configure Voice Self Service ... 303
Configure Voice Self Service for Avaya Oceana® overview ... 303
Configure Avaya Experience Portal ... 304
Configure Avaya Aura® Call Center Elite ... 315
Chapter 19: Configure Callback Assist ... 329
Callback Assist overview ... 329
Prerequisites for configuring Callback Assist ... 330

Creating a Web Service user in Experience Portal 330
Logging on to the Avaya Callback Assist Administration interface 331
Creating a site definition 331
Taking a note of the Outbound Callback application name 332
Setting the System ANI parameter 332
Setting the Storage URL parameter 333
Setting Avaya Oceana® -specific parameters 333
Creating a callback configuration 334
Configuring the default Line of Business configuration 337
Exporting the Avaya Oceana® Cluster 1 certificate 337
Importing certificates to Callback Assist 338
Deploying the OceanaCallback application 339
Adding Callback applications in Experience Portal 339
Verifying the dial plan for Avaya Oceana® 341
Creating the Callback Vector Directory Number 341
Configuring a vector for the Callback VDN 342
Editing the existing Treatment vector 343
Adding the Callback VDN to Avaya Control Manager 344
Creating the No Media Treatment Vector Directory Number 345
Configuring a vector for the No Media Treatment VDN 346
Adding the No Media Treatment VDN to Avaya Control Manager 347
Updating the voicemail announcement 347
Configuring the Voice workflow for Callback Assist 348
Configuring the session timer 348
Disabling video on the incoming SIP trunk 349
Chapter 20: Configure Post Call Survey 350
Post Call Survey overview 350
Deploying the OceanaSurvey application 352
Adding the OceanaSurvey application in Experience Portal 353
Creating the Survey Vector Directory Number 354
Configuring a vector for the Survey VDN 355
Configuring the Return Destination parameter on the Routing vector 356
Enabling the Allow VDN Override parameter on specific VDNs 357
Adding the Survey VDN to Avaya Control Manager 358
Chapter 21: Configure Authorization Service for Outbound Connector 359
Configuring authorization service for outbound connector provider cluster 359
Enabling authentication flag in the OCP service cluster 359
Chapter 22: Configure voice resources through Avaya Control Manager 361
Configure Voice resources through Avaya Control Manager 361
Configuring a Communication Manager Hunt Group 361
Creating variables using Avaya Control Manager 362
Configuring Vector Directory Numbers 364
Adding Provider, Skills, VDN, and Extensions to Avaya Oceana® 365

Creating a user to handle Voice contacts 367
Adding attributes to an agent 368
Creating a Transfer Target service for Voice 369
Restarting the CallServerConnector service 369
Chapter 23: Verify Voice contacts 371
Verify Voice contacts using Avaya Workspaces 371
Deploying Avaya Workspaces 371
Logging in to Avaya Workspaces 371
Starting work in Avaya Workspaces 372
Verifying Voice contact routing to agents 373
Chapter 24: Configure Avaya Oceana® with Avaya WebRTC Connect agents 375
Avaya WebRTC Connect solution configurations and prerequisites 375
Checklist for configuring Avaya Oceana® with Avaya WebRTC Connect agents 376
Configure LDAP 377
Preconfiguration 377
Creating a user in Active Directory 378
Synchronizing LDAP users in System Manager 379
Avaya Aura® Device Services deployment 380
Adding a data center 381
Assigning Session Manager to the data center 381
Deploy Avaya Aura® Device Services on a virtualized environment 381
Installing Avaya Aura® Device Services 383
Publishing COMM_ADDR_HANDLE values on Avaya Aura® Device Services 385
Avaya Aura® Media Server deployment 386
Install and configure Avaya Aura® Media Server for Avaya Breeze® platform 386
Changing the default password in Avaya Aura® Media Server 391
Installing Avaya Aura® Media Server updates 391
Setting up the Avaya Aura® Media Server cluster 392
Enrolling Avaya Aura® Media Server with System Manager 393
Configuring security certificates 394
Configuring Avaya Aura® Media Server 395
Assigning a location to media servers 396
Configure Avaya Aura® Media Server for Avaya Breeze® platform 396
Configure Avaya Aura® Media Server for Avaya Aura® Web Gateway 398
Avaya Aura® Web Gateway deployment and configuration 400
Prerequisites for Avaya Aura® Web Gateway 400
Deploying Avaya Aura® Web Gateway 400
Adding a device to System Manager 400
Configuring Avaya Aura® Web Gateway 401
Verifying the components connected to Avaya Aura® Web Gateway 403
Configuring Avaya Aura® for Avaya Aura® Web Gateway 403
Enabling Token Service and TestApp 404
Testing the installation of Avaya Aura® Web Gateway 405

Enabling port for remote access on Avaya Aura® Web Gateway HTTP Reverse Proxy..... 405
Troubleshooting the TestApp issues..... 406
Avaya Aura® Web Gateway authorization..... 407
Configure the voice media path..... 407
Configuring codecs in Avaya Aura® Web Gateway..... 407
Prioritizing codecs in Avaya Aura® Media Server..... 408
Prioritizing codecs in Communication Manager..... 408
Creating Avaya WebRTC Connect agents for Avaya Oceana®..... 409
Creating a user in Active Directory..... 409
Create a user in System Manager and Communication Manager..... 409
Creating users in Avaya Control Manager..... 411
Chapter 25: Configure Avaya Oceana® with web and mobile voice calls..... 416
Checklist for configuring Avaya Oceana® with web and mobile voice calls..... 416
Install and configure web and mobile applications..... 417
Installing the Javascript reference client..... 417
Configuring the Javascript reference client and making a call..... 418
Installing the iOS reference client..... 420
Configuring the iOS reference client and making a call..... 420
Installing the Android reference client..... 422
Configuring the Android reference client and making a call..... 423
Install and configure Avaya Aura® Session Border Controller..... 425
Configuring Avaya Aura® Session Border Controller networks..... 425
Creating a reverse proxy policy..... 426
Creating a reverse proxy service for Avaya Aura® Web Gateway..... 426
Deploying Identity Certificate on Avaya Aura® Session Border Controller..... 427
Creating a client profile for the AvayaMobileCommunications reverse proxy relay..... 432
Creating a server profile for the AvayaMobileCommunications reverse proxy relay..... 433
Creating a reverse proxy service for the AvayaMobileCommunications snap-in..... 433
Configure the Avaya WebRTC Connect client side TURN..... 434
Creating a server profile for the Avaya Aura® Session Border Controller signaling interface. 435
Creating the Avaya Aura® Session Border Controller signaling interface..... 436
Configuring the Avaya Aura® Session Border Controller external media interface..... 436
Configuring the Avaya Aura® Session Border Controller internal media interface..... 437
Creating an application rule..... 437
Creating an endpoint policy group..... 438
Creating a client profile for the Avaya Aura® Session Border Controller signaling interface.. 438
Creating an interworking profile without remote Avaya Aura® Session Border Controller..... 438
Adding a server configuration for Avaya Aura® Web Gateway..... 439
Adding a server configuration for Session Manager..... 440
Adding a server flow for Avaya Aura® Web Gateway..... 440
Adding a server flow for Session Manager..... 441
Configuring Avaya Aura® Session Border Controller for load monitoring..... 441
Adding Avaya Aura® Session Border Controller as a SIP entity in System Manager..... 442

Adding the Avaya Aura® Session Border Controller configuration to Avaya Aura® Web Gateway ... 442
Route web and mobile voice calls to Avaya WebRTC Connect workflows ... 443
Configuring routing to Engagement Designer ... 443
Configuring Engagement Designer Event Mapper to trigger the Web Voice workflow ... 446
Creating an Avaya Breeze® platform Implicit User Profile for the Web Voice service profile ... 447
Configuring routing for the AvayaMobileCommunications SVAR ... 448
Creating an application and application sequence ... 450
Administering implicit sequencing for Avaya Mobile Communications ... 451
Configuring an Implicit User Route Point for inbound Web Voice ... 451
Configure the transfer to service feature for web and mobile voice calls ... 452
Configuring Communication Manager settings to transfer web and mobile voice calls ... 452
Deploying the sample Transfer to Service workflow for Web Voice ... 454
Configuring Engagement Designer Event Mapper to trigger the Web Voice Transfer to Service workflow ... 455
Configuring the first Transfer to Service Implicit User for Web Voice ... 456
Creating a Vector Directory Number for Web Voice Transfer ... 457
Configuring a vector for the Web Voice Transfer VDN ... 457
Configuring the second Transfer to Service Implicit User for Web Voice ... 458
Creating a Transfer Target service for Web Voice ... 459
Chapter 26: Configure Avaya Oceana® with web and mobile voice calls and Avaya WebRTC Connect agents ... 460
Checklist for configuring Avaya Oceana® with web and mobile voice calls and Avaya WebRTC Connect agents ... 460
Chapter 27: Configure Avaya Oceana® with web and mobile video calls and Avaya WebRTC Connect agents ... 462
Checklist for configuring Avaya Oceana® with web and mobile video calls and Avaya WebRTC Connect agents ... 462
Deploying the sample Web Video workflow ... 464
Route web and mobile video calls to Avaya WebRTC Connect workflows ... 465
Configuring Engagement Designer Event Mapper to trigger the Web Video workflow ... 465
Configuring an Implicit User Route Point for inbound Web Video ... 466
Create Avaya WebRTC Connect video agents ... 467
Configuring customer options ... 467
Configuring the signaling group for Web Video ... 467
Enabling Video on a Communication Manager SIP station ... 468
Enable Video for Avaya Oceana® SIP agents ... 468
Configuring a provider to support Video ... 468
Enabling Video for an Avaya Oceana® agent ... 468
Configure the video media path ... 469
Configuring media servers for Web Video ... 469
Configuring an IP codec set for Video ... 469
Configuring codecs in Avaya Aura® Web Gateway ... 470

Prioritizing codecs in Avaya Aura® Media Server ... 470
Prioritizing codecs in Communication Manager ... 471
Configure the transfer to service feature for web and mobile video calls ... 471
Configuring Communication Manager settings to transfer web and mobile video calls ... 471
Deploying the sample Transfer to Service workflow for Web Video ... 473
Configuring Engagement Designer Event Mapper to trigger the Web Video Transfer to Service workflow ... 474
Configuring the first Transfer to Service Implicit User for Web Video ... 475
Creating a Vector Directory Number for Web Video Transfer ... 476
Configuring a vector for the Web Video Transfer VDN ... 476
Configuring the second Transfer to Service Implicit User for Web Video ... 477
Creating a Transfer Target service for Web Video ... 478
Chapter 28: Remote worker solution ... 479
Remote worker solution overview ... 479
Remote workers capabilities ... 479
Remote workers limitations ... 480
Remote worker solution architecture ... 481
Remote worker solution process flow ... 484
Configuration and deployment details for the remote worker solution ... 486
Chapter 29: Deploy Web Voice and Web Video for remote workers ... 489
Deploy Web Voice and Web Video for remote workers overview ... 489
Checklist for configuring Avaya Oceana® with remote Avaya WebRTC Connect agents ... 489
Install and configure Avaya Aura® Session Border Controller ... 490
Chapter 30: Configure Avaya Session Border Controller for external mobile client access ... 508
Overview ... 508
Configuring the TLS server profile for Avaya Aura® Session Border Controller external communication ... 508
Configuring the TLS server profile for Avaya Aura® Session Border Controller media tunneling ... 509
Configuring the TLS client profile on Avaya Aura® Session Border Controller ... 510
Configuring Avaya Aura® Session Border Controller network interfaces ... 511
Configuring the Avaya Aura® Session Border Controller signaling interface ... 511
Configuring the Avaya Aura® Session Border Controller media interface for external mobile client ... 512
Configuring Avaya Aura® Session Border Controller load monitoring for external mobile access ... 514
Configuring Avaya Aura® Session Border Controller server flows for external mobile calls ... 515
Configuring Avaya Aura® Session Border Controller STUN TURN server for external mobile calls ... 517
Chapter 31: Deploy Multimedia channels for remote workers ... 519
Deploy Multimedia channels for remote workers overview ... 519
Prerequisites ... 519
Checklist for deploying Multimedia channels for remote workers ... 520

Documentation of FQDNs and IP addresses of solution interfaces for Multimedia remote workers ... 520
Publishing of FQDNs external to the enterprise for Multimedia remote workers ... 521
Configure the external firewall for Multimedia remote workers ... 521
Configure the reverse proxy for Multimedia remote workers ... 521
Checklist for configuring a sample reverse proxy relay ... 523
Configure the internal firewall for Multimedia remote workers ... 530
Chapter 32: Configure the sample Chat client ... 531
Configure the sample Chat client overview ... 531
Deploying the sample Chat client on an Apache HTTP server ... 531
Configuring the solution URLs for testing ... 532
Adding custom attributes ... 533
Changing the workflow type ... 534
Downloading the root certificate from Avaya Aura® System Manager ... 535
Installing the root certificate ... 536
Verifying to ensure the browser accepts the certificate ... 536
Chapter 33: Configure Chat ... 537
Configure Chat overview ... 537
Enabling Automation Startup message overview ... 537
Configuring BotConnector Snap-in licenses ... 537
Deploying the sample Chat workflow ... 538
Adding a rule to the sample Chat workflow for priority, rank, and service ... 539
Deploying the sample Transfer to Service workflow for Chat ... 540
Configuring the sample Transfer to Service workflow for Chat ... 541
Configuring a Chat provider ... 542
Creating a user to handle Chat contacts ... 542
Configuring Chat for Transfer to Service ... 544
Chat limits ... 545
Configuring AgentControllerService to access UnifiedAgentController ... 545
Setting the Authorization Service address to enable authorized access to Oceana transcripts ... 546
Chapter 34: Verify Chat contacts ... 547
Verify Chat contacts using Avaya Workspaces ... 547
Deploying Avaya Workspaces ... 547
Logging in to Avaya Workspaces ... 547
Starting work in Avaya Workspaces ... 548
Making a test Chat contact ... 549
Making a test Chat contact using Avaya Co-Browsing Snap-in ... 550
Chapter 35: Configure Email ... 552
Configure Email overview ... 552
Configuring an Email provider ... 552
Configuring an Email Route Point ... 553
Configuring Email server certificates ... 553

Configuring an Email server and mailboxes..... 554
Configuring the maximum number of days to retain active email contacts..... 554
Configuring an Outbound SMTP server..... 556
Configuring an Inbound Mail server..... 556
Configuring keyword groups..... 557
Configuring an automatic response..... 558
Configuring an automatic suggestion response..... 558
Configuring Email inboxes..... 559
Configuring rule groups..... 564
Configuring system default rule..... 567
Configuring system delivery failure rule..... 568
Configuring email settings..... 568
Configuring Email Templates..... 569
Blacklisting email addresses and domains..... 570
Deploying the sample Email workflow..... 571
Deploying the sample Transfer to Service workflow for Email..... 572
Configuring the sample Transfer to Service workflow for Email..... 573
Resume email flow..... 573
Creating a user to handle Email contacts..... 574
Configuring Email for Transfer to Service..... 575
Outbound email approval..... 576
Configuring AgentControllerService to access UnifiedAgentController..... 579
Creating or editing Authorization grants for the UnifiedAgentController service..... 580
Setting the Authorization Service address to enable authorized access to Oceana transcripts..... 580
Conversation Transcripts through Email..... 581
Chapter 36: Verify Email contacts..... 582
Verify Email contacts using Avaya Workspaces..... 582
Deploying Avaya Workspaces..... 582
Logging in to Avaya Workspaces..... 582
Starting work in Avaya Workspaces..... 583
Verifying Email contact routing to agents..... 584
Chapter 37: Configure SMS..... 585
Configure SMS overview..... 585
Prerequisites for ZangSmsConnector Snap-in..... 585
Configuring an SMS provider..... 586
Configuring SMS Gateway..... 587
Loading and installing the ZangSmsConnector or SMSVendorSnapin SVAR..... 589
Setting ZangSmsConnector Snap-in or SMSVendorSnapin attributes..... 591
Verifying the SMSVendorSnapin deployment..... 592
Verifying the ZangSmsConnector Snap-in..... 593
Deploying the sample SMS workflow..... 593
Deploying the sample Transfer to Service workflow for SMS..... 595

Configuring the sample Transfer to Service workflow for SMS ... 596
Configuring the maximum number of days to retain active SMS contacts ... 597
Creating a user to handle SMS contacts ... 598
Configuring SMS for Transfer to Service ... 599
SMS limits ... 600
Configuring AgentControllerService to access UnifiedAgentController ... 600
Setting the Authorization Service address to enable authorized access to Oceana transcripts ... 601
Chapter 38: Verify SMS contacts ... 602
Verify SMS contacts using Avaya Workspaces ... 602
Deploying Avaya Workspaces ... 602
Logging in to Avaya Workspaces ... 602
Starting work in Avaya Workspaces ... 603
Verifying SMS contact routing to agents ... 604
Chapter 39: Configure Social Media ... 605
Configure Social Media overview ... 605
Configuring a Social Media provider ... 605
Configuring Social Media for third-party gateways ... 605
Configuring secure communication to third-party gateways ... 607
Deploying the sample Social Media workflow ... 607
Deploying the sample Transfer to Service workflow for Social Media ... 608
Configuring the sample Transfer to Service workflow for Social Media ... 609
Configuring the maximum number of days to retain active social media contacts ... 610
Creating a user to handle Social Media contacts ... 612
Configuring Social Media for Transfer to Service ... 613
Deployment process for the Asynchronous Connector ... 614
Configuring AgentControllerService to access UnifiedAgentController ... 616
Setting the Authorization Service address to enable authorized access to Oceana transcripts ... 617
Chapter 40: Verify Social Media contacts ... 618
Verify Social Media contacts using Avaya Workspaces ... 618
Deploying Avaya Workspaces ... 618
Logging in to Avaya Workspaces ... 618
Starting work in Avaya Workspaces ... 619
Verifying Social Media contact routing to agents ... 620
Chapter 41: Configure Messaging ... 622
Configure Messaging overview ... 622
Deploying the sample Messaging workflow ... 624
Deploying the sample Transfer to Service workflow for Messaging ... 625
Configuring the sample Transfer to Service workflow for Messaging ... 627
Configuring a Messaging provider ... 628
Configuring the maximum number of days to retain active messaging contacts ... 628
Creating a user to handle Messaging contacts ... 630

Configuring Messaging for Transfer to Service 631
Configuring a Transfer to Service Route Point for Messaging 631
Creating a Transfer Target service for Messaging 631
Configuring screen pops for Messaging 632
Messaging limits 634
Incoming messages limit 634
Configuring Message Connector parameters in Omnichannel Administration Utility 635
Installing Certificate Authority and Identity Certificate for Messaging HA 635
Viewing contact status in Oceana Data Viewer for Messaging HA 636
Configuring AgentControllerService to access UnifiedAgentController 637
Setting the Authorization Service address to enable authorized access to Oceana transcripts 638
Delivery Failure Notification 638
Credit Card Redaction 640
Routing enhancement - contact priority 640
Chapter 42: Configure the sample Messaging clients 642
Configure sample Messaging clients 642
Chapter 43: Verify Messaging contacts 643
Verify Messaging contacts using Avaya Workspaces 643
Deploying Avaya Workspaces 643
Logging in to Avaya Workspaces 643
Starting work in Avaya Workspaces 644
Verifying Messaging contact routing to agents 645
Chapter 44: Configure Outbound 646
Configure Outbound overview 646
Install and configure POM 646
Configuring and exchanging certificates for Proactive Outreach Manager 646
Configuring the POM server certificate for Avaya Oceana® Cluster 3 649
Configuring an Outbound provider 649
Adding Disposition Codes for Outbound contacts 650
Creating a user to handle Outbound contacts 651
Configuring After Contact Work time 652
Chapter 45: Verify Outbound contacts 654
Verify Outbound contacts using Avaya Workspaces 654
Deploying Avaya Workspaces 654
Logging in to Avaya Workspaces 654
Starting work in Avaya Workspaces 655
Verifying Outbound contact routing to agents 655
Chapter 46: Avaya Workspaces for Avaya Oceana® logging 657
Logs 657
Downloading the Avaya Workspaces logs 657
Modifying the logging configuration 658
Chapter 47: Deploy Avaya Oceana® for High Availability 659

Avaya Oceana® High Availability overview 659
Recovery from failure scenarios 661
Avaya Control Manager HA 663
Omnichannel Provider HA 663
Omnichannel Database HA 663
Omnichannel Database HA configuration checklist 664
Retrieve certificate files 665
Exporting the Certificate Authority file 665
Installing the Arbiter service 665
Configuring Cache Mirroring on the active Omnichannel Database server 666
Configuring Cache Mirroring on the standby Omnichannel Database server 668
Setting the Omnichannel Database Address attribute for HA 670
Configuring the Omnichannel Database address in Avaya Control Manager 671
Securing the Cache Mirror on the Omnichannel Database servers 671
Removing Cache Mirroring from the standby Omnichannel Database server 673
Removing Cache Mirroring from the active Omnichannel Database server 673
Recommissioning physical servers or virtual machines after a network outage 674
EU Data Center Deployments 675
Chapter 48: Configure Oceana Customer Management Tool and Omnichannel Administration Tool 676
Configuring access to Oceana Customer Management Tool 676
Omnichannel Administration Utility access configuration 677
Configuring access to Omnichannel Administration Utility 677
Creating end entities 678
Creating a Certificate Signing Request 679
Creating a certificate from a CSR 680
Generating a certificate pfx file 680
Importing certificate pfx file to Omnichannel Database server 681
Configuring admin certificates for HA 681
Exporting the Certificate Authority file 682
Importing the Certificate Authority as a Trusted Root Certificate Authority through the mmc application 682
Performing non-secure communication between Avaya Control Manager and Omnichannel Windows server 683
Enabling SSL for secure browser access 683
Starting Oceana Customer Management Tool 684
Starting Omnichannel Administration Utility 685
Exporting customer details from Salesforce 685
Customer data import template 686
Oceana Customer Management Tool 689
Account Types 690
Customer accounts management 690
Adding new account types to Avaya Oceana® 692

Customer data import ... 693
Importing customer data from a text file ... 693
Importing customer data from an ODBC database ... 694
Adding customer data manually ... 695
Adding custom fields ... 695
Customer data cleanup ... 696
Validating customer data ... 696
Inserting text ... 696
Removing text ... 697
Replacing text ... 698
Splitting a phone number ... 698
Checking for duplicate customer data ... 699
Customer data search ... 700
Checking the length of fields ... 700
Checking for a value ... 701
Checking for alphabetic characters ... 702
Customer match ... 702
Checking customer matches ... 703
Import to Avaya Oceana® ... 703
Importing customer data into Avaya Oceana® ... 703
Export customer data ... 704
Exporting customer data ... 704
General settings ... 705
Viewing log files ... 705
Selecting the language configuration ... 706
Configuring the maximum number of days to retain active generic contacts ... 706
Capacity specifications ... 707
WorkAssignmentManagerService attributes ... 711
Chapter 49: Configure Avaya CRMGateway snap-in ... 714
Avaya CRMGateway snap-in overview ... 714
Prerequisites ... 715
Configuring secure communication to customer CRM entity ... 715
Verifying Avaya CRMGateway installation ... 716
Setting the Avaya CRMGateway snap-in attributes ... 716
CRMGateway attributes ... 716
Verifying CRM adapter configuration ... 719
Restarting the Avaya CRMGateway snap-in service ... 720
Uninstalling the Avaya CRMGateway snap-in service ... 720
Verifying Avaya CRMGateway snap-in uninstallation ... 721
Deleting the Avaya CRMGateway snap-in ... 721
Chapter 50: Configure secure connections from Avaya Oceana® Cluster 1 to External Data Mart ... 723
Overview ... 723

Secure space ... 723
Configuring space security ... 724
Cross Origin Resource Sharing ... 725
Transport Layer Security encryption checklist ... 725
Configuring the prerequisites for certificate management and usage ... 726
Creating Transport Layer Security certificate in System Manager ... 727
Downloading Transport Layer Security certificate from System Manager ... 728
Importing Transport Layer Security certificate from System Manager ... 729
Exporting Transport Layer Security certificate from MS SQL server ... 730
Configuring Avaya Context Store Snap-in for secure connections ... 731
Configuring MS SQL Server for forced encryption ... 732
Configuring the MS SQL server to listen on a static port ... 733
Breeze Authorization Service Integration ... 733
Port utilization ... 736
Chapter 51: Centralized logging ... 737
Centralized Logging overview ... 737
Checklist for centralized logging ... 737
Adding Breeze CA certificate to the Elasticsearch truststore on CCM ... 738
Loading the Breeze CA certificate into the Elasticsearch truststore ... 739
Restarting the Elasticsearch cluster ... 739
Adding Breeze node Common Name (CN) to CSP ... 740
Retrieving the Breeze node CN ... 740
Adding Breeze CN to CCM through CLI ... 740
Adding CSP CA to Avaya Breeze truststore ... 741
Changing the targeted Breeze cluster in Deny New Service state ... 741
Configuring Centralized Logging on the cluster editor ... 742
Changing the Avaya Breeze cluster state to accept new service ... 742
Installing the Metricbeat and Packbeat Snap-in on the Breeze cluster ... 743
Logging in to OpenSearch UI ... 743
Creating custom index patterns ... 744
Creating index policies for the custom index patterns ... 744
Policy recommendations for different deployment sizes ... 746
Discovering data using new index patterns ... 747
Recovery steps if the elasticsearch disk size is full ... 747
Chapter 52: Resources ... 749
Documentation ... 749
Finding documents on the Avaya Support website ... 750
Avaya Documentation Center navigation ... 751
Training ... 752
Support ... 755
Appendix A: Service attributes ... 756
Service attributes overview ... 756
Setting service attributes ... 756

CallServerConnector attributes..... 756
ContactCenterService attributes..... 758
ContextStoreManager attributes..... 760
ContextStoreQuery attributes..... 768
ContextStoreRest attributes..... 770
Support for CustomerJourneyService attributes..... 771
CustomerManagement attributes..... 775
EngagementDesigner attributes..... 777
OceanaCoreDataService attributes..... 781
OceanaMonitorService attributes..... 783
OmniCenterProvisioningCollector attributes..... 786
UCAStoreService attributes..... 787
UCMDataCollector attributes..... 788
UCMService attributes..... 789
WorkAssignmentManagerService attributes..... 790
AuthorizationService attributes..... 792
AvayaMobileCommunications attributes..... 793
BotConnector attributes..... 795
UnifiedAgentContextService attributes..... 796
UnifiedAgentController attributes..... 797
AgentControllerService attributes..... 800
AutomationController attributes..... 802
CustomerControllerService attributes..... 803
EmailService attributes..... 805
GenericChannelAPI attributes..... 807
MessagingService attributes..... 808
OBCService attributes..... 813
OCPDataServices attributes..... 814
ORCRestService attributes..... 815
OceanaDataViewer attributes..... 817
SocialConnector attributes..... 818
CoBrowse attributes..... 820
CRMGateway attributes..... 821
ZangSmsConnector attributes..... 823

Chapter 1: Introduction

Purpose

This document provides information about how to prepare, install, and configure Avaya Oceana®.

This document is intended for anyone who wants to deploy Avaya Oceana®.

Change history

Issue	Date	Summary of changes
4.0	February 2026	Updated WAS memory size from 3 GB to 6 GB in the procedure Creating Avaya Oceana Cluster 1 on page 105
3.0	July 2025	Updated the procedure for Configuring Avaya Aura Media Server media files for Voice on page 272.

Chapter 2: Overview

Avaya Oceana® overview

Avaya Oceana® is the next-generation customer engagement solution. Enterprises can use Avaya Oceana® to seamlessly handle Voice, Web and Mobile Chat, Web Voice/Video, Email, SMS, Social Media, Messaging, and Outbound channels using a single, intelligent, attribute-based call routing system through a unified Agent Desktop. Avaya Oceana® is built on the Avaya Breeze® platform using modular snap-ins that can be independently scaled, managed, and extended.

You can merge existing resources into the routing strategies of Avaya Oceana® to significantly improve customer service and sales outcomes.

With these routing strategies, you can:

- Obtain customer information from Customer Relationship Management (CRM) of the enterprise and other third-party systems.
- Combine the information with the current journey context of the customer.
- Apply business goals-oriented strategies to match the customer to the best available resource.

The routing strategies also integrate with the back office systems of enterprises to route work items such as claims and contracts.

Avaya Oceana® provides:

- Functionality to map a customer's journey across various self-service and assisted service channels by storing the related data crumbs in External Data Mart (EDM). Resources and routing workflows use these data crumbs.
- An easy-to-use HTML5-based Desktop for agents and supervisors.
- Reporting and Analytics, designed to provide new and powerful insights for blended agent contact centers.

The Social contact type is for the original Oceana integration traditionally using Social Connector to Social network infrastructure. For example, Facebook or Twitter.

The Messaging contact type uses an alternative mechanism through Messaging connector to enable integration with social networks. See Configure Messaging overview on page 622 on page 645.

Architecture

The following image is the high-level architecture of Avaya Oceana®:

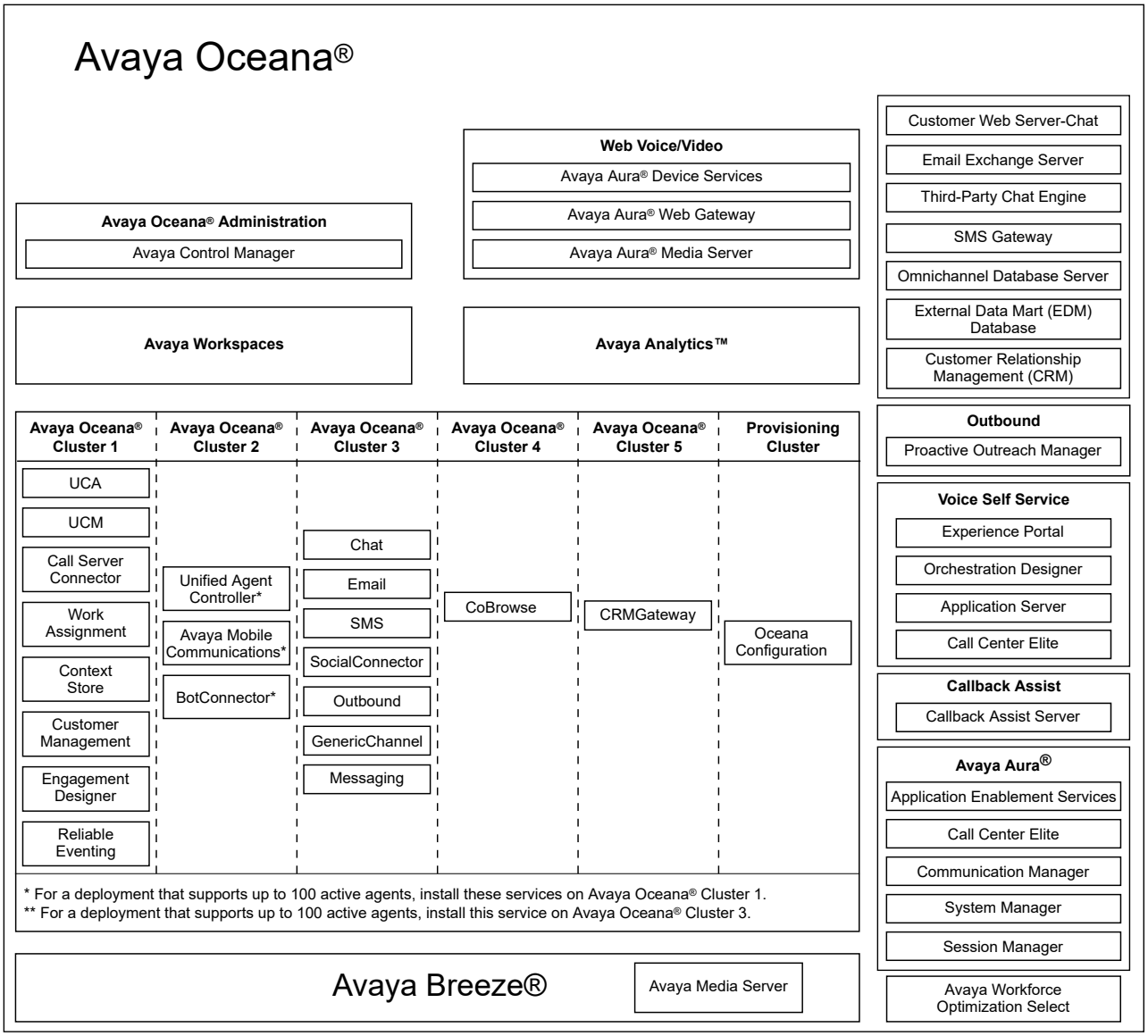


Figure 1: Avaya Oceana® architecture

Important:

- Do not install any third-party or custom Service Archives (SVARs) on the Avaya Breeze® platform nodes and the clusters used in Avaya Oceana®.

  These nodes and clusters are for the exclusive use of Avaya Oceana®.

- Do not add the Avaya Breeze® platform nodes to the specified Avaya Oceana® clusters.

- Do not use Context Store to store data for any other purpose. Instead, Context Store stores contextual data relating to work requests within Avaya Oceana®.

Chapter 3: Security Considerations for Avaya Oceana® and Avaya Analytics™ deployments

Introduction

Before starting the deployment process, use Avaya Oceana® and Avaya Analytics™ capabilities to enable or configure the security layers before you commence the deployment process. Customers must engage the expertise of their security staff early in the implementation process.

Multiple configurations turn off security by default while all other options are turned on. For example, customers can turn the security settings off manually. The staff must decide how to incorporate the security system into the routine maintenance for virus protection, patches, and service packs.

Payment card industry compliance

The following are the security standards to meet Payment Card Industry (PCI) compliance:

- A 256-bit Advanced Encryption Standard (AES) encryption to protect data while it is recorded, transmitted, and stored. Files related to voice and screen captures are stored in an encrypted form so that only users with proper access to the application can playback calls and view screens.
- A CRM integration API (HTTP) to mute a portion of the call recording. For example, muting segments with credit card information.
- The ability to capture audit trail information in logs and a database. For example, trails must be available of who performed the operations, what operations were performed, and when the operations were performed. The information captured in this database provides the ability to generate audit trail reports on user activity, such as who played recorded calls, how many times, data deletes, and data updates.
- The ability to modify the storage folder structure to include client alias, which sets different archival cycles and provides folder-level security across multiple clients.
- Tight integration and synchronization with Active Directory for user settings and single sign-on authentication.

Password policy

Every customer must create a password policy for their users. Administrators define a set of rules to maintain system security. The policies include rules for the following:

- Password syntax: The length and syntax of the password.

- Password history: The number of unique passwords required before reusing an old one.
- Password expiration and lockout: The validity, warning, and grace period for expiration and lockout rules.

Role-based access control

You can use roles to improve security and administration. Use a role-based access control application to define administrative roles for your business.

Administrators can group a set of privileges into a role to implement access control. Roles are assigned to users. The following are some roles: Agent, Supervisor, Manager, Quality Manager, and Administrator.

Data privacy

You can use the Data Management utility to handle customer data privacy requests. For example, if a customer exercises the right to access information or their right to be forgotten, the Data Management utility provides a method to act on these requests.

SAL Policy Manager

Avaya SAL Policy Manager increases security and simplifies the management of authentication policies. Customers use SAL Policy Manager to set various policies to access managed devices remotely. For example, the SAL Policy Manager comes with SSH proxy, which isolates the remote user from the connected device and prevents hosts from hopping during an SSH session.

Secure Communications using Transport Layer Security

Transport Layer Security (TLS) is a cryptographic protocol that increases computer network security. The solution supports TLS 1.0 and TLS 1.2. By default, when you deploy the solution, TLS 1.0 is configured.

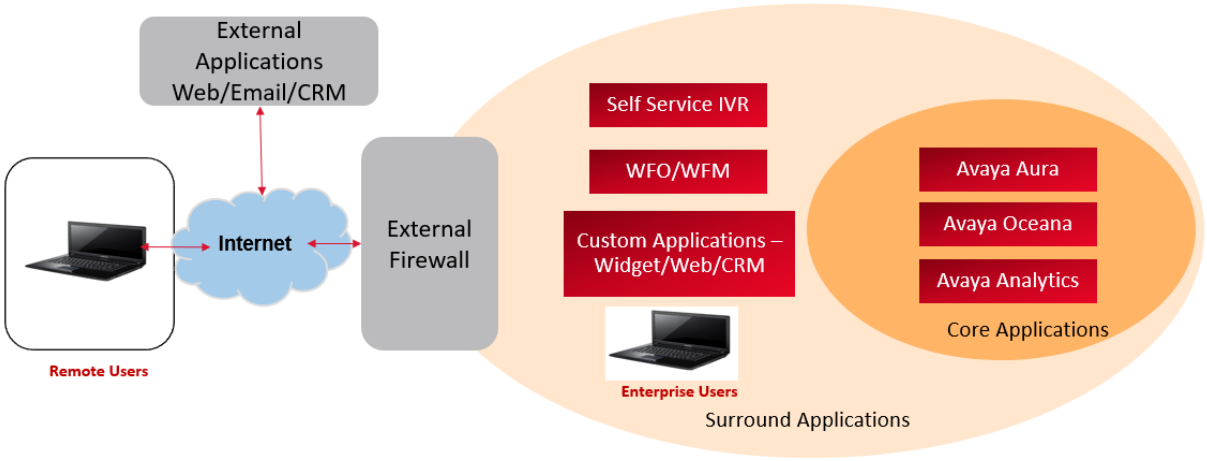
You can use the following options to change the TLS versions:

- Globally from Avaya Aura® System Manager
- Through the Cluster Editor page in the System Manager

Setting TLS is a security requirement for internal and external communications with databases and LDAP.

Overview

The core applications of the solution must be secured at the core level, followed by the clients and applications, which connect securely to the inner core, and then the security at the entire enterprise level in the internet zone and beyond.



The inner layer of the solution contains the core applications, Avaya Aura® Core, Avaya Oceana® and the Avaya Analytics™ applications. The solution is secured by enabling the security between all the core applications. The applications outside of the core interact with the core applications. Security must be enabled for all communications and data exchange between these two layers. The applications and clients on the internet must access the contact center functionality in a secure and reliable manner.

This chapter describes the types of configurations, settings, and the techniques that the customer can use to secure all the areas, starting at the core, to the internet zone at the edge of company networks.

Core Applications Security

The operations require the three core applications to communicate with each other. Avaya Oceana® uses the Avaya Aura® Suite of applications comprising Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, Application Enablement Services, and Avaya Aura® Media Server to provide the voice platform for PSTN voice contacts. Avaya Oceana® is deployed with Avaya Analytics™ as it provides the reporting platform for real time and historical data.

You can secure communications and data transfer for the core applications using:

- Secure Communications with https and wss (web socket secure)
- Token Based Authorization
- TLS 1.2
- FQDNs
- A root CA certificate in conjunction with Identity Certificates to deliver a Server Authentication Model

Avaya Oceana® core applications are primarily Avaya Breeze® platform-based software applications called snap-ins or services. The software applications take the configuration data from configurable parameters called Attributes.

The following are examples of snap-in attributes related to security, which can be set on the Oceana Configuration Service, and automatically applied to all other Avaya Oceana® services:

- Secure Connections to Database - Default Value = True
- Toggle Secure Mode - Default Value = False (https on by default)
- Enable Tokenless Access - Default Value= False (Token required by default). All REST requests for these interfaces must contain a valid token within the request header or they are rejected.
- TLS version - Default Value = 1.2
- Enable Secure Communications - Default Value = True
- Authorization Required to Contact Service - Default Value = True
- Authorization Required for Service - Default Value = True

For all these attributes except the **Enable Tokenless Access** attribute, a value of `True` specifies that the web communications into these snap-ins are secure and also use token-based authorization. However, for enhanced security, Avaya recommends that all customers use the combination of Fully Qualified Domain Name (FQDN) and Domain Name Server (DNS) in conjunction with security certificates for all interfaces accessible in the solution. Avaya Oceana® Breeze Clusters must use an FQDN. After you configure all applications in the solution for security, all clients and applications can securely communicate with Avaya Oceana® and Avaya Analytics™.

Certificate Authority (CA)

A Certificate Authority (CA) is a trusted entity that issues digital certificates and public-private key pairs. A CA verifies the identity of an individual or organization before issuing a digital certificate. A CA can be an external (public) or internal (private) entity configured inside an enterprise network. A Certificate Authority is a critical security service in a network.

Every Avaya Oceana® deployment has an Avaya Aura® System Manager deployed, and one of its functions is that of a CA. You can use System Manager's CA to secure the communications between the Avaya Aura® components, Avaya Oceana®, Avaya Breeze® platform, Avaya Analytics™ components, and all the other surrounding components in the solution.

Customers can implement a solution with their own Enterprise CA, either replacing System Manager as the CA or using it as a sub CA. Before attempting to make certificate changes in the deployed solution, you must have a solution level view to understand which network elements are affected. This requires planning and network audits before deploying new certificates.

A certificate change goes through the following four stages:

- Assessment: Identify and scope the migration work for your network.
- Planning: Plan and schedule the migration tasks.
- Migration: The actual migration which includes software upgrades, Trust Certificates deployment, and Identity Certificate deployment.
- Post-migration: Ongoing audits to avoid certificate expiration.

For public or private CA, the procedures for enabling security and applying the required certificates are almost identical. If you are using a third-party public CA, a third-party vendor certificates require time to be made available and the customer to work with the third-party to

obtain the certificates after the correct information about their system is provided. When using third-party CA, configure client authentication and server authentication on the CA for Avaya Analytics™ configuration to work.

Using System Manager as a Root CA means the end customer can perform the certificate creation process themselves. For more details on System Manager as a CA, see the Avaya Aura® System Manager documentation suite.

Operating Systems

The solution comprises different Operating Systems (OS), such as Linux, Windows, and Windows server hosting the EDM Context Store database. There are different procedures for each OS type.

Omnichannel Database Server is one of the Windows-based OS applications in the core suite of products. This server runs the Omnichannel Database software, including the database that contains the digital channel media history information with the configuration items for digital channels.

For security, Avaya provides the following guidance and configuration instructions for this server:

- Secure Remote Access
- Antivirus Software Scanning Guidelines
- Firewall Guidelines

The other Windows-based server in the core solution is Avaya Control Manager. For more information about security guidelines and recommended security practices, see the respective product documentation. Communications from the Avaya Control Manager Server to the Avaya Oceana® component, Unified Contact Center Administration (UCA), are fully secured using https and token-based authorization.

Avaya Analytics™ is a core application suite on the core solution, running Linux-based OS application servers in a Kubernetes environment hosted on VMware.

Surround Applications and Client Security

Apart from the core applications, many optional surround applications communicate with the Avaya Oceana® and Avaya Analytics™ components. Different clients must interact and share information with the core components. Communications and information transport from these applications and clients must also be secured. Communications and data traffic from surrounding applications such as the IVR platform, the Avaya Experience Platform™ (Public Cloud Workforce Engagement) platform, and other value-added applications can all be secured using https, token-based authorization, and secure certificates. Avaya Oceana® and Avaya Analytics™ users use active directory/LDAP authentication with authorization tokens to secure sessions from the clients to the core applications.

Avaya Oceana® and Avaya Analytics™ users access their functionality through supported browsers. With a secure deployment, all communications from these clients are over https and trusted browser sessions.

These communications are within the contact center enterprise boundaries protected by the IT security infrastructure, such as firewalls. However, all contact centers must open their infrastructure to the outside Internet world securely if they are to provide contact center services to their end customers, which is the final layer of the solution.

EASG-based authentication of Web Administrative Interfaces for Avaya Oceana®

EASG overview

Enhanced Access Security Gateway (EASG) is a challenge-response authentication and authorization solution that service engineers can use to access Web-based applications of Avaya Oceana®. Avaya service engineers can access these applications without redirection to Avaya Breeze® Authorization Service or System Manager (SMGR).

EASG configuration

EASG is already configured with SMGR and SSH-Login. You need to install Avaya Breeze platform with EASG enabled option.

EASG supports the following login IDs: `craft`, `init`, `inads`, and `sroot`.

Prerequisites for EASG authentication

- You should be able to log in to Avaya Oceana® Oceana Manager and DataViewer.
- Authentication implementation must be compatible with Avaya SAL Policy Manager, which is based on point-to-point access to the end systems.

Using EASG to access applications

Application	Access Procedure
SMGR	You can enable or disable EASG authorization in SMGR. In the EASG authentication config section, you can select **true** or **false** in the **Effective Value** column to enable or disable EASG Authentication. You can disable EASG authorization only for Oceana Manager and Oceana DataViewer. 1. Use the appropriate URL to open the SMGR login page. For example: `https://{SMGR_FQDN}/services` 2. In the **Username** field, type `init` or `craft` and then click **Next**. 3. Copy the Product ID, Login Name, and Challenge one by one to the corresponding fields on the EASG Web Mobile Response page. 4. Click **Query** to generate the Response token. 5. Click **Copy Response to Clipboard** to copy the Response token. 6. Go back to the SMGR login page to enter the token in the **Response** field. 7. Click **Login** to successfully log in to SMGR.

Table continues…

Application	Access Procedure
OceanaMonitor	1. Use the appropriate URL to open the OceanaMonitor login page. For example: `https://{cluster_fqdn}/services/OceanaMonitorService/services-login.html` 2. In the **Username** field, type one of the following login names: `init`, `inads`, `sroot`, or `craft`. Then click **Next**. 3. Copy the Product ID, Login Name, and Challenge one by one to the corresponding fields on the EASG Web Mobile Response page. 4. Click **Query** to generate the Response token. 5. Click **Copy Response to Clipboard** to copy the Response token. 6. Go back to the OceanaMonitor login page to enter the token in the **Response** field. 7. Click **Login** to successfully log in to OceanaMonitor.
Oceana DataViewer	1. Use the appropriate URL to open the DataViewer login page. For example: `https://{Cluster_OCP_FQDN}/services/OceanaDataViewer/easgLogin.jsp` 2. In the **Username** field, type one of the following login names: `init`, `inads`, `sroot`, or `craft`. Then click **Next**. 3. Copy the Product ID, Login Name, and Challenge one by one to the corresponding fields on the EASG Web Mobile Response page. 4. Click **Query** to generate the Response token. 5. Click **Copy Response to Clipboard** to copy the Response token. 6. Go back to the DataViewer login page to enter the token in the **Response** field. 7. Click **Login** to successfully log in to DataViewer.

Limitations

- You should have access to EASG Web Mobile.
- You must know the full URL path of the EASG login page.

Beyond the Enterprise Applications Security

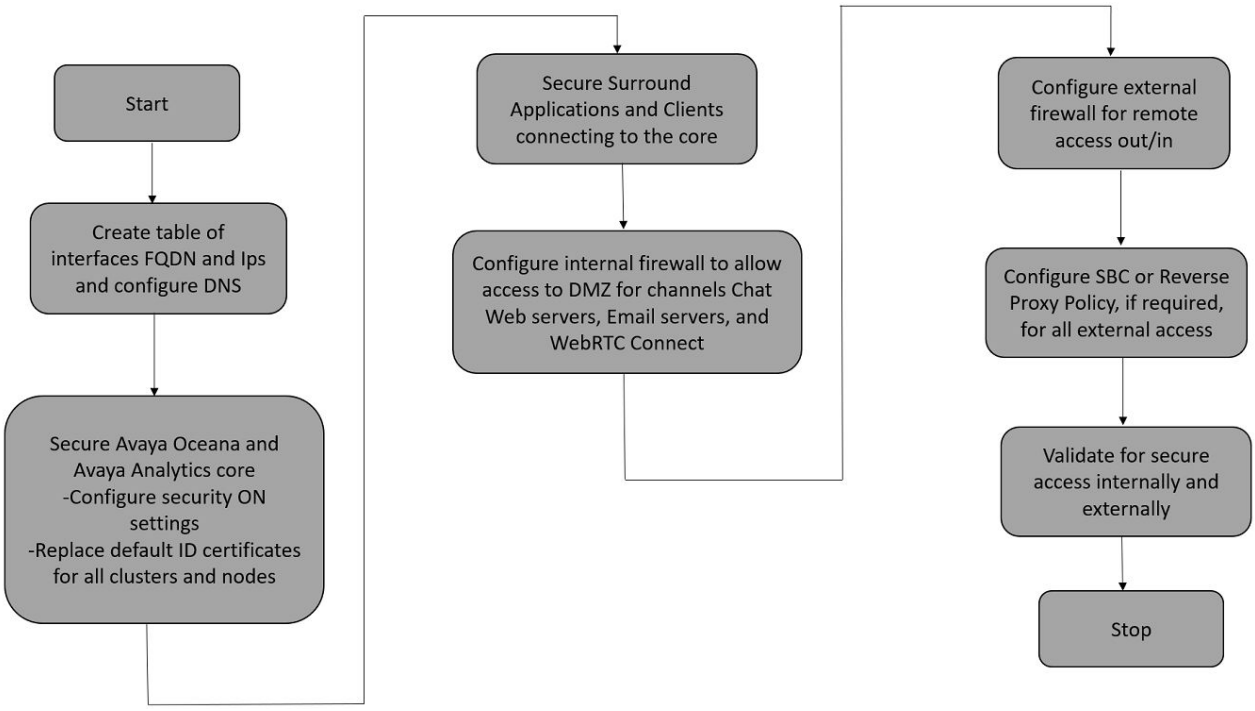
All Avaya Oceana® and Avaya Analytics™ deployments must be accessible to the Internet world. This access cannot be direct, but is allowed and made available in a secure manner through various security specific applications.

The following are examples of external access that are required for Avaya Oceana® and Avaya Analytics™ deployments:

- Avaya Oceana® Chat and Messaging customers require their communications to be securely routed in and out of the Avaya Oceana® core and surround applications including users' desktops and browser. Avaya Workspaces users require Internet access for messaging.
- Avaya Oceana® Email contacts require routing in and out of the Avaya Oceana® Email processing engine and its agent desktop client.
- Avaya WebRTC Connect customers using either voice and/or Video require their communications to be securely routed in and out of the Avaya Oceana® core and surround applications including users' desktop and browser.
- Other supported channels like SMS, Social and Generic, all require access from the Internet world in and out of the enterprise deployment.
- Remote users require secure access to all the functionality available inside the enterprise when they are working remotely.

Secure Solution Deployment

The flow chart displays the order in which Avaya Oceana® and the Avaya Analytics™ solution must be rolled out in a secure manner.

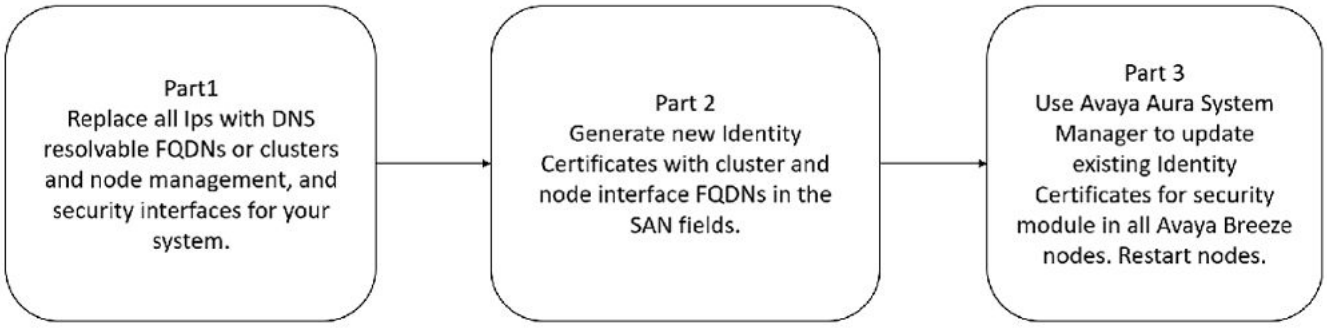


How to replace Default Breeze Node Identity Certificates

Overview

This section describes a method to replace the default Identity Certificates in both Avaya Oceana® and Avaya Analytics™. This section also describes how to create Identity Certificates using the System Manager built-in Certificate Authority.

A summary of the process outlined is captured in the following flow chart.



Avaya Oceana® Cluster Identity Certificate requirements

Avaya Oceana® is mostly built on the Avaya Breeze® platform. For enhanced security, Avaya provides the ability to add or replace Trust and Identity Certificates. Identity Certificates are

administered individually for Avaya clusters. Five default Identity Certificates are generated as part of the Avaya OVA deployment process. You can replace a default certificate with a certificate from a well-known Certificate Authority (CA).

The Security Module HTTPS certificate is visible to applications and endpoints. If you are using HTTPS with hostname validation checks, you must replace the default HTTP certificate. There are many ways of generating Identity Certificates for Avaya Oceana®. This section describes one of the methods of creating an Identity Certificate for each Avaya Oceana® cluster. The Identity Certificate for each cluster must include the following in the Subject Alternative Name (SAN) fields:

- Cluster FQDN
- Management FQDN for each node in the cluster
- SIP FQDN for each node in the cluster

The entities that access Avaya through HTTPS must resolve the Common Name (CN) and SAN fields in the certificate with the FQDNs of the Avaya node. To resolve the certificate CN or SAN fields, enter the Management FQDN and SIP FQDN of each Avaya node in your DNS server. Also enter the Cluster FQDNs in your DNS server. In a cluster with a single node, the cluster FQDN is the SIP FQDN of the one node in the cluster.

Avaya Oceana® Cluster 1 – Identity Certificate Request

Note:

In customer production deployments, where the security and management interfaces are in separate subnets, there can only be 4 DNS entries for cluster 1 – cluster FQDN + 3 Management FQDNs for 3 nodes. A second separate certificate has 4 DNS for cluster 1 – cluster FQDN + 3 Security FQDNs for 3 nodes.

The Avaya Oceana® Cluster 1 certificate includes the following:

- CN Common Name = Avaya Oceana® Cluster 1 FQDN
- SAN DNS Name = Avaya Oceana® Cluster 1 Node 1 Management FQDN
- SAN DNS Name = Avaya Oceana® Cluster 1 Node 1 SIP FQDN
- SAN DNS Name = Avaya Oceana® Cluster 1 Node 2 Management FQDN
- SAN DNS Name = Avaya Oceana® Cluster 1 Node 2 SIP FQDN
- SAN DNS Name = Avaya Oceana® Cluster 1 Node 3 Management FQDN
- SAN DNS Name = Avaya Oceana® Cluster 1 Node 3 SIP FQDN

Avaya Oceana® Cluster 2 – Identity Certificate Request

Note:

In customer production deployments, where the security and management interfaces are in separate subnets, there can only be 3 DNS entries for cluster 2 – cluster FQDN + 2 Management FQDNs for 2 nodes. A second separate certificate has 3 DNS also for cluster 2 – cluster FQDN + 2 Security FQDNs for 3 nodes.

The Avaya Oceana® Cluster 2 certificate includes the following:

- CN Common Name = Avaya Oceana® Cluster 2 FQDN
- SAN DNS Name = Avaya Oceana® Cluster 2 Node 1 Management FQDN

- SAN DNS Name = Avaya Oceana® Cluster 2 Node 1 SIP FQDN
- SAN DNS Name = Avaya Oceana® Cluster 2 Node 2 Management FQDN
- SAN DNS Name = Avaya Oceana® Cluster 2 Node 2 SIP FQDN

Avaya Oceana® Cluster 3 – Identity Certificate Request

Note:

In customer production deployments, where the security and management interfaces are in separate subnets, there can only be 3 DNS entries for cluster 3 – cluster FQDN + 2 Management FQDNs for 2 nodes. A second separate certificate has 3 DNS also for cluster 3 – cluster FQDN + 2 Security FQDNs for 3 nodes.

The Avaya Oceana® Cluster 3 certificate includes the following:

- CN Common Name = Avaya Oceana® Cluster 3 FQDN
- SAN DNS Name = Avaya Oceana® Cluster 3 Node 1 Management FQDN
- SAN DNS Name = Avaya Oceana® Cluster 3 Node 1 SIP FQDN
- SAN DNS Name = Avaya Oceana® Cluster 3 Node 2 Management FQDN
- SAN DNS Name = Avaya Oceana® Cluster 3 Node 2 SIP FQDN

Modifying the End Entity Profile to support Avaya Oceana®

About this task

Avaya Oceana® certificates require more DNS entries than is supported by the default settings in Avaya Aura® System Manager. Therefore, you must edit an End Entity Profile to allow additional DNS Entries. Alternatively, you can create a new profile for Avaya Oceana®.

Procedure

1. On the Avaya Aura® System Manager Web console, click **Home** > **Services** > **Security**.
2. In the left pane, click **Certificates** > **Authority**.
3. In the **RA Functions** list, select **End Entity Profiles**.
4. Select the profile to modify.
5. Click **Edit End Entity Profile**.
6. In the **Other subject attributes** area, from the **Subject Alternate Names field** list, select **DNS Name**.
7. Click **Add**.

   Continue to add additional **DNS Name** fields to the SAN until you have a total of 7.
8. Click **Save**.

Creating and replacing default Identity Certificates for Avaya Oceana® Cluster 1

Procedure

1. On the Avaya Aura® System Manager web console, click **Home** > **Services** > **Security**.
2. In the left pane, click **Certificates** > **Authority**.
3. In the **RA Functions**, select **Add End Entity**.
4. In the **End Entity Profile** field, select the profile you modified or created earlier.
5. Type a **Username** and **Password** for Avaya Oceana® Cluster 1 and confirm the password.

   Note the user name and password. These are required when creating the certificate.
6. In the **CN Common Name** field, enter the FQDN of Avaya Oceana® Cluster 1.
7. In the **Subject Alternative Name** area, in the first **DNS Name** field, enter the FQDN of Avaya Oceana® Cluster 1.
8. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 1 Node 1 Management FQDN.
9. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 1 Node 1 SIP FQDN.
10. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 1 Node 2 Management FQDN.
11. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 1 Node 2 SIP FQDN.
12. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 1 Node 3 Management FQDN.
13. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 1 Node 3 SIP FQDN.
14. From the **Token** list, select **P12 file**.
15. Click **Add**.
16. Select **Public Web**.
17. Click **Create Keystore**.
18. Enter the **Username** and **Password** for Avaya Oceana® Cluster 1.
19. From the **Key Length** list, select **2048** or higher.
20. Click **Enroll**.

    The p12 certificate downloads to your **Downloads** folder.
21. On the Avaya Aura® System Manager Web console, click **Services** > **Inventory**.
22. In the left navigation pane, click **Manage Elements**.
23. On the **Manage Elements** page, select an Avaya Oceana® Cluster 1 server/node and click **More Actions** > **Configure Identity Certificates**.
24. On the **Identity Certificates** page, select the **Security Module HTTPS** certificate.

25. Click **Replace**.
26. On the **Replace Identity Certificate** page, select **Import third party certificate**.
27. Click **Choose File**.
28. In the **Password** field, enter the Avaya Oceana® Cluster 1 password used earlier.
29. Click **Retrieve Certificate**.

    The certificate is loaded.
30. Click **Commit**.
31. Replace the Identity Certificate for the other two nodes in Avaya Oceana® Cluster 1 using this same **P12 file**.
32. Restart all three nodes in Avaya Oceana® Cluster 1 and wait for the cluster to be fully started before setting to Acceptance State.

Creating and replacing default Identity Certificates for Avaya Oceana® Cluster 2

Procedure

1. On the Avaya Aura® System Manager web console, click **Home** > **Services** > **Security**.
2. In the left pane, click **Certificates** > **Authority**.
3. In the **RA Functions**, select **Add End Entity**.
4. In the **End Entity Profile** field, select the profile you modified or created earlier.
5. Type a **Username** and **Password** for Avaya Oceana® Cluster 2 and confirm the password.

   Note the user name and password. These are required when creating the certificate.
6. In the **CN Common Name** field, enter the FQDN of Avaya Oceana® Cluster 2.
7. In the **Subject Alternative Name** area, in the first **DNS Name** field, enter the FQDN of Avaya Oceana® Cluster 2.
8. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 2 Node 1 Management FQDN.
9. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 2 Node 1 SIP FQDN.
10. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 2 Node 2 Management FQDN.
11. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 2 Node 2 SIP FQDN.
12. From the **Token** list, select **P12 file**.
13. Click **Add**.
14. Select **Public Web**.
15. Click **Create Keystore**.

16. Enter the **Username** and **Password** for Avaya Oceana® Cluster 2.
17. From the **Key Length** list, select **2048** or higher.
18. Click **Enroll**.

    The p12 certificate downloads to your **Downloads** folder.
19. On the Avaya Aura® System Manager web console, click **Services** > **Inventory**.
20. In the left navigation pane, click **Manage Elements**.
21. On the **Manage Elements** page, select an Avaya Oceana® Cluster 2 server/node and click **More Actions** > **Configure Identity Certificates**.
22. On the **Identity Certificates** page, select the **Security Module HTTPS** certificate.
23. Click **Replace**.
24. On the **Replace Identity Certificate** page, select **Import third party certificate**.
25. Click **Choose File**.
26. In the **Password** field, enter the Avaya Oceana® Cluster 2 password used earlier.
27. Click **Retrieve Certificate**.

    The certificate is loaded.
28. Click **Commit**.
29. Replace the Identity Certificate for the other node in Avaya Oceana® Cluster 2 using this same **P12 file**.
30. Restart both nodes in Avaya Oceana® Cluster 2.

Creating and replacing default Identity Certificates for Avaya Oceana® Cluster 3

Procedure

1. On the Avaya Aura® System Manager web console, click **Home** > **Services** > **Security**.
2. In the left pane, click **Certificates** > **Authority**.
3. In the **RA Functions**, select **Add End Entity**.
4. In the **End Entity Profile** field, select the profile you modified or created earlier.
5. Type a **Username** and **Password** for Avaya Oceana® Cluster 3 and confirm the password.

   Note the user name and password. These are required when creating the certificate.
6. In the **CN Common Name** field, enter the FQDN of Avaya Oceana® Cluster 3.
7. In the **Subject Alternative Name** area, in the first **DNS Name** field, enter the FQDN of Avaya Oceana® Cluster 3.
8. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 3 Node 1 Management FQDN.

9. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 3 Node 1 SIP FQDN.
10. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 3 Node 2 Management FQDN.
11. In the next **DNS Name** field, enter the Avaya Oceana® Cluster 3 Node 2 SIP FQDN.
12. From the **Token** list, select **P12 file**.
13. Click **Add**.
14. Select **Public Web**.
15. Click **Create Keystore**.
16. Enter the **Username** and **Password** for Avaya Oceana® Cluster 3.
17. From the **Key Length** list, select **2048** or higher.
18. Click **Enroll**.

    The p12 certificate downloads to your **Downloads** folder.
19. On the Avaya Aura® System Manager web console, click **Services** > **Inventory**.
20. In the left navigation pane, click **Manage Elements**.
21. On the **Manage Elements** page, select an Avaya Oceana® Cluster 3 server/node and click **More Actions** > **Configure Identity Certificates**.
22. On the **Identity Certificates** page, select the **Security Module HTTPS** certificate.
23. Click **Replace**.
24. On the **Replace Identity Certificate** page, select **Import third party certificate**.
25. Click **Choose File**.
26. In the **Password** field, enter the Avaya Oceana® Cluster 3 password.
27. Click **Retrieve Certificate**.

    The certificate is loaded.
28. Click **Commit**.
29. Replace the Identity Certificate for the other node in Avaya Oceana® Cluster 3 using this same **P12 file**.
30. Restart both nodes in Avaya Oceana® Cluster 3.

Viewing Breeze Identity Certificate details

Procedure

1. On the Avaya Aura® System Manager web console, in **Services**, click **Inventory** > **Manage Elements**.
2. Click the check box in front of the Avaya server.
3. From the **More Actions** menu, select **Configure Identity Certificates**.

4. In the list of certificates, click the Security Module HTTPS certificate.

   The certificate details for the Security Module HTTPS certificate are displayed below the certificate list.

5. Ping each DNS entry and verify if it returns the correct IP address to ensure that all the DNS entries are resolvable.
6. Click **Done**.

User's Client Software and Platform requirements for secure connections

Avaya Oceana® and Avaya Analytics™ users require client PCs and browser clients to access the contact center functionality provided by the solution. The software client is Avaya Workspaces which is a browser-based client, with no client software download required to the user's PC.

When the user is configured as an Avaya Oceana® or Avaya Analytics™ user, with the correct permissions, the user can login and activate to perform the contact center functions and reporting tasks. An important aspect for all users, on premise in the enterprise or remote on the internet, is the ability for secure communications between the user's client PC and software, and the solution components. This can be achieved by the use of security certificates specifically importing the CA or root cert into the trust store of the user’s PC and browser.

Transport Layer Security (TLS) is an industry wide standard for encrypting data between clients (browsers) and servers (applications). This is achieved through the use of a security certificate that is trusted between the client and the server application. Key to this trust is the issuer or signing authority of the certificate more commonly referred to as the CA. The CA must be trusted by the client browser and in order to achieve this trust, the CA root certificate must be installed in the browser’s trust store.

The root certificates of a known external Certificate Authority are installed and trusted by default in most browsers. However, if for example, you are using Avaya Aura® System Manager or a private Enterprise CA, then the root or CA certificate cannot be automatically installed in the user’s browser.

Many enterprises have the ability for IT tools, policies and applications to push out the required root or CA certificates to all users' browsers or client PC trust stores. After the certificates are installed, the users are able to securely connect to their required applications without further action. However, if the certificate is not in place, the user has to accept the risk to connect insecurely to the server applications.

Clicking on the **Proceed to an application** means the user is bypassing the warning and setting up an insecure connection from their browser to the end application server. The user has to do this every time they connect to a particular backend server that has a CA issued SSL certificate.

Chapter 4: Deployment process

Work flow

This work flow shows the sequence of tasks that you must perform to deploy Avaya Oceana®.

Important:

- PSTN Voice, Web Voice, and Web Video channels share a common configuration of Communication Manager, Call Center Elite, Application Enablement Services, Avaya Control Manager, and Avaya Workspaces.
- Avaya Oceana® must have the campus Avaya Control Manager applications and its associated databases, Omnichannel Database servers, and EDM SQL server in the same physical data center as the Avaya Breeze® platform nodes.
- Avaya does not support physically locating Avaya Control Manager or Omnichannel campus applications in a different location from Avaya Breeze® platform. All must be reside in the same location.

  This requirement does not apply to a Disaster Recovery solution that has two interdependent deployments connected over a WAN.
- All Avaya Oceana®/Avaya Breeze® platform deployments rely on a highly available DNS server. Therefore, ensure that you have backup DNS server capabilities.
- Avaya Oceana® needs access to a DNS with forward and reverse lookup. You can configure forward and reverse lookup DNS entries for the Fully Qualified Domain Names (FQDNs) and IP addresses for all components within Avaya Oceana®.

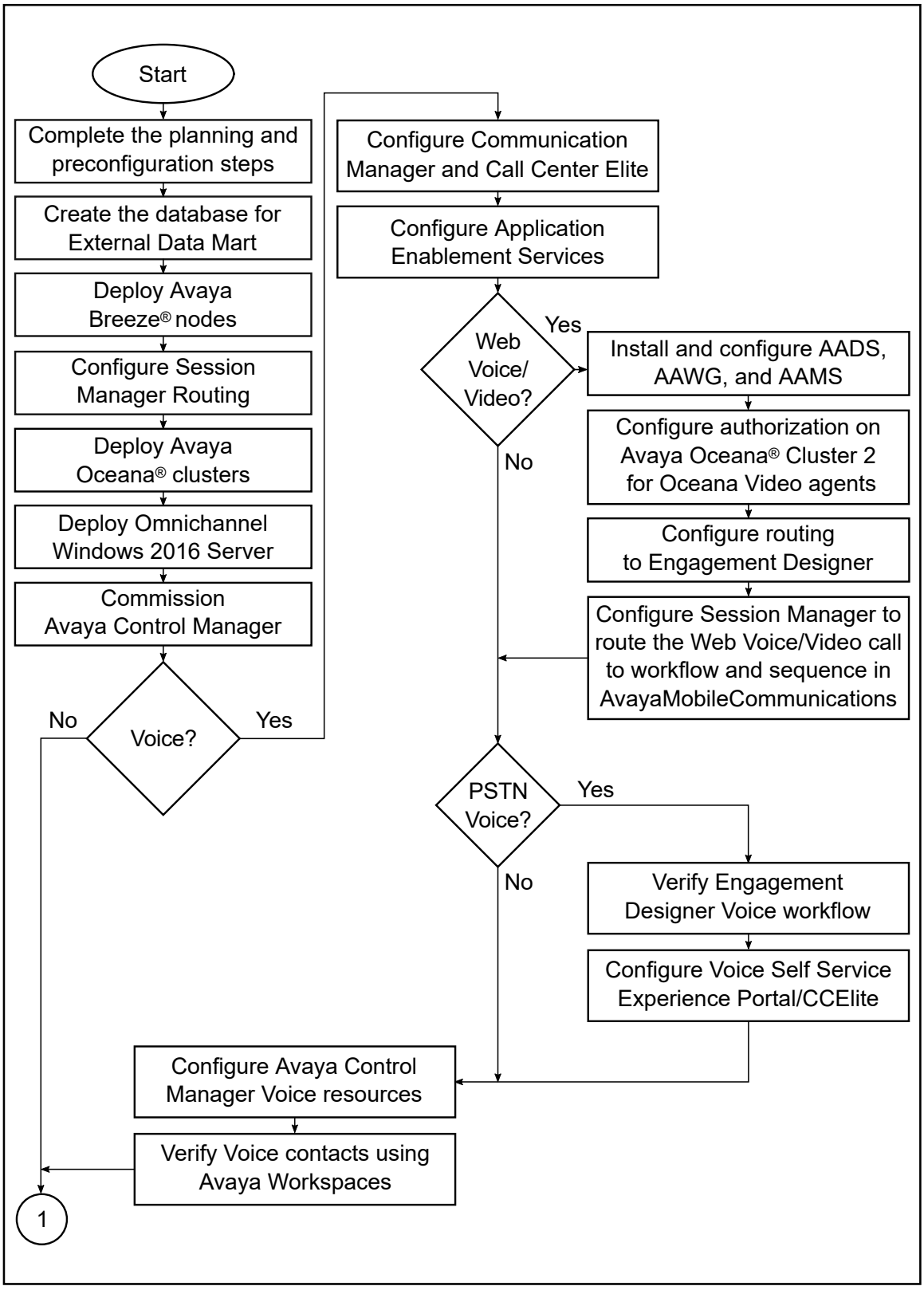
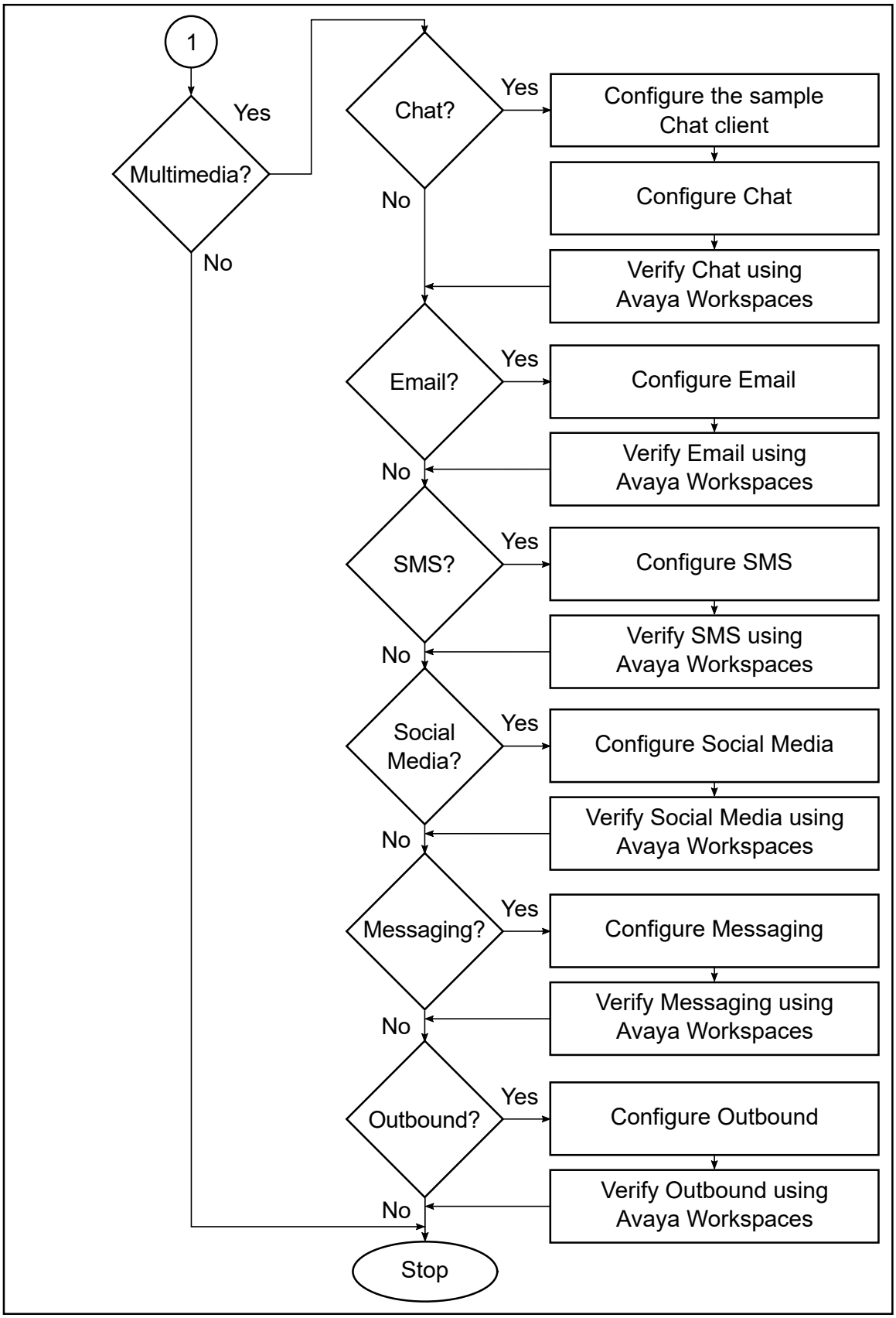


Figure 2: Deployment process


1
Multimedia?
Yes
No
Chat?
Yes
No
Configure the sample Chat client
Configure Chat
Verify Chat using Avaya Workspaces
Email?
Yes
No
Configure Email
Verify Email using Avaya Workspaces
SMS?
Yes
No
Configure SMS
Verify SMS using Avaya Workspaces
Social Media?
Yes
No
Configure Social Media
Verify Social Media using Avaya Workspaces
Messaging?
Yes
No
Configure Messaging
Verify Messaging using Avaya Workspaces
Outbound?
Yes
No
Configure Outbound
Verify Outbound using Avaya Workspaces
Stop

Chapter 5: Planning and preconfiguration

Planning and preconfiguration

This section provides information about capacities, hardware requirements, software requirements, and general planning considerations for Avaya Oceana® deployments.

Based on your solution requirements, install and commission the following components for Avaya Oceana®:

Component	Supported release
Avaya Aura® System Manager	The Compatibility Matrix provides compatibility information for the Avaya products that are supported with the various releases of Avaya Oceana®. Access the Compatibility Matrix page at https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml.
Avaya Aura® Communication Manager	
Avaya Aura® Call Center Elite	
Avaya Aura® Session Manager	
Avaya Aura® Application Enablement Services	
Avaya Experience Portal	
Avaya Control Manager	
Avaya Orchestration Designer	
Avaya Aura® Session Border Controller	
Avaya Proactive Outreach Manager	
Avaya Workforce Engagement Select	
Avaya Experience Platform™ (Public Cloud Workforce Engagement)	
Avaya Agent for Desktop	
Avaya Aura® Web Gateway	
Avaya Aura® Device Services	
Avaya Aura® Media Server	
Avaya Workplace Client	

Note:

- The solution in production requires a dedicated AES application for Avaya Workspaces for Call Center Elite or Avaya Oceana®.
- AES must not be shared with other CTI applications for Screen Pop, CRM integrations, and AWE integrations.

For the most recent information, see the individual product Release Notes available on https://support.avaya.com.

- Ensure that all your server hardware and virtualization infrastructure meet the requirements.
- Ensure that you have sufficient knowledge about the installation and configuration that you want to use in your solution.

Capacity specifications

The following table shows the capacity specifications for Avaya Oceana® when deployed on-premise:

Parameter: Maximum supported number of …	On-Premise only: Agents			
	4500	**2000**	**1000**	**100**
Active Avaya Workspaces agents (including supervisors logged in as active agents)	4500 Of this, 2000 can be digital agents.	2000	1000	100
Configured channels per Agent	4 (1 voice + 3 digital)			
Active Avaya Workspaces users including supervisors and agents (Supervisors not logged in as active agents)	4950	2200	1100	110
Configured users (agents and supervisors)	14850	6600	3300	330
Configured agents	13500	6000	3000	300
Configured supervisors	1350	600	300	30
Active supervisors using Avaya Workspaces	450	200	100	10
Active voice agents	4500	2000	1000	100
Configured Social agents	300	300	300	100
Active Social agents	300	300	300	30
Configured Outbound agents	500	300	300	10
Active Outbound agents	500	300	300	10
Concurrent Avaya Workspaces instances per agent	1	1	1	1
Concurrent Avaya Workspaces instances per supervisor	1	1	1	1
Voice Busy Hour Call Completion (BHCC) - Self Service	45000	30000	30000	3000
Voice BHCC) - Assisted Service	45000	20000	10000	1000
BHCC - Outbound	10000	6000	6000	200
Chat/Email/SMS interactions per hour	15000	15000	6000	600

Table continues…

Parameter: Maximum supported number of …	On-Premise only: Agents			
	4500	**2000**	**1000**	**100**
Chat interactions per hour Assumes no other multimedia channel is active.	15000	15000	6000	600
Messaging interactions per hour Assumes no other multimedia channel is active.	15000	15000	6000	600
Emails per hour Assumes no other multimedia channel is active.	15000	15000	6000	600
SMS per hour Assumes no other multimedia channel is active.	15000	15000	6000	600
Social per hour Assumes no other multimedia channel is active.	15000	15000	6000	600
Generic Channel per hour Assumes no other multimedia channel is active.	15000	15000	6000	600
Concurrent Web Voice sessions***	1000	1000	1000	100
Concurrent Web Video sessions***	500	500	500	50
Ad-hoc Email per agent	1	1	1	1
Deferred Email interactions	10000	6000	3000	500
Deferred Emails per agent	20	20	20	20
Observe Chat per agent	3	3	3	3
Co-Browse sessions per node	200	200	200	20
Concurrent Chat sessions	2200	2200	1100	110
Concurrent Chat sessions per customer	10	10	10	10
Total Services supported	5000	5000	5000	1000
Services supported per agent	2000	2000	2000	1000
Attributes per Service	10 Channel + 9 attributes	10 Channel + 9 attributes	10 Channel + 9 attributes	10 Channel + 9 attributes
Attributes per agent*	500	500	500	500
Queued contacts across all channels	25000	25000	10000	1000
Queued Voice contacts	8000	8000	4000	400

Table continues…

Parameter: Maximum supported number of …	On-Premise only: Agents			
	4500	**2000**	**1000**	**100**
Queued Chat contacts	2000	2000	1000	100
Queued Messaging contacts	4500	4500	2250	225
Queued Email contacts**	25000	25000	10000	1000
Queued Social contacts	5000	5000	2500	250
Queued SMS contacts	2200	2200	1100	110
Queued Generic Channel contacts	10000	10000	3000	200
Avaya WebRTC Connect agents	1000	1000	1000	100
Concurrent Chatbot sessions with two Chatbot servers	900	900	900	150
Number of Communication Managers	One of the following: • 1 CM/CCElite Simplex • 1 CM/CCElite Duplex • 1 CM/CCElite Simplex or Duplex with associated ESS			
Transfer to Service operations	2000			
Engagement Designer Workflow Instances (WFIs) per cluster	25000	25000	10000	1000
Engagement Designer Workflow Definitions (WFDs) per cluster	200			
Contacts allowed on the OCP database	7 million			
Digital contacts per customer	700			
Public real-time views an administrator can create and view	60			
Private real-time views a supervisor can create and view	60			
Public dashboards an administrator can create	10			
Private dashboards a supervisor can create	10			

Table continues…

Parameter: Maximum supported number of …	On-Premise only: Agents			
	4500	2000	1000	100
Notes: * The total number of attributes is 50 times the maximum number of configured users. For example, in a 2000-agent deployment, the maximum number of configured users is 6600. Therefore, you can configure a total of 6600*50 attributes. **Queued emails - Emails that arrive at the contact center but are not yet closed. These include active emails that agents are currently processing, emails in deferred state, and emails that are awaiting agent's availability. *** To calculate the maximum supported sessions for a mixed Web Voice and Web Video environment, 1 Web Video session is equivalent to 2 Web Voice sessions. For example, a large profile system can support one of the following: • maximum 1000 Web Voice • maximum 500 Web Video • maximum 500 Web Voice and 250 Web Video Ensure that your solution is engineered correctly to support the required WebRTC session counts.				

Hardware and software specifications

Avaya Oceana® is a suite of software applications comprising of a set of Avaya Breeze® platform Snap-Ins and additional installation software. Avaya Oceana® is deployed on virtualized platforms utilizing VMware ESXi. This deployment in turn is deployed on actual physical hosts. Each Avaya Breeze® platform server instance on the host virtual machine must be allocated the reserved memory and vCPU configuration.

Supported virtualized environments

The customer and the external integrator must supply all virtualization software and hardware to host the virtualized deployment. Avaya recommends that the Avaya Breeze® platform installation, which is part of a single cluster, must be hosted on different VMware ESXi hosts. This guarantees service availability and ensures high availability of the solution even if one of the VMware ESXi hosts is unavailable.

All solution applications that are part of the Avaya Oceana® suite require the following virtualized environments:

VMware ESXi	Avaya Oceana®	Avaya Control Manager	Avaya Analytics™
VMware ESXi 7.0	Yes	Yes	Yes
VMware ESXi 8.0	Yes	Yes	Yes
Citrix/Xenapp 7.6	Yes	Yes	Yes

Supported operating systems

All operating systems that Avaya Oceana® requires must be provided by the end customer where it is not explicitly provided by Avaya.

Operating system	Avaya Oceana®
Red Hat Enterprise Linux 8.8	Avaya Breeze® platform
Red Hat Enterprise Linux 8.x	Avaya Analytics™
Microsoft Windows 10 and Windows 11 (x32 and x64)	Avaya Workspaces
Apple Mac OS 10.11+	Avaya Workspaces
Microsoft Windows Server 2012, 2016, and 2019 (Standard and Enterprise) with SQL Server 2012, 2014, and 2016 (Standard and Enterprise).	Avaya Control Manager
Microsoft Windows Server 2019	OCP database External Data Mart (EDM) database

Note:

- Red Hat Enterprise Linux for Avaya Breeze® platform is provided by Avaya.
- Red Hat Enterprise Linux for Common Services is provided by Avaya.

Supported browsers

Component	Microsoft Edge Chromium	Google Chrome (Windows and Apple MAC)	Mozilla	
			Firefox Standard	Firefox Enterprise
Avaya Workspaces for Avaya Oceana® • Supervisor and agent role Avaya Workspaces admin role • Customer Journey • Co-Browsing Snap-in agent role	144, 145	144, 145, 146	147, 148	140.8
Co-Browsing Snap-in customer	145	145, 146	148	140.8
Avaya Control Manager	145	145, 146	148	Not supported
Avaya Workspaces for Avaya Oceana® — Avaya WebRTC Connect Voice and Video agent	145 Video: Not supported Voice: supported	146	148	Not supported
Customer Avaya WebRTC Connect application	145 Video: Not supported Voice: supported	146	148	Not supported
Avaya Analytics™ Release 4.x Real Time Reporting (using supervisor Avaya Workspaces for Avaya Oceana®)	144, 145	145, 146	147, 148	140.8

Table continues…

Component	Microsoft Edge Chromium	Google Chrome (Windows and Apple MAC)	Mozilla	
			Firefox Standard	Firefox Enterprise
Avaya Analytics™ Release 4.x Historical Reporting	144, 145	145, 146	147, 148	140.8
Avaya Oceana® Multimedia Data Viewer & Avaya Oceana® Dashboard & Monitor	144, 145	145, 146	148	Not supported
Avaya Oceana® Administration Tool and OCMT	144, 145	145, 146 with Click Once Extension	148 with Click Once Extension	Not supported

Supported endpoints

In addition to Avaya Workspaces for Windows, Avaya Oceana® supports the following endpoints:

Avaya endpoint/softphone	Supported versions
9600 Series IP Deskphone 96x1 (SIP)	9608, 9611, 9621, and 9641
9600 Series IP Deskphone 96x1 (H.323)	9650, 9608, and 9611
16xx series IP deskphone	1608 and 1611
46xx series IP deskphone	4620 and 4621
J100 Series	J169 and J179
Avaya one-X® Agent (H.323)	2.5.8 and later
Avaya Agent for Desktop	1.7.x, 2.0

Supported mobile and desktop operating systems

Avaya WebRTC Connect supports the following mobile and desktop operating systems:

Platforms	Supported versions
iOS	13.4.1
Android	10.0
Windows	Windows 10 Pro and Windows 10 Pro for Workstations 64-bit OS
Mac OS	11.2.3

Supported WebRTC Agent Client Software Versions

Platforms	Supported versions
Google Chrome	89

Avaya Oceana® hardware requirements

The following table provides information about the memory, disk, and vCPU requirements for each component of Avaya Oceana®:

Component/ Platform	Requirement	Avaya Oceana® Agents					
		4500	2000	1000	500	250	100
Avaya Oceana® Cluster 1 Avaya Breeze® platform	Nodes	3	3	3	3	3	3
	Memory/node	98GB	98GB	66GB	50GB	50GB	34GB
	Minimum disk size/node	505GB	505GB	505GB	505GB	505GB	505GB
	vCPUs/node	16	12	12	8	8	8
	Input Output Processing / sec (IOPs)	120	100	100	50	50	50
Avaya Oceana® Cluster 2 Avaya Breeze® platform	Nodes	2	2	2	2	2	–
	Memory/node	34GB	34GB	26GB	26GB	18GB**	–
	Minimum disk size/node	355GB	355GB	355GB	355GB	355GB	–
	vCPUs/node	8	8	4	4	4	–
	IOPs	50	50	50	25	25	–
Avaya Oceana® Cluster 3 Avaya Breeze® platform	Nodes	2	2	2	2	2	2
	Memory/node	34GB	34GB	18GB	18GB	18GB	14GB
	Minimum disk size/node	405GB	405GB	405GB	405GB	405GB	405GB
	vCPUs/node	8	8	4	4	4	4
	IOPs	50	50	50	25	50	50
Avaya Oceana® Cluster 4 (Optional) Avaya Breeze® platform	Nodes	3	3	2	2	2	2
	Memory/node	18GB	18GB	18GB	18GB	18GB	10GB
	Minimum disk size/node	405GB	405GB	405GB	405GB	405GB	105GB
	vCPUs/node	4	4	4	4	4	4
	IOPs	50	50	50	25	25	25
Avaya Oceana® Cluster 5 (Optional) Avaya Breeze® platform	Nodes	2	2	2	2	2	2
	Memory/node	14GB	14GB	14GB	14GB	14GB	10GB
	Minimum disk size/node	305GB	305GB	305GB	305GB	305GB	305GB
	vCPUs/node	4	4	4	4	4	4
	IOPs	50	50	50	50	50	50
Omnichannel Datastore Windows	Nodes	2	2	2	2	2	2
	Memory/node	16GB	16GB	16GB	16GB	16GB	12GB

Table continues…

Component/ Platform	Requirement	Avaya Oceana® Agents					
		4500	2000	1000	500	250	100
	Minimum disk size/node	4 Disks (100GB, 60GB, 1TB, and 60GB)	4 Disks (100GB, 60GB, 1TB, and 60GB)	4 Disks (100GB, 60GB, 1TB, and 60GB)	4 Disks (100GB, 60GB, 100GB, and 60GB)	4 Disks (100GB, 60GB, 100GB, and 60GB)	4 Disks (100GB, 60GB, 100GB, and 60GB)
	vCPUs/node	8	8	4	4	4	4
	IOPs	100	100	100	50	50	50
Avaya Control Manager Windows	Nodes	2	2	2	2	2	2
	Memory/node	12GB	12GB	12GB	12GB	12GB	12GB
	Minimum disk size/node	300GB	300GB	300GB	300GB	300GB	300GB
	vCPUs/node	8	8	8	8	8	8
	IOPs	50	50	50	25	25	25
Avaya Control Manager Database Windows	Nodes	2	2	2	2	2	2
	Memory/node	12GB	12GB	12GB	12GB	12GB	12GB
	Minimum disk size/node	300GB	300GB	300GB	300GB	300GB	300GB
	vCPUs/node	8	8	8	8	8	8
	IOPs	50	50	50	25	25	25
Avaya Context Store External Data Mart and Customer Journey Database Windows	Nodes	1	1	1	1	1	1
	Memory/node	24GB	16GB	16GB	16GB	16GB	12GB
	Minimum disk size/node	3200GB	2105GB	2105GB	2105GB	2105GB	215GB
	vCPUs/node	12	8	8	8	8	4
	IOPs	100	100	100	50	50	50
Avaya Control Manager Database co-resident with Avaya Context Store External Data Mart (EDM) and Customer Journey Database Windows	Nodes	2	2	2	2	2	2
	Memory/node	24GB	24GB	24GB	24GB	24GB	24GB
	Minimum disk size/node	3500GB	2405GB	2405GB	2405GB	2405GB	515GB
	vCPUs/node	12	12	12	12	12	12
	IOPs	750	750	750	750	750	750

Table continues…

Component/ Platform	Requirement	Avaya Oceana® Agents					
		4500	2000	1000	500	250	100
Avaya Aura® Web Gateway (Optional) RHEL	Nodes	2	2	2	2	2	2
	Memory/node	8GB	8GB	8GB	8GB	6GB	6GB
	Minimum disk size/node	132GB	132GB	132GB	132GB	132GB	132GB
	vCPUs/node	8	8	8	8	4	4
	IOPs	100	100	100	100	100	100
Avaya Aura® Device Services (Optional) RHEL	Nodes	2	2	2	2	2	2
	Memory/node	9GB	9GB	9GB	9GB	9GB	9GB
	Minimum disk size/node	250GB	250GB	250GB	250GB	250GB	250GB
	vCPUs/node	6	6	6	6	6	6
	IOPs	100	100	100	100	100	100
Avaya Aura® Media Server (Avaya Aura® Web Gateway) (Optional) RHEL	Nodes	3*	3*	3*	2	2	2
	Memory/node	16GB	16GB	16GB	16GB	8GB	8GB
	Minimum disk size/node	50GB	50GB	50GB	50GB	50GB	50GB
	vCPUs/node	16	16	16	16	8	8
	IOPs	100	100	100	100	100	100
Avaya Aura® Media Server (Avaya Breeze® platform) (Optional) RHEL	Nodes	2	2	2	2	2	2
	Memory/node	8GB	8GB	8GB	8GB	8GB	8GB
	Minimum disk size/node	50GB	50GB	50GB	50GB	50GB	50GB
	vCPUs/node	8	8	8	8	8	8
	IOPs	100	100	100	100	100	100
Avaya Aura® Session Border Controller (Optional) RHEL	Nodes	2	2	2	2	2	2
	Memory/node	16GB	16GB	16GB	16GB	16GB	16GB
	Minimum disk size/node	100GB	100GB	100GB	100GB	100GB	100GB
	vCPUs/node	6	6	6	6	6	6
**For 250 Avaya WebRTC Connect agents, Avaya Oceana® Cluster 2 requires at least 24 GB RAM to support the Avaya Mobile Video Snap-in and Avaya BotConnector Snap-in Avaya WebRTC Connect services. * For 1000 Avaya WebRTC Connect agents, you must have 3 Avaya Aura® Media Server nodes.							

Note:

- Each Avaya Breeze® platform node of a cluster must reside on a different physical server.
- For Red Hat Enterprise Linux (RHEL), Avaya Oceana® only supports the version that Avaya ships with the solution.

- For new deployments, Avaya Oceana® only supports the External Data Mart database running Microsoft SQL Server on a supported version of Windows Operating System.

  For supported version combinations, see the following:

  - SQL Server 2019: https://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server-ver15?view=sql-server-ver15.
  - SQL Server 2016 and 2017: https://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server?view=sql-server-ver15.

- For Avaya WebRTC Connect:
  - Avaya Aura® Web Gateway OVA Profile = medium
  - Avaya Aura® Device Services OVA Profile = 1
  - Avaya Aura® Media Server (Avaya Aura® Web Gateway) OVA Profile = 5
  - Avaya Aura® Media Server (Avaya Breeze® platform) OVA Profile = 3

  For High Availability (HA) deployments, you must have two instances of each of these WebRTC Connect components.

- Drive F of Omnichannel Datastore requires engineering based on the email and chat/SMS profiles of the customer.
- Avaya recommends two dedicated standalone Application Enablement Services (AES) servers for all Avaya Oceana® deployments to ensure AES High Availability in the solution. Currently, Avaya Oceana® does not support AES GRHA.
- For co-resident deployment of Avaya Control Manager and External Data Mart (EDM) databases, the minimum disk size/node includes the amount of disk space required to store one year of EDM Data and does not include the disk space required for SQL transaction logs or database backups. Therefore, you must create an appropriate SQL Server Agent Job or Maintenance Plan to prevent the transaction log from growing rapidly.

  For more information about maintenance plans, see https://docs.microsoft.com/en-us/sql/relational-databases/maintenance-plans/maintenanceplans?view=sql-server-2016 and select the appropriate version of SQL Server. Also, if you migrate EDM data from a source EDM to the co-resident Microsoft SQL server, ensure that you add sufficient disk space to accommodate the data.

- Avaya Oceana® 3.10.0.1 deployment requires an addition of 2 GB RAM and 5 GB hard disk for each node. Avaya Breeze® platform Supports VMware/ESXi 7.x and VMware/ESXi 8.x

Virtual Machine requirements

The section describes the minimum number of nodes that must be provisioned for the deployment of Avaya Oceana®. Each Avaya Breeze® platform node on the host virtual machine must be allocated with the reserved RAM and CPU configuration.

Component	Number of nodes for Avaya Oceana® 4500 Agents	Number of nodes for Avaya Oceana® 2000 Agents	Number of nodes for Avaya Oceana® 1000 Agents	Number of nodes for Avaya Oceana® 500 Agents	Number of nodes for Avaya Oceana® 250 Agents	Number of nodes for Avaya Oceana® 100 Agents
Avaya Oceana® Cluster 1	3	3	3	3	3	3
Avaya Oceana® Cluster 2	2	2	2	2	2	0
Avaya Oceana® Cluster 3	2	2	2	2	2	2
Avaya Oceana® Cluster 4 (Optional)	3	3	2	2	2	2
Avaya Oceana® Cluster 5 (Optional)	2	2	2	2	2	2

Note:

For Avaya Oceana® deployments that support up to 100 agents, install the CRMGateway SVAR on Avaya Oceana® Cluster 3.

ESXi hosts configuration

The following table lists the configuration of the ESXi hosts for Avaya Breeze® platform nodes:

Processor	[Dual CPU] Intel Xeon E5-2697 v3 @ 2.60GHz
Network Interface	Network Interface Controller (NIC)
Disk type and speed	SATA, SSD, Minimum 15000 RPM

Virtual resource allocation in vSphere

Avaya Oceana® virtual machine RAM requirements

Full RAM reservations must be implemented for all Avaya Oceana® / Avaya Breeze® platform nodes and the Omnichannel Windows server running on the customer-provided VMware hardware and software infrastructure. See the product documentation for Avaya Control Manager and Avaya Aura® for guidelines on memory reservations for those products that form part of Avaya Oceana®.

For Avaya Pod Fx deployments, RAM reservations are not required as this platform is engineered by Avaya for maximum supported capacities in terms of memory requirements.

- The VMware reservation on memory must match the memory requirement of the virtual machine for Avaya Breeze® platform nodes and the Omnichannel Windows server.

Avaya Oceana® virtual machine CPU requirements

Full vCPU reservations must be implemented for all Avaya Oceana® / Avaya Breeze® platform nodes and the Omnichannel Windows server running on the customer-provided VMware hardware and software infrastructure. See the product documentation for Avaya Control Manager and Avaya Aura® for guidelines on vCPU reservations for those products that form part of Avaya Oceana®.

For Avaya Pod Fx deployments, vCPU reservations are not required as this platform is engineered by Avaya for maximum supported capacities in terms of vCPU requirements.

- Hyperthreading support is not available on any Avaya Oceana® / Avaya Breeze® platform nodes as vCPU reservations are required.
- CPU reservations are calculated in terms of processor cycles MHz/GHz. See the VMware documentation for calculations of total processor cycles for a given number of vCPUs.
- When selecting the distribution of cores per socket for each virtual machine, use the VMware-provided defaults. For example, for 8 vCPUs, VMware sets by default a flat and wide selection of 1 core per socket across 8 sockets.
- Ensure that you deploy the same physical CPU type across all Avaya Oceana® / Avaya Breeze® platform clusters. Mixing of CPU types is not supported on the different physical hosts running Avaya Oceana® / Avaya Breeze® platform virtual machines.
- The VMware reservation on CPU must match the number of vCPU assigned to the virtual machine times the individual clock speed of the vCPU for the Avaya Breeze® platform nodes and the Omnichannel Windows server.
- The VMware reservation on the CPU count must match the CPU requirement for Avaya Breeze® platform nodes and the Omnichannel Windows server.
- The VMware CPU benchmark must minimally match a Dual (2 Socket) E5-2697 V3 @2.6GHz processor.
- This is a 2 CPU socket configuration meaning 2 CPUs. This reference dual processor benchmark score and thread rating is published on https://www.cpubenchmark.net.
- The VMware CPU benchmark for the VMware physical host running Avaya Oceana® and Avaya Analytics™ must be equal to or greater than 90% of the individual core benchmark and thread value score for the Avaya Oceana® reference dual processor.
- Other VMware settings and capabilities that can be supported or not supported in an Avaya Oceana® deployment are presented in a table in later sections of this document.

Avaya Oceana® VMware physical host server minimum CPU specification

Configure each VMware virtual machine with CPU resources to support Avaya Oceana®. For each virtual machine and required agent count, configure a specified number of vCPU cores and CPU reservations in MHz’s

Avaya Oceana® VMware profiling uses a Dual 14-core Intel Xeon E5-2697 V3 2.60 GHz CPU as a reference CPU. This reference processor has 28 physical CPU cores. Each of the cores has an individual benchmark value that is one twenty-eighth of the overall benchmark score of the reference processor. You use this individual core benchmark value to compare the cores from different processors and to select suitable VMware host hardware for Avaya Oceana® virtualization.

The individual core benchmark value for the processor in your VMware host server must be equal to or greater than 90% of the individual core benchmark value for Avaya Oceana® reference processor.

Do the following to ensure that your proposed VMware host CPUs meet the Contact Center minimum requirements:

- Using the https://www.cpubenchmark.net website, determine the individual core benchmark value for the reference CPU, Dual 14-core Intel Xeon E5-2697 V3 2.60GHz.

  Reference individual core benchmark value = Reference CPU benchmark from the website / Number of cores in the reference CPU.

- Using the https://www.cpubenchmark.net website, determine the individual core benchmark value for your chosen VMware physical host server CPU.

  Individual core benchmark value = Your chosen physical host server CPU benchmark from the website / Number of cores in the host server CPU.

- To support Contact Center virtualization, the individual core benchmark value of your chosen VMware physical host must be equal to or greater than 90% of the reference individual core benchmark value.

- To support Contact Center, your chosen physical VMware host must have a sufficient number of CPU cores with each core having at least the minimum individual core benchmark value.

  For more information, see Working example - CPU Model [Dual CPU] Intel Xeon Gold 6240R @ 2.40GHz 24 Core Processor for Avaya Oceana Breeze Virtual Machines on page 60.

Avaya Oceana®, Avaya Analytics™, and VMware snapshot considerations

VMware snapshots save the current state of the virtual machine so that you can return to the current state 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.

Snapshots are permitted on Avaya Oceana® and Avaya Breeze® platform virtual machines for maintenance and upgrade purposes.

The following considerations apply when using snapshots with Avaya Oceana® on VMware:

Creation of snapshots:

- A maintenance window is required as snapshots must only be taken while all the Avaya Oceana® and Avaya Analytics™ virtual machines are in a powered down state. It reduces the risk of data corruption and significantly reduces the time taken to create the snapshots.
- Avaya recommends that additional disk space is provisioned before any snapshot is taken so that you have space available for the snapshot and virtual machine.

  A guiding figure for the minimum additional disk space that must be provisioned for each Avaya Oceana® virtual machine is 50% of the disk space required for the virtual machine. For example, if an Avaya Oceana® virtual machine requires 200 GB disk space for normal operation, then you must have 100 GB additional disk space for snapshots, which means that you must have total 300 GB disk space.

- The time taken to create a snapshot is minimal when the virtual machine is in a powered off state.
- All snapshots must be taken on Avaya Oceana® virtual machines at the same time.
- A snapshot can only be in place during the system maintenance window assigned for the activity.

Removal of snapshots:

- Avaya recommends that you remove all snapshots from the physical host within 8 hours after completion of maintenance tests or any software upgrade, patching, or migration activity. Keeping a snapshot on the physical host can lead to performance issues resulting in a loss of contact center capabilities.
- All snapshots must be removed from all Avaya Oceana® virtual machines at the same time.
- Avaya Oceana® virtual machines must be powered down prior to removing snapshots to reduce the risk of data corruption and significantly reduce the times taken to consolidate the changes back to the original disks.

  The time can be considerable depending on the amount of change. For example, software change, workload under snapshot, or snapshot duration.
- Avaya Oceana® and Avaya Analytics™ maintenance windows must build in time for the removal of all snapshots.

  Time required to remove snapshots is more than the time required to create them.

Restoration of snapshots:

- Avaya Oceana® and Avaya Analytics™ virtual machines must be powered down prior to restoring snapshots to reduce the risk of data corruption and significantly reduce the times taken to consolidate the changes back to the original disks.

  The time can be considerable depending on the amount of change. For example, software change, workload under snapshot, or snapshot duration.
- All snapshots must be restored from all Avaya Oceana® virtual machines at the same time.
- When restoring snapshots, carefully consider the possible impact from out-of-date antivirus definitions, missed operating system updates, and lapsed domain accounts on the contact center. Isolate the restored virtual machine until these issues are resolved.

VMware Performance Monitoring Guidelines

- For Performance and Monitoring tools and capabilities, see the *Interpreting esxtop Statistics* document at https://communities.vmware.com/docs/DOC-9279 to investigate and avoid performance problems at the virtualization layer.
- Observe the following for using esxtop data at the host level:
  - CPU Load Average: A load average of 1.00 specifies that the physical CPUs of the host are fully utilized. A load average of 0.5 specifies that the physical CPUs of the host are half utilized. Any value greater than 1 specifies performance problems.

    Note:

    Performance problems can also occur with values less than 1.
- Physical CPU: Performance is impacted if the Physical CPU consistently exceeds the 70% level. Ensure that the Physical CPU usage does not consistently exceed 70%. Short spikes of up to 80% are tolerated.
- VMware provides additional tools such as esxtop and resxtop for determining performance characteristics. Esxtop and VMware Infrastructure Clients provide large quantities of

performance data for all levels of granularity, from host through Virtual Machine and per vCPU. Observe the following for using esxtop data at the Virtual Machine level:

- RDY: The percentage of time that something is waiting for a CPU to be available to take its workload. Ensure that RDY does not exceed 5% for any vCPU.
- MLMTD: The percentage of time that a vCPU was waiting due to a limit set on the Virtual Machine for CPU usage. Ensure that you increase or remove your limit if this value is greater than 0.

Avaya Oceana® physical host requirements

Avaya Oceana® Cluster 1 has the largest cluster size in terms of Avaya Breeze® platform nodes. Avaya Oceana® Cluster 1 contains three Avaya Breeze® platform nodes deployed as virtual machines. This requirement is applicable for all Avaya Oceana® footprints from 100 to 4500 agents. Therefore, the minimum number of supported physical hosts required for an Avaya Oceana® deployment is three. This is to ensure a minimum level of redundancy for Avaya Oceana® Cluster 1 nodes where each node must be deployed on a different physical host.

- Other Avaya Breeze® platform nodes from Avaya Oceana® Cluster 2, Avaya Oceana® Cluster 3, Avaya Oceana® Cluster 4, or Avaya Oceana® Cluster 5 can be deployed across 1, 2 or 3 of these physical hosts to maximize redundancy for these clusters in addition to Avaya Oceana® Cluster 1.
- In all circumstances, avoid deploying multiple nodes from the same cluster on one physical host.
- The nodes of Avaya Oceana® Cluster 1, Avaya Oceana® Cluster 2, Avaya Oceana® Cluster 3, Avaya Oceana® Cluster 4, and Avaya Oceana® Cluster 5 can share a common physical host with no restrictions on which physical host they are located on or other Breeze Node they co-share the host with for normal operations.
- Avaya has published an application PSN (PSN005416U) https://downloads.avaya.com/css/P8/documents/101057845 on the Avaya Support website at http://support.avaya.com. The PSN provides details about using VMware DRS affinity rules to locate Avaya Oceana® cluster nodes to specified physical hosts.

Working example - CPU Model [Dual CPU] Intel Xeon Gold 6240R @ 2.40GHz 24 Core Processor for Avaya Oceana Breeze Virtual Machines

Procedure

1. To view the CPU Benchmark score for this processor, click https://www.cpubenchmark.net/cpu.php?cpu=Intel+Xeon+Gold+6240R+%40+2.40GHz&id=3739&cpuCount=2

   Benchmark score = 54024

   Note:

   The benchmark scores change as they are updated regularly.

2. For this 24 Core Processor, divide the benchmark score 54024 by the total number of cores 48.

   Individual core rating = 1125.50 approximately.

3. To view the CPU Benchmark score for the Avaya reference processor, click https://www.cpubenchmark.net/cpu.php?cpu=Intel+Xeon+E5-2697+v3+%40+2.60GHz&id=2333&cpuCount=2

   Benchmark score = 30323

   Note:

   The benchmark scores change as they are updated regularly.

4. For a 14 Core Avaya reference processor, divide the benchmark score 30323 by the total number of cores 28.

   Individual core rating = 1082.96 approximately.

5. Compare the two values 1125.50 and 1082.92.

   The individual score for the 6240R processor is greater than the individual score for the 2697 processor, and therefore, is appropriate for use in an Avaya Oceana Breeze deployment.

   Important:

   - A processor that meets 90% of the Avaya reference processor is suitable for deployment. It does not have to be equal or greater than the individual core score for the Avaya reference processor.

     The following is a short list of suitable CPU types for physical hosts running the Avaya Oceana Breeze and Avaya Analytics CSP based virtual machines, currently in use by existing Avaya Oceana customers:

     - 14 core [Dual CPU] Intel® Xeon® Gold 6132 @ 2.60GHz
     - 16 core [Dual CPU] Intel® Xeon® Gold 5218 @ 2.30GHz
     - 24 core [Dual CPU] Intel® Xeon® Platinum 8280 @ 2.70GHz
     - 14 core [Dual CPU] Intel® Xeon® Gold 6132 @ 2.60GHz
     - 16 core [Dual CPU] Intel® Xeon® Gold 6226R 2.9GHz
     - 24 core [Dual CPU] Intel® Xeon® Gold 6240R @ 2.40GHz

   - Newer processors may not have a benchmark score rating and are not recommended for use in an Avaya Oceana and Analytics deployment.
   - High-specification processors with 32 or 48 cores or higher, and lower clock speeds (< 2.3 GHz), may not meet the specification required for Avaya Oceana and Analytics deployments.

Inputs for Omnichannel Windows Server

The following table lists the main inputs to consider before installing Microsoft Windows Server 2019 (Desktop Experience):

Name	Description
Computer name	The name of the server where you want to install Microsoft Windows Server 2019 (Desktop Experience). Ensure that: • The name does not have spaces or underscores. • The name does not exceed 15 characters. • The name starts with an alphabetic character. • The name adheres to RFC1123. • The final production name is configured before installing the Omnichannel software. • The name matches the DNS name and is case sensitive.
Disk drives	Format the partitions as required for the server.
Domain name	Configure as required for your site. You must check to ensure the DNS Domain name (including case) matches the server name if the server is added to a domain after configuration.
Licensing modes	Select Per server licensing mode. Accept the default five concurrent connections.
Network components	Configure IP Address, WINS, and DNS for one or two network cards as per configuration. Omnichannel does not support IPv6.
Network connections	If the server has more than one NIC/adapter, ensure that the Omnichannel subnet appears first in the network adapter binding order.
Hard Disk Partitions	Configure C: drive to be a primary Operating system drive. Configure the other drives on your server to meet the requirements according to the Omnichannel specification: • D: Application partition 60 GB minimum • F: Database partition 100 GB minimum • G: Journal partition 60 GB minimum **Note:** You can label the drive letters as desired. However, you must ensure that the specified minimum drive size for each drive is available.

VMware configuration

VMware Feature	Avaya Oceana®	Avaya Analytics™ **Warning:** **Do not delete nodes or VMs from your VMware.**
A single VMware cluster can be shared between Avaya Oceana® 3.10.x and Avaya Analytics™ 4.2.x/4.3.x. • The cluster contains virtual machines for both Avaya Oceana® 3.10.x and Avaya Analytics™ 4.2.x/4.3.x. • The cluster can also contain virtual machines of other applications without contention. **Note:** Avaya Oceana® 3.10.x and Avaya Analytics™ 4.2.x/4.3.x. can also be supported in separate clusters.	Yes For instructions on enabling affinity rules in a DRS-enabled VMware cluster, see PSN005416u located at https://downloads.avaya.com/css/P8/documents/101057845.	Yes For more information, see PSN005633u located at https://downloads.avaya.com/css/P8/documents/101067348.
Cloning	No	No Avaya Analytics™ supports cloning cluster node VMs during the initial OVA deployment before they are powered up.
Distributed Resource Scheduler (DRS)	Yes For the documented guidelines in conjunction with affinity rules, see PSN005416u located at https://downloads.avaya.com/css/P8/documents/101057845.	Yes For the documented guidelines on HA and DRS rules for Avaya Analytics™ 4.x, see PSN005633u located at https://downloads.avaya.com/css/P8/documents/101067348.
Storage DRS	No Avaya Oceana® does not support this feature. There are impacts to the datastores. The input or output load balancing occurring in production can cause outages.	No **Note:** Avaya Analytics™ 4.x does not support Storage DRS nor datastore clusters.
Distributed Power Management (DPM)	No	No

Table continues…

VMware Feature	Avaya Oceana®	Avaya Analytics™ **Warning:** **Do not delete nodes or VMs from your VMware.**
Distributed Switch (Network)	Yes • Requires VMware Enterprise Plus license. **Note:** Loss of vCenter indicates that you cannot manage data networks on the hosts. • If you use standard vSwitch, you can do the management from each host.	Yes • Requires VMware Enterprise Plus license. **Note:** Loss of vCenter indicates that you cannot manage the data networks on the hosts. • If you use standard vSwitch, you can do the management from each host.
Fault Tolerance	No	No
High Availability (HA)*	No • Avaya Oceana® does not support impacts to the virtual machines occurring in production. • For more information on configuring VMware HA in an Avaya Oceana® and Avaya Analytics™ single cluster deployment, see PSN005633u located at https://downloads.avaya.com/css/P8/documents/101067348.	Yes • Mandatory for Avaya Analytics™ 4.x High Availability feature. • For the documented guidelines on HA and DRS rules for Avaya Analytics™ 4.x, see PSN005633u located at https://downloads.avaya.com/css/P8/documents/101067348.
Snapshots***	Partial • Yes, as part of maintenance window** procedures only for upgrades or patching. • You must remove all snapshots before putting the contact center back into production.	Partial • Yes, as part of maintenance window** procedures for upgrades or patching only for the following Avaya Analytics™ application: • Cluster Control Manager (CCM) - You must remove all snapshots before putting the contact center back into production. • Snapshots are supported for all the VMs in the cluster.

Table continues…

VMware Feature	Avaya Oceana®	Avaya Analytics™ **Warning:** **Do not delete nodes or VMs from your VMware.**
Storage Thin Provisioning	Partial • Yes, for SAN storage. • No, for local hard disk storage.	Yes • Yes, for SAN storage. • No local storage supported. **Note:** Applicable only to Avaya Analytics™ on HA. • For more information on specifics of thin provisioning, see Thin provisioning of disk storage in VMware on page 67.
Suspend and Resume	No	No
Cold Migration	Yes • You can do a cold migration only on a virtual machine in a powered-off state. • Avaya Oceana® uses static IPs. Therefore, the new ESXI host(s) must have access to the original data network and datastore for the migrated virtual machines.	Yes • You can do cold migration only on a virtual machine in a powered-off state. • Avaya Analytics™ uses static IPs. Therefore Avaya Analytics™ virtual machines can only be migrated to hosts in the same VMware that has the same access to all elements in the cluster as existing hosts. When performing any cold migrations of Avaya Analytics™ virtual machines from host to host, see the *Considerations for upgrading Physical Hosts running Avaya Analytics™ virtual Machine* section in *Deploying Avaya Analytics™*.

Table continues…

VMware Feature	Avaya Oceana®	Avaya Analytics™ ⚠ **Warning:** **Do not delete nodes or VMs from your VMware.**
Reservations on vCPU and memory required to be enabled	Yes • Set to `Yes`. For production environments, Avaya Oceana® customers provide the VMware deployments wherever there is contention for resources. • Physical hosts running Avaya Oceana® virtual machines can have other virtual machines running and co-residing with the Avaya Oceana® virtual machines. • On Avaya Pod Fx systems, reservations are not required, because the Avaya supplied hardware is engineered not to be over provisioned.	No Avaya Analytics™ 4.x reservations on vCPU and memory are not mandatory, as long as the environment is not over provisioned and there is no contention for resources with other virtual machines.
Hyperthreading	No • Avaya Oceana® requires reservations. Therefore, Hyperthreading does not add any additional value. • You can enable on the VMware infrastructure for the other applications.	Yes

- * Avaya Oceana® provides its own HA mechanism.
- ** A maintenance window specifies a scheduled out-of-production window where the system does not process contacts, agents are all logged out, and queues are empty. This timeframe is dedicated to tasks such as patching, upgrades, and configuration.
  - During this timeframe, Avaya Oceana® and the applications such as Avaya Breeze® platform nodes, System Manager, Avaya Control Manager, and Omnichannel Database remain powered on and accessible on the customer network but do not process any contacts or operations.
  - During the creation of snapshots, you must power down Avaya Oceana® and the applications such as Avaya Breeze® platform nodes, Avaya Control Manager, and Omnichannel Database.
- *** You must delete snapshots from Avaya Oceana® virtual machines before placing Avaya Oceana® back into production. Snapshots must only be taken or deleted when the virtual machine is powered down.

Upgrading ESXi hosts running Avaya Oceana® or Avaya Analytics™ virtual machines

Hosts running virtual machines that are part of Avaya Oceana®, Avaya Analytics™ and/or Avaya Breeze® platform, must be kept up-to-date, including VMware ESXi.

Host software maintenance and updates must be planned into a maintenance windows where the contact center is not in service. In these maintenance windows, one or more physical hosts may be out of service, including all the virtual machines running on these hosts.

Important:

- Host maintenance must include consideration of all components of the customer solution. For example Avaya Analytics™, Avaya Breeze® platform and Avaya Oceana®. Refer to the relevant maintenance documents for each solution component:
- - The *VMware host maintenance* section in the *Maintaining and Troubleshooting Avaya Oceana®* manual.
  - The *Upgrading Avaya Analytics™ ESXI hosts* section in the *Maintaining and Troubleshooting Avaya Analytics™ for Avaya Oceana®* manual.
  - The *Maintaining and upgrading ESXi host software* section in the *Maintaining and Troubleshooting Avaya Breeze® platform* manual.

The following are important considerations when removing or adding physical hosts to the deployment:

- Do not remove or replace the physical VMware ESXi hosts running Avaya Analytics™ virtual machines from the VMware cluster during maintenance windows.
- You can add one or more physical hosts to the VMware cluster to facilitate host maintenance. Adding physical hosts enables migrating host virtual machines to a new host while the existing host is updated.
- You must propagate all the VMware permissions for the same user account used to deploy the Avaya Analytics™ cluster to the new host. You must perform this before removing the new host from maintenance mode and putting it into production. Avaya Analytics™ virtual machines cannot access resources on the new host if you fail to propagate VMware permissions.

Thin provisioning of disk storage in VMware

Avaya Analytics™ supports thin provisioning of disk storage in VMware for all agent configurations. Though this document specifies the required disk storage space for each agent configuration, you do not have to provision the entire disk space on day 1. You can add space as and when needed. No maintenance window is required.

Warning:

You must actively manage your VMware disk space and add more space before the application runs out of space.

Insufficient disk space provided to the system when operating with thin provisioning can result in disk write errors in the logs and data loss. Avaya bears no responsibility for errors and data loss.

To ensure efficient thin provisioning, do the following:

- Provision additional disk space whenever the remaining disk space is less than 0.25 TB, assuming that you can provision additional storage within an hour or less. You are accountable for the time required to provision additional disk storage before the system reaches its current limit.
- When the datastore capacity does not initially meet the requisite footprint, the minimum storage requirement for a deployment requires the datastore to be at least the size of disk 2 on cluster node 1 or 2.

  You can find this storage size in the spreadsheet on the Deployment Properties tab in the Footprint Summary table under Disk Storage Requirements for Cluster Node 1 or 2.

Adding additional disk space is a standard VMware operation.

Avaya Oceana® virtualized deployment checklist

Perform the following checks for a virtualized deployment of Avaya Oceana®:

Task	Yes/No
Physical hosts CPU specifications meet Avaya reference CPU per benchmark site	
Virtual machine CPU reservations ON	
Virtual machine Memory reservations ON	
All snapshots of Avaya Oceana® virtual machines removed before production	

Create the database for External Data Mart

External Data Mart (EDM) is a feature of Context Store that enables persistence of context information from the in-memory data-grid to an external database. This feature is mandatory for an Avaya Oceana® deployment. It stores the data required to build Customer Journey View in Avaya Workspaces.

You must create the required schema in the Context Store-supported database type and configure EDM through the **External Data Mart Configuration** group in OceanaConfigurationService.

For more information on supported databases, see Deploy External Data Mart overview on page 145

All existing users must migrate to one of the supported versions of Microsoft SQL Server 2016. For procedures to migrate from Oracle or PostgreSQL to MS SQL Server, see the *Upgrading Avaya Oceana®* document.

Avaya Oceana® Release 3.8 and higher supports the following installation options for EDM:

- EDM and Avaya Control Manager co-resident on the same Microsoft SQL server.
  - For new Avaya Oceana® deployments, see the *Deploy External Data Mart on Avaya Control Manager SQL Server* section in this document.

- For upgrading to install EDM co-resident with the Avaya Control Manager on the same MS SQL server, see the relevant chapter in the *Upgrading Avaya Oceana®* document.

- EDM standalone installation on MS SQL.
  - For information on how to install an EDM database and create tables, see the *Deploy External Data Mart on standalone SQL Server* section in this document.

Important:

- In an Avaya Oceana® deployment, EDM is a mandatory requirement.
- You must monitor and maintain the EDM database to ensure that it does not consume unnecessary space. Keep purging old or unused data from the EDM database at regular intervals. Take a backup of the EDM database before undertaking any maintenance activity.

Note:

When installing SQL Server on virtual machines, Avaya recommends reading VMware's best practices published at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/sql-server-on-vmware-best-practices-guide.pdf. A summary of these recommendations includes:

- Store database Log files and database Data files on separate disks. This avoids I/O contention and improves performance.
- Install SQL Server and the Windows operating system on the same disk.

Planning tasks

- Read *Avaya Oceana® Solution Description*.
- Ensure that the time on all servers in Avaya Oceana® is synchronized.

Configuring the TLS version

About this task

Use this procedure to configure the TLS version through System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Security** > **Configuration** > **Security Configuration**.
2. On the Security Configuration page, do the following:
   a. Select the **Global** tab.
   b. In the **Minimum TLS Version** field, select `TLSv1.2`.
   c. Click **Commit**.
3. Restart System Manager.

Configuration and deployment details

The following tables list the configuration and deployment details that you must know before deploying and commissioning Avaya Oceana®.

Avaya Aura® Communication Manager

Name	Your value
Release	
IP address	
User Name	
Password	
SAT Password	
Hunt Group number	
CTI-Link number	
Ingress VDN	
Routing VDN	
RONA VDN	
Transfer to Service VDN	

Avaya Aura® System Manager

Name	Your value
Release	
Hostname	
Management IP address	
Enrollment Password	
LDAP Server FQDN	
LDAP User name	
LDAP Password	
LDAP Base Distinguished Name	
Security IP address	

Avaya Aura® Session Manager

Name	Your value
Release	
Hostname	
Management IP address	
Security IP address	

Avaya Aura® Application Enablement Services

Name	Your value
Release	
Server 1 - Hostname	
Server 1 - Management IP address	
Server 1 - Switch CTI Link Number	
Server 2 - Hostname	
Server 2 - Management IP address	
Server 2 - Switch CTI Link Number	

Avaya Control Manager

Name	Your value
Release	
Hostname	
IP address	
Location	
Standalone Microsoft SQL Server - IP address	

Avaya Experience Portal

Name	Your value
Hostname	
Management IP address	
Orchestration Designer version	
WorkAssignmentSelfService sample application version	
Tomcat IP address	
MPP server 1 IP address	
MPP server 2 IP address (Optional)	
Nuance TTS server IP Address	
Nuance server English language Voice	

Avaya Oceana® Cluster 1

Name	Your value
Node 1 - Hostname	
Node 1 - Management IP address	
Node 1 - Security IP address	
Node 2 - Hostname	

Table continues…

Name	Your value
Node 2 - Management IP address	
Node 2 - Security IP address	
Node 3 - Hostname	
Node 3 - Management IP address	
Node 3 - Security IP address	
Cluster IP address	
Cluster Hostname	

Avaya Oceana® Cluster 2

Name	Your value
Node 1 - Hostname	
Node 1 - Management IP address	
Node 1 - Security IP address	
Node 2 - Hostname	
Node 2 - Management IP address	
Node 2 - Security IP address	
Cluster IP address	
Cluster Hostname	

Avaya Oceana® Cluster 3

Name	Your value
Node 1 - Hostname	
Node 1 - Management IP address	
Node 1 - Security IP address	
Node 2 - Hostname	
Node 2 - Management IP address	
Node 2 - Security IP address	
Cluster IP address	
Cluster Hostname	
Primary System Manager IP address	
Exchange Server IP address	
Exchange Server Port	
Exchange Server Protocol (POP3/IMAP)	
SMTP Server IP address	
SMTP Server Port	

Avaya Oceana® Cluster 4

Name	Your value
Node 1 - Hostname	
Node 1 - Management IP address	
Node 1 - Security IP address	
Node 2 - Hostname	
Node 2 - Management IP address	
Node 2 - Security IP address	
Cluster IP address	
Cluster Hostname	

Avaya Oceana® Cluster 5

Name	Your value
Node 1 - Hostname	
Node 1 - Management IP address	
Node 1 - Security IP address	
Node 2 - Hostname	
Node 2 - Management IP address	
Node 2 - Security IP address	
Cluster IP address	
Cluster Hostname	

Omnichannel Windows Server

Name	Your value
Hostname	
IP address	

External Data Mart

Name	Your value
Database Type	
Database Name	
FQDN	
Port number	
Username	
Password	

Messaging

Name	Your value
Cloud Provider	
Avaya Oceana® Cluster 3 FQDN	
Avaya Oceana® Cluster 3 IP address	
Avaya Common Services (CSP) Cluster External FQDN	
Avaya Common Services (CSP) Cluster External IP address	

Configuring LDAP server integration

About this task

Avaya Aura® System Manager supports integration with an LDAP authentication server. Therefore, you must configure System Manager to integrate with an LDAP server.

Note:

- This procedure is a basic example of System Manager and LDAP integration. For more information, see *Administering Avaya Aura® System Manager*.
- Avaya Oceana® only supports secure binding. When you use Active Directory as an LDAP server, you must install a Certificate Authority on the Active Directory server.

Before you begin

Add an LDAP server to the solution.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select the **System Manager** check box, and click **More Actions** > **Manage Trusted Certificates**.
3. On the Manage Trusted Certificates page, click **Add**.
4. On the Add Trusted Certificate page, perform the following steps:
   a. Click **Import using TLS**.
   b. In the **IP Address** field, enter the IP address of your LDAP server.
   c. In the **Port** field, enter the port number as `636`.
   d. Click **Retrieve Certificate**.
   e. Click **Commit**.
5. On the System Manager web console, click **Users** > **Directory Synchronization** > **Sync Users**.
6. On the User Synchronization page, on the Synchronization Datasources tab, click **New**.

7. On the New User Synchronization Datasource page, in the Directory Parameters section, perform the following steps:
   a. In the **Datasource Name** field, enter the name to identify Active Directory.
   b. In the **Host** field, enter the FQDN address of your LDAP server.

      Ensure that LDAP certificates contain a SAN entry.
   c. In the **Principal** field, enter the LDAP login details.

      For example, myDomain\Administrator.
   d. In the **Password** field, enter the password for the LDAP login account that you specified.
   e. In the **Port** field, enter the port number as `636`.
   f. In the **Base Distinguished Name** field, enter the LDAP details.

      For example, CN=user,DC=myDomain,DC=com
   g. In the **LDAP User Schema** field, enter the LDAP User Schema details.
   h. In the **Search Filter** field, enter the LDAP search string.

      For example, CN=Alex*.
   i. Select the **Use SSL** check box.
   j. Click **Test Connection**.
8. On the New User Synchronization Datasource page, in the Attribute Parameters section, perform the following steps:
   a. Click **Add Mapping** to add a row.
   b. From the drop-down list on the left, select **cn**.
   c. From the corresponding drop-down list on the right, select **sourceUserKey**.
   d. Click **Add Mapping** to add another row.
   e. From the drop-down list on the left, select **mail**.
   f. From the corresponding drop-down list on the right, select **loginName**.

      Note:

      Instead of the **mail** field pointing to **loginName**, you can also use **userPrincipalName** depending on the configuration of the LDAP server. For example, if the **mail** field is not set in the LDAP server.
   g. Click **Add Mapping** to add another row.
   h. From the drop-down list on the left, select **sn**.
   i. From the corresponding drop-down list on the right, select **surname**.
   j. Click **Add Mapping** to add another row.

k. From the drop-down list on the left, select **givenName**.
l. From the corresponding drop-down list on the right, select **givenName**.
m. Click **Add Mapping** to add another row.
n. From the drop-down list on the left, select **displayName**.
o. From the corresponding drop-down list on the right, select **displayName**.

9. Click **Save**.
10. On the User Synchronization page, click **Active Synchronization Jobs**.
11. Click **Create New Job**.
12. On the New User Synchronization Job page, in the **Datasource Name** field, select the LDAP server and click **Run Job**.

    Wait for the job to complete so that all LDAP users are loaded in System Manager.
13. On the User Synchronization page, click **Synchronization Job History**.
14. In the **Status** column, verify that the status of the job is `RUNNING`.

    The status changes to `COMPLETED` when the job is complete.

Avaya Workspaces single sign-on

You can configure Avaya Breeze® platform Authorization Service attributes to enable SAML. The Avaya Breeze® platform Authorization Service also supports IWA/Kerberos authentication.

LDAP integration:

When attempting to access the Avaya Workspaces URL, unauthorized users are redirected to the Avaya Breeze® platform Authorization Service. If LDAP integration is configured, Avaya Breeze® platform prompts the user for credentials. After a successful authentication Avaya Breeze® platform grants users authorization permissions using an authorization token, and if users have the correct permissions set in ACM they can access Avaya Workspaces.

SAML integration:

When attempting to access the Avaya Workspaces URL, unauthorized users are redirected to the Avaya Breeze® platform Authorization Service. If SAML integration is configured, the Authorization Service redirects users to your identity provider (IdP), and prompts the user for credentials. After a successful authentication Avaya Breeze® platform grants users authorization permissions using an authorization token, and if users have the correct permissions set in ACM they can access Avaya Workspaces

Note:

When SAML is enabled it overrides all other authentication methods like Standard login, LDAP login and EASG.

IWA/Kerberos integration:

If the Avaya Breeze® platform Authorization Service is configured for IWA/Kerberos authentication, the Authorization Service automatically uses the Windows credentials of the user for

authentication. You do not need to manually enter your credentials when accessing Avaya Workspaces. When attempting to access the Avaya Workspaces URL, users are redirected to the Avaya Breeze® platform Authorization Service, which uses IWA to automatically grant users authorization permissions using an authorization token. If users have the correct permissions set in ACM they can access Avaya Workspaces.

When users exit Avaya Workspaces, they are redirected to the Exit page. Users can choose to immediately return to Avaya Workspaces and if permitted by the Authorization Service, the Activate Agent screen immediately appears and users can log on again without entering credentials.

For more information about Avaya Breeze® platform, SAML, and Kerberos authentication, see Avaya Breeze® platform documentation, available on https://support.avaya.com.

Adding Avaya Contact Recorder or Avaya Contact Recorder Advanced to Avaya Oceana®

For more information, see the following documents at http://support.avaya.com:

- *Avaya Contact Recorder Planning, Installation and Administration Guide*
- *Workforce Optimization Distributor Technical Reference*
- *Avaya Workforce Optimization - ACR Advanced Recorder Avaya Integration Guide*
- *Oceana to WFM Integration Application Note*

Route Points configuration

In Avaya Oceana®, you must associate the multimedia contacts for all channels with a Route Point. Route Points differentiate whether contacts are under contact center control or are personal agent interactions. Route Points provide differentiation in reporting and customer business logic. You can create Route Points using Avaya Control Manager.

In Avaya Oceana®, you must configure Route Points in all multimedia rules, including system rules, before EmailService starts. After upgrading the solution, you must also restore the existing rules that you configured with Route Points before the upgrade.

The following table lists the channels that require Route Point configuration:

Channel	Description
Email	See Configuring rule groups on page 564.
Chat	See Configure the sample Chat client overview on page 531.
SMS	See Configuring SMS Gateway on page 587.
Social Media	See Configuring Social Media for third-party gateways on page 605.
Messaging	See Configure sample Messaging clients on page 642.

Table continues…

Channel	Description
Web Voice	See Configuring an Implicit User Route Point for inbound Web Voice on page 451.
Web Video	See Configuring an Implicit User Route Point for inbound Web Video on page 466.
Generic Channel	See the SDK documentation for information about using Route Points with the Generic Channel.

Chapter 6: Deploy Avaya Breeze® nodes

Deploy Avaya Breeze® platform nodes overview

You can deploy the Avaya Breeze® platform nodes for the following clusters of Avaya Oceana®:

- Avaya Oceana® Cluster 1
- Avaya Oceana® Cluster 2
- Avaya Oceana® Cluster 3
- Avaya Oceana® Cluster 4
- Avaya Oceana® Cluster 5

For an Avaya Oceana® deployment that supports up to 100 active agents:

- Do not create Avaya Oceana® Cluster 2 and Avaya Oceana® Cluster 5.
- Install the following SVARs of Avaya Oceana® Cluster 2 on Avaya Oceana® Cluster 1:
  - AuthorizationService
  - AvayaMobileCommunications
  - BotConnector
  - UnifiedAgentContextService
  - UnifiedAgentController

  Configure the Lightweight Directory Access Protocol (LDAP) server certificates for Avaya Oceana® Cluster 1 nodes.
- Install the CRMGateway SVAR on Avaya Oceana® Cluster 1.
- Install the ZangSmsConnector snap-in on Avaya Oceana® Cluster 3

Important:

- To deploy Avaya Breeze® platform nodes and create clusters, you must have sufficient privileges in System Manager. For information about how to manage groups and roles for resources in System Manager, see *Administering Avaya Aura® System Manager*.
- Deploy all Avaya Breeze® platform nodes on the same version of VMware ESXi.

Avaya Breeze® platform authorization

When a request is made between a client and a third-party server, an authorization token is passed with the request. The authorization is handled through the cluster that hosts

AuthorizationService. Avaya Aura® Web Gateway and Avaya Aura® Device Services are examples of third-party servers. You must import the Avaya Breeze® platform Authorization Certificate on these servers if they are part of your solution.

Each Avaya Breeze® platform node in the cluster has a different Authorization Identity Certificate and when load balancing is enabled between the nodes, some requests are rejected. Therefore you must first replace the Authorization Identity Certificate on each Avaya Breeze® platform node with a single System Manager-generated Identity Certificate, and then import this common certificate on any servers in your solution that require this Identity Certificate.

This section includes procedures for creating the common certificate, importing it onto Avaya Breeze® platform nodes, and export it from Avaya Breeze® platform.

Avaya Breeze® platform nodes deployment checklist

Use the following checklist to deploy the Avaya Breeze® platform nodes for your Avaya Oceana®:

No.	Task	Notes	✔
1	Download *Avaya Oceana® Solution Description*	-	
2	Download *Deploying Avaya Breeze® platform* Click the following link to support site: https://support.avaya.com/support/en/public		
3	Review Avaya Breeze® platform and server requirements for your solution	See *Avaya Oceana® Solution Description*.	
4	Review Avaya Oceana® specifications against your solution requirements	See *Avaya Oceana® Solution Description*.	
5	Calculate the number of Avaya Breeze® platform nodes required for your solution	See *Avaya Oceana® Solution Description*.	

Table continues…

No.	Task	Notes	✔
6	Deploy the Avaya Breeze® platform nodes	See *Deploying Avaya Breeze® platform*. If you deploy Avaya Breeze® platform using the OVF template, the default disk size is 50 GB thick-provisioned. The installer must also select multiple profiles to define CPU and RAM requirements. Based on your deployment type, you must change the disk size, CPU, and RAM of Avaya Breeze® platform nodes through the vSphere client. For information about the minimum requirements for Avaya Breeze® platform nodes in each deployment type, see Avaya Oceana hardware requirements on page 51. **Important:** These Avaya Breeze® platform nodes are for the exclusive use of Avaya Oceana®. Therefore, do not install any third-party or custom Service Archives (SVARs) on these nodes.	

Verifying the Avaya Breeze® platform deployment using System Manager

About this task

Use this procedure to verify that the Avaya Breeze® platform replication is in sync with System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. On the Replica Groups page, perform one of the following steps to view the replica nodes for a replica group:
   - Select the replica group and click **View Replica Nodes**.
   - Click the replica group name.
3. Verify that **Synchronization Status** for the new Avaya Breeze® platform nodes is `Synchronized`.

   The `Synchronized` status indicates that the system has successfully replicated the data that the replica node requested from the master database to the database of the replica node.

4. **(Optional)** If **Synchronization Status** for a node is not `Synchronized`, then perform the following steps:
   a. Log in to the Avaya Breeze® platform node using an SSH client application, such as PuTTy.
   b. Run the **`AvayaNetSetup`** command.
   c. Review configuration details.

CylancePROTECT deployment on Avaya Breeze®

Installing CylancePROTECT

About this task

To install CylancePROTECT for Avaya Analytics on CSP.

Procedure

1. Copy the **`Cylance tar`** **CylancePROTECT.centos8.tar** file to the Cluster Control Manager (CCM) folder.You need to copy the tar file to the customer folder For example: `/home/cust location.`

   This tar file contains the following packages that must be installed

   - CylancePROTECTOpenDriver-3.0.1005-2344.el8.x86_64.rpm
   - CylancePROTECTDriver-3.0.1005-2344.el8.x86_64.rpm
   - CylancePROTECT.el8.rpm
2. Untar the tar file using the command, `tar -xvf CylancePROTECT.centos8.tar`
3. Before installing RPM, create the following file:

   `/opt/cylance/config_defaults`

   The file contains the following configuration:

```
InstallToken=QFyc1OvU9DhT7K5fqZQ8rf08
SelfProtectionLevel=2
LogLevel=2
VenueZone=LABS-CSP-prasannak
UiMode=2
```

Note:

The above example depicts the installation token and zone information allocated to CSP. Adopting products need to obtain their own tokens and zones created by the Avaya antivirus team.

The `config_defaults` is available at the location `/opt/cylance/`. If you are unaware of VenueZone, do not add to the configuration file.

4. To install Cylance on Cluster Control Manager (CCM), use the below command

```
rpm -ivh CylancePROTECTOpenDriver-3.0.1005-2344.el8.x86_64.rpm
rpm -ivh CylancePROTECTDriver-3.0.1005-2344.el8.x86_64.rpm
rpm -ivh CylancePROTECT.el8.rpm
```

5. Use the following command from the SSH to the node where you want to install Cylance:

   cluster_ssh

6. Copy the cylance rpm from the CCM to the `/var/vcap/data folder` on each of the nodes using the below commands (assuming the CCM IP is 10.30.7.51 where customer is the customer user).

   Note:

   Before proceeding, take a snapshot and remove it within 72 hours of completing the process.Take a backup of Analytics data and also a backup of the CCM.

```
scp cust@10.30.7.51:/home/cust/
CylancePROTECTOpenDriver-3.0.1005-2344.el8.x86_64.rpm
scp cust@10.30.7.51:/home/cust/CylancePROTECTDriver-3.0.1005-2344.el8.x86_64.rpm
scp cust@10.30.7.51:/home/cust/CylancePROTECT.el8.rpm
```

   When prompted, enter the password for the customer account on CCM.

7. Create the file `/opt/cylance/config_defaults.txt` similar to step 3.

8. To install Cylance use the following command:

```
cd /var/vcap/data
```

```
rpm -ivh CylancePROTECTOpenDriver-3.0.1005-2344.el8.x86_64.rpm
```

```
rpm -ivh CylancePROTECTDriver-3.0.1005-2344.el8.x86_64.rpm
```

```
rpm -ivh CylancePROTECT.el8.rpm
```

9. If you view a failure message during rpm installation, use the following command to uninstall rpm and reinstall using the following commands:

   a. To find the rpm version, use **rpm -qa|grep Cylance**

      You view the following output is displayed:

      [root@ data]# rpm -qa|grep Cylance

      CylancePROTECTOpenDriver-3.0.1005-2344.el8.x86_64

      CylancePROTECTDriver-3.0.1005-2344.el8.x86_64

   b. Uninstall the rpm using the following command.The value passed after -e in the command above is the name obtained in step 1. (After the command, not before)

      rpm -e CylancePROTECT-3.0.1005-2335.x86_64

      rpm -e CylancePROTECTDriver-3.0.1005-2344.el8.x86_64

      rpm -e CylancePROTECTOpenDriver-3.0.1005-2344.el8.x86_64

   If a node is recreated or a new node is added to the k8s cluster, Cylance needs to be installed manually.

10. Repeat steps 4 to 8 for each of the nodes.

Verifying CylanceProtect running status

Procedure

To verify the CylancePROTECT status, run the following command:

systemctl status cylancesvc

The application must show the following output with Active and running status:

```
[root@ ~]# systemctl status cylancesvc
cylancesvc.service - Cylance PROTECT Loaded: loaded (/usr/lib/systemd/
system/cylancesvc.service; enabled; vendor preset: disabled) Active:
active (running) since Tue 2021-03-02 18:39:00 IST; 7s ago
```

Important:

You can find the Linux kernel version in the following hostnamectl output:

```
[root@ ~]# hostnamectl|grep Kernel
Kernel: Linux 3.10.0-1160.15.2.el7.x86_64
```

Disabling CylancePROTECT before the upgrade

Before you begin

Run the following commands on CCM as well as every node in the cluster.

Procedure

1. To disable CylancePROTECT, run the following commands:

   systemctl stop cylancesvc.service

   systemctl disable cylancesvc.service

   systemctl is-enabled cylancesvc.service

   systemctl status cylancesvc.service

2. To verify that CylancePROTECT is not running, run the following command:

   systemctl --type=service | grep Cy

Re-enabling CylancePROTECT post upgrade

Before you begin

Run the following commands on CCM as well as every node in the cluster.

Procedure

To re-enable CylancePROTECT, run the following commands:

```
systemctl enable cylancesvc.service
systemctl is-enabled cylancesvc.service
systemctl start cylancesvc.service
systemctl status cylancesvc.service
```

Chapter 7: Configure certificates

Exporting root, intermediate, and LDAP certificates

About this task

For Avaya Oceana®, LDAP Server user authentication is mandatory. System Manager integration is required for Avaya Oceana® and Avaya Breeze® platform deployment.

Procedure

1. Log in to the Avaya Breeze® platform server using an SSH client application, such as PuTTy.
2. Run the **`openssl s_client -connect <LDAPSERVERNAME>:636`** command.
3. Scroll up until you find the server certificate.
4. Copy the content of the certificate that is present between the `---BEGIN CERTIFICATE REQUEST---` and `---END CERTIFICATE REQUEST---` lines.
5. Open a text editor such as Notepad and paste the copied content.
6. Save as a `.cer` file.
7. Double-click the `.cer` file.
8. On the **Certificate Path** tab, select the root certificate and click **View Certificate**.
9. On the Details tab, click **Copy to File**.
10. On the Certificate Export Wizard screen, do the following:
    a. Click **Next**.
    b. Select **Base-64 encoded X.509 (.CER)** and click **Next**.
    c. Browse to the location where you want to export the certificate.
    d. Specify a name for the certificate and save as `.cer` file.
    e. Click **Save**.
    f. Click **Next**.
    g. Click **Finish** after you successfully export the certificate.
11. Change the file type of the certificate to `.pem`.
12. Repeat steps 8 to 11 for intermediate and LDAP certificates.

Next steps

You must configure in System Manager to ensure that the certificates are part of the trusted certificate authorities.

Configuring server certificates for Avaya Breeze® platform nodes

About this task

Configure the Avaya Breeze® platform nodes of Avaya Oceana® cluster to trust your server certificates.

Add the trusted certificates to all nodes of the Avaya Oceana® cluster running Authorization Service.

Before you begin

Add the server certificates to the solution.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select the **System Manager** check box, and click **More Actions** > **Manage Trusted Certificates**.
3. On the Manage Trusted Certificates page, click **Add**.
4. On the Add Trusted Certificate page, perform the following steps:
   a. Click **Import file** from file.
   b. Browse to the root certificate.
   c. Click **Retrieve Certificate**.
   d. Click **Commit**.
5. Repeat step 3 and step 4 for intermediate and LDAP certificates.
6. Click **Done**.
7. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
8. On the Cluster Administration page, select Avaya Oceana® Cluster 2.
9. Change the state to **DENY**.
10. Go back to **Manage Elements**.
11. Select Avaya Oceana® Cluster 2 node 1.
12. Repeat step 2 to step 6 for node 1.
13. Select Avaya Oceana® Cluster 2 node 2.
14. Repeat step 2 to step 6 for node 2.

    After you complete the configuration, you must reboot Avaya Oceana® Cluster 2. When the servers are online, change the state of Avaya Oceana® Cluster 2 to **Accept** mode.

Note:

If you are replacing a certificate, you must delete all instances of that certificate from System Manager and the Avaya Oceana® Cluster 2 servers before rebooting the Avaya Oceana® Cluster 2 nodes.

Importing the authorization certificate

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select the check box for the Avaya Breeze® platform node, and click **More Actions** > **Manage Identity Certificates**.
3. On the Manage Identity Certificates page, select **Authorization** and click **Replace**.
4. On the Replace Identity Certificate page, select the **Import third party certificate** option.
5. In the **Please select a file (PKCS#12 format)** field, browse and select the P12 file that you generate.
6. In the **Password** field, enter the password that you specified while creating the end entity.
7. Click **Commit**.
8. Repeat Step 2 to Step 7 for the other nodes of the cluster.
9. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
10. Select the cluster that contains AuthorizationService.
11. Click **Certificate Management** > **Update/Install Identity Certificate (Authorization Service)**.

    System Manager displays a message stating that the certificate has been updated successfully.
12. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Authorization**.
13. On the Authorization Configuration page, on the Clients tab, select **UnifiedAgentController**.
14. Click **Edit Grants**.
15. On the Edit Grants for Authorization Client page, click **New**.
16. In the **Resource Name** field, select **UnifiedAgentController**.
17. In the **Resource Cluster** field, select the cluster that contains UAC.
18. In the **Feature** field, select **desktop**.
19. Select the check box for **access**.

20. Click **Commit**.
21. Click **Done**.

Exporting the Avaya Breeze® platform Authorization Identity Certificate

About this task

Requests from clients to the Avaya Aura® Web Gateway server involves passing an authorization token in the request. The authorization is handled through Avaya Workspaces for Call Center Elite cluster 2 that hosts the *AuthorizationService* snapin. Avaya Aura® Web Gateway is a third-party server. Therefore, you must configure the Avaya Breeze® platform Authorization Certificate on Avaya Aura® Web Gateway.

An issue arises because each Avaya Breeze® platform node in the cluster has a different Authorization Identity Certificate and when load balancing is enabled between the nodes, some requests are rejected. To enable authorization on Avaya Aura® Web Gateway, you must first replace the Authorization Identity Certificate on each Avaya Breeze® platform node with a single System Manager generated identity certificate. Import this identity certificate into your Avaya Aura® Web Gateway.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select the check box for any of the Avaya Breeze® platform nodes with the new certificate, and click **More Actions** > **Manage Identity Certificates**.
3. On the Manage Identity Certificates page, select **Authorization** and click **Export**.
4. Save the `.pem` file on your local machine.

Chapter 8: Configure Session Manager routing

Configuration overview

This section describes how to configure Avaya Aura® Session Manager for Avaya Oceana®.

Avaya Aura® Session Manager is a SIP routing and integration tool that integrates all the SIP entities across the enterprise network within a company. Session Manager provides a core communication service that builds on existing equipment and adds a SIP-based architecture. Session Manager uses direct SIP connections and acts as a system-wide dial plan for call processing applications such as Avaya Aura® Communication Manager.

The SIP network components are known as SIP entities in an enterprise solution. The connections or trunks between Session Manager and the SIP network components are known as entity links. Each SIP entity connects to Session Manager and relies on Session Manager to route calls to the correct destination. This approach reduces the need for manual dial plan and trunking administration for each SIP Entity by consolidating administration in a central location on Avaya Aura® System Manager.

Note:

Use Avaya Aura® System Manager to configure Avaya Aura® Session Manager.

To support the out-of-box functionality in Avaya Oceana®, connect Experience Portal, Session Manager, and Communication Manager over SIP. Avaya Oceana® does not support H.323 connections between Experience Portal and Communication Manager.

Creating a routing location

About this task

Session Manager uses the origination location to determine the dial pattern when routing calls and to limit the number of calls coming from or going to a physical location.

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **Locations**.
2. On the Location page, click **New**.
3. In the **Name** field, enter the location name.
4. In the **Notes** field, enter a description about the location.

5. In the Dial Plan Transparency in Survivable Mode section, enter the Dial Plan Transperancy (DPT) parameters.
6. In the Overall Managed Bandwidth section, enter the parameters for the location.
7. In the Per-Call Bandwidth Parameters section, enter the average bandwidth per call for the location.
8. In the Alarm Threshold section, enter the alarm threshold percentage for audio and multimedia calls for the location.
9. In the Location Pattern section, click **Add**.
10. In the **IP address Pattern** field, enter the IP address pattern to match.
11. In the **Notes** field, enter a description about the location pattern.
12. Continue adding location pattern by clicking **Add** until you configure all the required location patterns.
13. Click **Commit**.

Creating a Session Initiation Protocol (SIP) entity for Session Manager

About this task

A SIP entity represents a SIP network element.

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **SIP Entities**.
2. On the SIP Entities page, click **New**.
3. In the **Name** field, enter a name for the SIP entity.
4. In the **FQDN or IP Address** field, enter the FQDN or IP address of the SIP entity.

   To add a SIP entity for Session Manager, you must enter the Security Module IP address instead of the Management IP address.
5. In the **Type** field, select **Session Manager**.
6. Click **Commit**.

Creating a SIP entity for Communication Manager

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **SIP Entities**.
2. Verify the SIP Entity for Communication Manager.

   If a SIP entity is not configured for Communication Manager, complete the remainder of this procedure.
3. On the SIP Entities page, click **New**.

4. In the **Name** field, enter a name for the SIP entity.
5. In the **FQDN or IP Address** field, enter the FQDN or IP address of the SIP entity.
6. In the **Type** field, select **CM**.
7. Click **Commit**.

Creating a SIP entity for Avaya Breeze® platform

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **SIP Entities**.
2. Verify the SIP Entity for Avaya Breeze® platform.

   If a SIP entity is not configured for Avaya Breeze® platform, complete the remainder of this procedure.
3. On the SIP Entities page, click **New**.
4. In the **Name** field, enter a name for the SIP entity.
5. In the **FQDN or IP Address** field, enter the FQDN or IP address of the SIP entity.

   To add a SIP Entity for Avaya Breeze® platform, you must enter the Security Module IP address instead of the Management IP address.
6. In the **Type** field, select **Avaya Breeze**.
7. Click **Commit**.

Creating a SIP entity for Experience Portal Media Processing Platform

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **SIP Entities**.
2. Verify the SIP Entity for Experience Portal Media Processing Platform.

   If a SIP entity is not configured for Experience Portal Media Processing Platform, complete the remainder of this procedure.
3. On the SIP Entities page, click **New**.
4. In the **Name** field, enter a name for the SIP entity.
5. In the **FQDN or IP Address** field, enter the FQDN or IP address of the SIP entity.
6. In the **Type** field, select **Voice Portal**.
7. Click **Commit**.

Creating an entity link from Session Manager to Experience Portal Media Processing Platform

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **Entity Links**.
2. Verify the entity link from the Session Manager SIP entity to Experience Portal Media Processing Platform SIP entity.

   If the entity link does not exist, complete the remainder of this procedure.
3. On the Entity Links page, click **New**.
4. Create an entity link between the Session Manager SIP entity to Experience Portal Media Processing Platform SIP entity.
5. Click **Commit**.

Creating an entity link from Session Manager to Communication Manager

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **Entity Links**.
2. Verify the entity link from the Session Manager SIP entity to Communication Manager SIP entity.

   If the entity link does not exist, complete the remainder of this procedure.
3. On the Entity Links page, click **New**.
4. Create an entity link between the Session Manager SIP entity to Communication Manager SIP entity.
5. Click **Commit**.

Creating a routing policy for the Experience Portal Media Processing Platform entity link

About this task

A routing policy defines how Session Manager routes calls between SIP network elements. Session Manager uses the data configured in the routing policy to find the best match against the number or address of the called party.

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **Routing Policies**.
2. Verify the routing policy for the Experience Portal Media Processing Platform entity link.

   If the routing policy does not exist, complete the remainder of this procedure.
3. On the Routing Policies page, click **New**.

4. In the **Name** field, enter a name for the routing policy.
5. In the **Retries** field, enter the number of retries.
6. In the SIP Entity as Destination section, click **Select**.
7. Select the Experience Portal Media Processing Platform SIP entity as the destination for the routing policy and click **Select**.
8. Click **Commit**.

Creating a routing policy for the Communication Manager entity link

About this task

A routing policy defines how Session Manager routes calls between SIP network elements. Session Manager uses the data configured in the routing policy to find the best match against the number or address of the called party.

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **Routing Policies**.
2. Verify the routing policy for the Communication Manager entity link.

   If the routing policy does not exist, complete the remainder of this procedure.
3. On the Routing Policies page, click **New**.
4. In the **Name** field, enter a name for the routing policy.
5. In the **Retries** field, enter the number of retries.
6. In the SIP Entity as Destination section, click **Select**.
7. Select the Communication Manager SIP entity as the destination for the routing policy and click **Select**.
8. Click **Commit**.

Creating Dial Patterns for Experience Portal Media Processing Platform Routing Policy

About this task

A Dial Pattern specifies a set of criteria and a set of Routing Policies for routing calls that match the criteria. The criteria include the called party number and SIP domain in the Request-URI, and the location from which the call originated. For example, if a call arrives at Session Manager and matches a certain Dial Pattern, then Session Manager selects one of the Routing Policies specified in the Dial Pattern. The selected Routing Policy in turn specifies the SIP Entity to which the call is to be routed.

Dial Patterns are matched after ingress Adaptations have already been applied.

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **Dial Patterns**.
2. On the Dial Patterns page, click **New**.
3. In the General section, perform the following steps:
   a. In the **Pattern** field, enter a pattern.

      The pattern can have 1 to 49 characters. The valid pattern formats for different pattern types are as follows:

      - For regular patterns, [+*#0-9x][0-9x]{0,35}
      - For pattern ranges, [+0-9][0-9]{0,23}[:][+0-9][0-9]{0,23}
      - For patterns with Emergency number, [0-9]{0,35}

      Note:

      If you specify a Dial Pattern range, the system disables the **Min**, **Max**, and **Emergency Call** fields.

   b. In the **Min** field, enter the minimum number of digits to match in the Dial Pattern.
   c. In the **Max** field, enter the maximum number of digits to match in the Dial Pattern.
   d. In the **SIP Domain** field, select the correct SIP domain for your environment.
4. In the Originating Locations and Routing Policies section, perform the following steps:
   a. Click **Add**.
   b. Select a Location.
   c. Select the appropriate Routing Policy.
   d. Click **Select**.
5. Click **Commit**.

Creating Dial Patterns for Communication Manager Routing Policy

About this task

Create a Dial Pattern using the Session Manager to Communication Manager Routing Policy. Session Manager uses this Dial Pattern to route calls to Communication Manager. A Dial Pattern specifies which Routing Policy or Routing Policies are used to route a call based on the digits dialed by a user which match that pattern. The originating location of the call and the domain in the request-URI also determine how the call gets routed.

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **Dial Patterns**.
2. On the Dial Patterns page, click **New**.

3. In the General section, perform the following steps:
    a. In the **Pattern** field, enter a pattern.

       The pattern can have 1 to 49 characters. The valid pattern formats for different pattern types are as follows:

       - For regular patterns, [+*#0-9x][0-9x]{0,35}
       - For pattern ranges, [+0-9][0-9]{0,23}[:][+0-9][0-9]{0,23}
       - For patterns with Emergency number, [0-9]{0,35}

       Note:

       If you specify a Dial Pattern range, the system disables the **Min**, **Max**, and **Emergency Call** fields.

    b. In the **Min** field, enter the minimum number of digits to match in the Dial Pattern.
    c. In the **Max** field, enter the maximum number of digits to match in the Dial Pattern.
    d. In the **SIP Domain** field, select the correct SIP domain for your environment.
4. In the Originating Locations and Routing Policies section, perform the following steps:
    a. Click **Add**.
    b. Select a Location.
    c. Select the appropriate Routing Policy.
    d. Click **Select**.
5. Click **Commit**.

Chapter 9: Deploy Avaya Oceana® clusters

Deploy Avaya Oceana® clusters

Avaya Oceana® includes the following clusters:

- Avaya Oceana® Cluster 1
- Avaya Oceana® Cluster 2
- Avaya Oceana® Cluster 3
- Avaya Oceana® Cluster 4
- Avaya Oceana® Cluster 5
- Provisioning Cluster

Important:

These clusters are for the exclusive use of Avaya Oceana®. Therefore, do not install any third-party or custom Service Archives (SVARs) on these clusters.

For an Avaya Oceana® deployment that supports up to 100 active agents:

- Do not create Avaya Oceana® Cluster 2 and Avaya Oceana® Cluster 5.
- Install the following SVARs of Avaya Oceana® Cluster 2 on Avaya Oceana® Cluster 1:
  - AuthorizationService
  - AvayaMobileCommunications
  - BotConnector
  - UnifiedAgentContextService
  - UnifiedAgentController
- Install the CRMGateway SVAR on Avaya Oceana® Cluster 1.
- Install the ZangSmsConnector snap-in on Avaya Oceana® Cluster 3.

A cluster provides scaling by distributing the services across multiple Avaya Breeze® platform nodes. With this distribution of services, the system achieves overall throughput and avoids interruption in the event of failure. Clients access the services through a Cluster IP address that supports high availability.

Verifying the host name resolution for Avaya Breeze® platform nodes

Procedure

1. Register the fully qualified domain names (FQDNs) of the following servers and virtual machines with a Domain Name System (DNS) server:
   - System Manager
   - Avaya Oceana® Cluster 1 IP address and FQDN
   - Avaya Oceana® Cluster 2 IP address and FQDN

     Register the IP address and FQDN of Avaya Oceana® Cluster 2 for an Avaya Oceana® deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents.
   - Avaya Oceana® Cluster 3 IP address and FQDN
   - Avaya Oceana® Cluster 4 IP address and FQDN
   - Avaya Oceana® Cluster 5 IP address and FQDN

     Register the IP address and FQDN of Avaya Oceana® Cluster 5 for an Avaya Oceana® deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents.
   - Omnichannel Windows Server 2019 (Desktop Experience)
   - Avaya Breeze® platform node host names
   - Avaya Breeze® platform security IP addresses

   Important:

   - If you do not complete this step, the Avaya Breeze® platform replication does not synchronize for each node. Failure to synchronize prevents the deployment from completing.
   - The returned DNS record is case-sensitive. Therefore, it must exactly match the node.
   - You must deploy minimum two DNS servers to have the Highly Available DNS server capability. If you only have as single DNS server and it goes down, Avaya Breeze® platform/Avaya Breeze® platform ceases to operate.
2. Verify that System Manager can resolve the host name of Avaya Breeze® platform nodes.

   Note:

   The following Avaya Analytics™ features are not supported when Avaya Breeze® platform nodes have `.local` domain name:

   - Avaya Analytics™ kafka open interface is not supported. It affects WFO integration and custom applications.
   - Avaya Analytics™ websocket open interface is not supported. It affects Agent Wallboard and other custom applications.

- GDPR feature is not supported.

Loading license files in System Manager

About this task

Use this procedure to load the license files for Avaya Breeze® platform nodes and services that are used in Avaya Oceana®.

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. Click **Install License**.
3. On the Install License page, perform the following steps:
   a. Browse to the location of the license that you want to install and select the license file.
   b. Click **Accept the License Terms & Conditions**.
   c. Click **Install**.

      The system installs the license.
4. In the navigation pane, click **Licensed Products** to view the installed license.
5. Perform steps 2 through 4 to install the license for the following services:
   - Context_Store
   - COLLABORATION_ENVIRONMENT (For the Avaya Breeze® platform)
   - Avaya_Oceana

     This license also covers UCM_Reporting.
   - Collaborative_Browsing_Snap_In
   - Work_Assignment
   - Collaboration_Designer
   - Control_Manager
6. In the navigation pane, click **WebLM Home** to verify that the WebLM Home page displays all the licenses.
7. After the services are running, perform the following steps to verify the licenses:
   a. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
   b. On the Services page, verify that the **License Mode** column for all the services displays a check mark.

Installation of Avaya Oceana® snap-ins

The manual installation method is available for installing Avaya Oceana® snap-ins:

Manual installation checklist

Use the following checklist for manual installation of Avaya Oceana® SVARs:

No.	Task	Description	✔
1	Load SVARs in System Manager.	See Loading SVARs in System Manager on page 101.	
2	Create Avaya Oceana® clusters.	See: • Creating Avaya Oceana Cluster 1 on page 105 • Creating Avaya Oceana Cluster 2 on page 108 • Creating Avaya Oceana Cluster 3 on page 110 • Creating Avaya Oceana Cluster 4 on page 113 • Creating Avaya Oceana Cluster 5 on page 114	
3	Create Provisioning Cluster.	See Creating Provisioning Cluster on page 116.	
4	Set OceanaConfiguration attributes.	See Setting OceanaConfiguration attributes on page 117.	
5	Add Avaya Breeze® platform nodes to clusters.	See: • Adding nodes to Avaya Oceana Cluster 1 on page 127 • Adding nodes to Avaya Oceana Cluster 2 on page 128 • Adding nodes to Avaya Oceana Cluster 3 on page 129 • Adding nodes to Avaya Oceana Cluster 4 on page 130 • Adding nodes to Avaya Oceana Cluster 5 on page 131	

Table continues…

No.	Task	Description	✔
6	Verify the status of Avaya Breeze® platform nodes.	See Verifying the status of Avaya Breeze platform nodes on page 132.	
7	Set the state of all clusters to Accepting.	See Setting Cluster State to Accepting on page 133.	
8	Enable CORS for clusters.	See Enabling CORS for clusters on page 133.	

Loading SVARs in System Manager

About this task

Use this procedure to load the following Avaya Breeze® platform Service Archive (SVARs) of Avaya Oceana® clusters in System Manager:

Cluster name	SVAR
Avaya Oceana® Cluster 1	• CallServerConnector (Required only for Voice) • ContactCenterService • ContextStoreManager • ContextStoreQuery • ContextStoreRest • CustomerJourneyService • CustomerManagement • EngagementDesigner • MetricbeatService This is an optional SVAR, which is used for Centralized Logging. If you do not need Centralized Logging, do not install this SVAR and free up some CPU cycles for contact processing. • OCPDataServices • OceanaCoreDataService • OceanaMonitorService • OmniCenterProvisioningCollector (Required only for Avaya Analytics™) • PacketbeatService This is an optional SVAR, which is used for Centralized Logging. If you do not need Centralized Logging, do not install this SVAR and free up some CPU cycles for contact processing. • UCAStoreService • UCMDataCollector • UCMService • WAIMRestService • WorkAssignmentManagerService

Table continues…

Cluster name	SVAR
Avaya Oceana® Cluster 2	• AuthorizationService • AvayaMobileCommunications (Required only for Web Voice/Video) • BotConnector • MetricbeatService This is an optional SVAR, which is used for Centralized Logging. If you do not need Centralized Logging, do not install this SVAR and free up some CPU cycles for contact processing. • OceanaMonitorService • PacketbeatService This is an optional SVAR, which is used for Centralized Logging. If you do not need Centralized Logging, do not install this SVAR and free up some CPU cycles for contact processing. • UnifiedAgentContextService • UnifiedAgentController

Table continues…

Cluster name	SVAR
Avaya Oceana® Cluster 3	• AgentControllerService • AutomationController (Required only for the Bot integration) • CustomerControllerService • EmailService (Required only for Email) • GenericChannelAPI • MessagingService (Required only for Short Message Service and Social Media) • MetricbeatService This is an optional SVAR, which is used for Centralized Logging. If you do not need Centralized Logging, do not install this SVAR and free up some CPU cycles for contact processing. • OBCService (Required only for Outbound) • ORCRestService • OceanaDataViewer • OceanaMonitorService • PacketbeatService This is an optional SVAR, which is used for Centralized Logging. If you do not need Centralized Logging, do not install this SVAR and free up some CPU cycles for contact processing. • SocialConnector (Required only for Social Media) • ZangSmsConnector
Avaya Oceana® Cluster 4	• CoBrowse • OceanaMonitorService
Avaya Oceana® Cluster 5	• CRMGateway • ZangSmsConnector (For more than 100-Agent deployments) • OceanaMonitorService
Provisioning Cluster	OceanaConfiguration

Before you begin

- Remove the older versions of SVARs.
- Download the latest versions of SVARs from PLDS.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. On the Services page, click **Load**.
3. In the Load Service dialog box, do the following:
   a. Click **Browse**.
   b. Select the SVAR and click **Open**.
   c. To load multiple SVARs at the same time, repeat Steps a and b for each SVAR.

      Note:

      You can select up to 50 files or a maximum of 3 GB files whichever limit is reached first.

   d. Click **Load**.
4. In the Accept End User License Agreement dialog box, click **Accept**.

   If you load multiple SVARs at the same time, you must click **Accept** for each SVAR.
5. On the Services page, verify that the state of the SVARs is `Loaded`.

Creating Avaya Oceana® Cluster 1

About this task

Use this procedure to create Avaya Oceana® Cluster 1.

Note:

Do not add nodes to the cluster while creating the cluster.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, click **New**.
3. On the Cluster Editor page, select the **General** tab.
4. In the Basic section, perform the following steps:
   a. In the **Cluster Profile** field, select **Customer Engagement**.
   b. In the **Cluster Name** field, enter a unique cluster name.

      The name must be a string of Alphanumeric characters. For example, `AvayaOceanaCluster1`.

c. In the **Cluster Group** field, select a cluster group.

Important:

Select the same cluster group for all clusters of Avaya Oceana® and ensure that you do not use the selected cluster group for any non-Avaya Oceana® cluster.

d. In the **Cluster IP** field, enter the IP address of the cluster.

The IP address of the cluster must be on the same subnet as the Security Module IP address of the Avaya Breeze® platform nodes that you plan to add to the cluster.

Ensure that you do not specify the IP address of any of the Avaya Breeze® platform nodes that you plan to add to the cluster.

The system uses the IP address of the cluster as the load balancer. The system does not provide an option to select Avaya Breeze® platform instances within the cluster for load balancing.

e. In the **Cluster Fully Qualified Domain Name** field, enter the FQDN of the cluster.

f. Select the **Enable Cluster Database** check box.

g. In the **Description** field, enter a description for the cluster.

5. In the Cluster Attributes section, perform the following steps:

a. If the AuthorizationService snap-in is installed on Avaya Oceana® Cluster 1, then in the **Authorization Services Address** field, enter the FQDN of Avaya Oceana® Cluster 1.

b. Increase the value of the attribute **Http or Https limit on connections** per client from the default value of 100, so that the cluster supports more connections simultaneously.

The suggested value is 6000.

c. In the **HTTP Load Balancer backend server max failure response timeout period (seconds)** field, type `60`.

d. In the **Max number of failure responses from HTTP Load Balancer backend server** field, type `10`.

e. In the **Network connection timeout to HTTP Load Balancer backend server (seconds)** field, type `3`.

f. Select or clear the **Only allow secure web communications** check box based on your requirement.

g. Clear the **Is load balancer enabled** check box.

Important:

After adding Avaya Breeze® platform nodes to the cluster, you must edit the cluster and select this check box.

h. Clear the **Is session affinity enabled** check box.

i. In the **Default SIP Domain** field, enter the default SIP domain for the cluster.

For a description of Cluster Attributes, see *Administering Avaya Breeze® platform*.

Important:

For the Avaya Oceana® deployment that supports up to 100 active agents, change the value of the **Limit on the memory (GB) to allocate for WAS** field to 6.

6. On the Cluster Editor page, select the **Services** tab.

   The system automatically adds CallEventControl and EventingConnector SVARs to the Assigned Services list.

7. In the Available Services list, click the plus sign **(+)** on the following SVARs to add the SVARs to Avaya Oceana® Cluster 1:

   - CallServerConnector
   - ContactCenterService
   - ContextStoreManager
   - ContextStoreQuery
   - ContextStoreRest
   - CustomerJourneyService
   - CustomerManagement
   - EngagementDesigner
   - MetricbeatService

     This is an optional SVAR, which is used for Centralized Logging. If you do not need Centralized Logging, do not install this SVAR and free up some CPU cycles for contact processing.
   - OCPDataServices
   - OceanaCoreDataService
   - OceanaMonitorService
   - OmniCenterProvisioningCollector
   - PacketbeatService

     This is an optional SVAR, which is used for Centralized Logging. If you do not need Centralized Logging, do not install this SVAR and free up some CPU cycles for contact processing.
   - UCAStoreService
   - UCMDataCollector
   - UCMService
   - WAIMRestService

- WorkAssignmentManagerService

For an Avaya Oceana® deployment that supports up to 100 active agents, ensure that you also add the following SVARs to Avaya Oceana® Cluster 1:

- AuthorizationService
- AvayaMobileCommunications
- BotConnector
- UnifiedAgentContextService
- UnifiedAgentController
- CRMGateway

8. **(Optional)** Perform the following steps if your solution supports Avaya Analytics™:
   a. On the Cluster Editor page, select the **Reliable Eventing Groups** tab.
   b. Configure the Reliable Eventing group for Avaya Oceana® Cluster 1.

      For more information, see *Deploying Avaya Analytics™ for Avaya Oceana®*.
9. Click **Commit**.

   The system prompts you to ensure that you restart all Avaya Breeze® platform nodes before placing the cluster into the Accept New Service state.
10. Click **OK**.

Creating Avaya Oceana® Cluster 2

About this task

Use this procedure to create Avaya Oceana® Cluster 2.

Note:

- For an Avaya Oceana® deployment that supports up to 100 active agents, do not create Avaya Oceana® Cluster 2 and install the SVARs of Avaya Oceana® Cluster 2 on Avaya Oceana® Cluster 1.
- Do not add nodes to the cluster while creating the cluster.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, click **New**.
3. On the Cluster Editor page, select the **General** tab.
4. In the Basic section, perform the following steps:
   a. In the **Cluster Profile** field, select **Customer Engagement**.
   b. In the **Cluster Name** field, enter a unique cluster name.

      The name must be a string of Alphanumeric characters. For example, `AvayaOceanaCluster2`.

c. In the **Cluster Group** field, select a cluster group.

Important:

Select the same cluster group for all clusters of Avaya Oceana® and ensure that you do not use the selected cluster group for any non-Avaya Oceana® cluster.

d. In the **Cluster IP** field, enter the IP address of the cluster.

The IP address of the cluster must be on the same subnet as the Security Module IP address of the Avaya Breeze® platform nodes that you plan to add to the cluster.

Ensure that you do not specify the IP address of any of the Avaya Breeze® platform nodes that you plan to add to the cluster.

The system uses the IP address of the cluster as the load balancer. The system does not provide an option to select Avaya Breeze® platform instances within the cluster for load balancing.

e. In the **Cluster Fully Qualified Domain Name** field, enter the FQDN of the cluster.

f. Select the **Enable Cluster Database** check box.

g. In the **Description** field, enter a description for the cluster.

5. In the Cluster Attributes section, perform the following steps:

a. If the AuthorizationService snap-in is installed on Avaya Oceana® Cluster 2, then in the **Authorization Services Address** field, enter the FQDN of Avaya Oceana® Cluster 2.

b. Increase the value of the attribute **Http or Https limit on connections** per client from the default value of 100, so that the cluster supports more connections simultaneously.

The suggested value is 6000.

c. In the **HTTP or HTTPS traffic rate limit in bytes/sec per client** field, set the value to 5000000.

d. In the **HTTP Load Balancer backend server max failure response timeout period (seconds)** field, type `60`.

e. In the **Max number of failure responses from HTTP Load Balancer backend server** field, type `10`.

f. In the **Network connection timeout to HTTP Load Balancer backend server (seconds)** field, type `3`.

g. Select or clear the **Only allow secure web communications** check box based on your requirement.

h. Clear the **Is load balancer enabled** check box.

Important:

After adding Avaya Breeze® platform nodes to the cluster, you must edit the cluster and select this check box.

i. Clear the **Is session affinity enabled** check box.

For a description of Cluster Attributes, see *Administering Avaya Breeze® platform*.

6. On the Cluster Editor page, select the **Services** tab.

   The system automatically adds the CallEventControl and EventingConnector SVARs to the Assigned Services list.

7. In the Available Services list, click the plus sign **(+)** on the following SVARs to add the SVARs to Avaya Oceana® Cluster 2:

   - AuthorizationService
   - AvayaMobileCommunications
   - BotConnector
   - MetricbeatService

     This is an optional SVAR, which is used for Centralized Logging. If you do not need Centralized Logging, do not install this SVAR and free up some CPU cycles for contact processing.

   - OceanaMonitorService
   - PacketbeatService

     This is an optional SVAR, which is used for Centralized Logging. If you do not need Centralized Logging, do not install this SVAR and free up some CPU cycles for contact processing.

   - UnifiedAgentContextService
   - UnifiedAgentController

8. Click **Commit**.

   The system prompts you to ensure that you restart all Avaya Breeze® platform nodes before placing the cluster into the Accept New Service state.

9. Click **OK**.

Creating Avaya Oceana® Cluster 3

About this task

Use this procedure to create Avaya Oceana® Cluster 3.

Note:

Do not add nodes to the cluster while creating the cluster.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, click **New**.
3. On the Cluster Editor page, select the **General** tab.
4. In the Basic section, perform the following steps:
   a. In the **Cluster Profile** field, select **Customer Engagement**.
   b. In the **Cluster Name** field, enter a unique cluster name.

      The name must be a string of Alphanumeric characters. For example, `AvayaOceanaCluster3`.
   c. In the **Cluster Group** field, select a cluster group.

      Important:

      Select the same cluster group for all clusters of Avaya Oceana® and ensure that you do not use the selected cluster group for any non-Avaya Oceana® cluster.
   d. In the **Cluster IPv4** field, enter the IP address of the cluster.

      The IP address of the cluster must be on the same subnet as the Security Module IP of the Avaya Breeze® platform nodes that you plan to add to the cluster.

      Ensure that you do not specify the IP address of any of the Avaya Breeze® platform nodes that you plan to add to the cluster.

      The system uses the IP address of the cluster as the load balancer. The system does not provide an option to select Avaya Breeze® platform instances within the cluster for load balancing.
   e. In the **Cluster Fully Qualified Domain Name** field, enter the FQDN of the cluster.
   f. Select the **Enable Cluster Database** check box.
   g. In the **Description** field, enter a description for the cluster.
5. In the Cluster Attributes section, perform the following steps:
   a. Increase the value of the attribute **Http or Https limit on connections** per client from the default value of 100, so that the cluster supports more connections simultaneously.

      The suggested value is 6000.
   b. In the **HTTP or HTTPS traffic rate limit in bytes/sec per client** field, type `5000000`.
   c. In the **HTTP Load Balancer backend server max failure response timeout period (seconds)** field, type `60`.
   d. In the **Max number of failure responses from HTTP Load Balancer backend server** field, type `10`.

e. In the **Network connection timeout to HTTP Load Balancer backend server (seconds)** field, type 3.

f. Select or clear the **Only allow secure web communications** check box based on your requirement.

g. Clear the **Is load balancer enabled** check box.

Important:

After adding Avaya Breeze® platform nodes to the cluster, you must edit the cluster and select this check box.

For a description of Cluster Attributes, see *Administering Avaya Breeze® platform*.

h. For only the Avaya Oceana® deployment that supports up to 1000 active agents, change the value of the **Limit on the memory (GB) to allocate for WAS** field to 6.

6. On the Cluster Editor page, select the **Services** tab.

The system automatically adds CallEventControl and EventingConnector SVARs to the Assigned Services list.

7. In the Available Services list, click the plus sign **(+)** on the following SVARs to add the SVARs to Avaya Oceana® Cluster 3:

- AgentControllerService
- AutomationController
- CustomerControllerService
- EmailService
- GenericChannelAPI
- MessagingService
- MetricbeatService

  This is an optional SVAR that is used for Centralized Logging. If you do not need Centralized Logging, do not install this SVAR and free up some CPU cycles for contact processing.
- OBCService
- ORCRestService
- OceanaDataViewer
- OceanaMonitorService
- PacketbeatService

  This is an optional SVAR that is used for Centralized Logging. If you do not need Centralized Logging, do not install this SVAR and free up some CPU cycles for contact processing.
- SocialConnector

For an Avaya Oceana® deployment that supports up to 100 active agents, ensure that you also add the following SVARs to Avaya Oceana® Cluster 3:

- ZangSmsConnector

8. Click **Commit**.

   The system prompts you to ensure that you restart all Avaya Breeze® platform nodes before placing the cluster into the Accept New Service state.

9. Click **OK**.

Creating Avaya Oceana® Cluster 4

About this task

Use this procedure to create Avaya Oceana® Cluster 4.

Note:

- For an Avaya Oceana® deployment that supports up to 100 active agents, do not create Avaya Oceana® Cluster 4 if you do not require the Co-Browsing feature.
- Do not add nodes to the cluster while creating the cluster.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, click **New**.
3. On the Cluster Editor page, select the **General** tab.
4. In the Basic section, perform the following steps:
   a. In the **Cluster Profile** field, select **Customer Engagement**.
   b. In the **Cluster Name** field, enter a unique cluster name.

      The name must be a string of Alphanumeric characters. For example, `AvayaOceanaCluster4`.

   c. In the **Cluster Group** field, select a cluster group.

      Important:

      Select the same cluster group for all clusters of Avaya Oceana® and ensure that you do not use the selected cluster group for any non-Avaya Oceana® cluster.

   d. In the **Cluster IP** field, enter the IP address of the cluster.

      The IP address of the cluster must be on the same subnet as the Security Module IP of the Avaya Breeze® platform nodes that you plan to add to the cluster.

      Ensure that you do not specify the IP address of any of the Avaya Breeze® platform nodes that you plan to add to the cluster.

The system uses the IP address of the cluster as the load balancer. The system does not provide an option to select Avaya Breeze® platform instances within the cluster for load balancing.

e. In the **Cluster Fully Qualified Domain Name** field, enter the FQDN of the cluster.

f. Select the **Enable Cluster Database** check box.

g. In the **Description** field, enter a description for the cluster.

5. In the Cluster Attributes section, perform the following steps:

a. In the **Max number of failure responses from HTTP Load Balancer backend server** field, type `10`.

b. In the **Network connection timeout to HTTP Load Balancer backend server (seconds)** field, type `3`.

c. Select or clear the **Only allow secure web communications** check box based on your requirement.

d. Clear the **Is load balancer enabled** check box.

Important:

After adding Avaya Breeze® platform nodes to the cluster, you must edit the cluster and select this check box.

e. Select the **Is session affinity enabled** check box.

For a description of Cluster Attributes, see *Administering Avaya Breeze® platform*.

6. On the Cluster Editor page, select the **Services** tab.

The system automatically adds the CallEventControl and EventingConnector SVARs to the Assigned Services list.

7. In the Available Services list, click the plus sign **(+)** on the following SVARs to add the SVARs to Avaya Oceana® Cluster 4:

- CoBrowse
- OceanaMonitorService

8. Click **Commit**.

The system prompts you to ensure that you restart all Avaya Breeze® platform nodes before placing the cluster into the Accept New Service state.

9. Click **OK**.

Creating Avaya Oceana® Cluster 5

About this task

Use this procedure to create Avaya Oceana® Cluster 5.

Note:

- Do not add nodes to the cluster while creating the cluster.

- Avaya Oceana® Cluster 5 is an optional cluster.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, click **New**.
3. On the Cluster Editor page, select the **General** tab.
4. In the Basic section, perform the following steps:
   a. In the **Cluster Profile** field, select **Customer Engagement**.
   b. In the **Cluster Name** field, enter a unique cluster name.

      The name must be a string of Alphanumeric characters. For example, `AvayaOceanaCluster5`.
   c. In the **Cluster Group** field, select a cluster group.
   d. In the **Cluster IP** field, enter the IP address of the cluster.

      The IP address of the cluster must be on the same subnet as the Security Module IP of the Avaya Breeze® platform nodes that you plan to add to the cluster.

      Ensure that you do not specify the IP address of any of the Avaya Breeze® platform nodes that you plan to add to the cluster.

      The system uses the IP address of the cluster as the load balancer. The system does not provide an option to select Avaya Breeze® platform instances within the cluster for load balancing.
   e. In the **Cluster Fully Qualified Domain Name** field, enter the FQDN of the cluster.
   f. Select the **Enable Cluster Database** check box.
   g. In the **Description** field, enter a description for the cluster.
5. In the Cluster Attributes section, perform the following steps:
   a. Increase the value of the attribute **Http or Https limit on connections** per client from the default value of 100, so that the cluster supports more connections simultaneously.

      The suggested value is 6000.
   b. In the **Max number of failure responses from HTTP Load Balancer backend server** field, type `10`.
   c. In the **Network connection timeout to HTTP Load Balancer backend server (seconds)** field, type `3`.
   d. Select or clear the **Only allow secure web communications** check box based on your requirement.
   e. Clear the **Is load balancer enabled** check box.

Important:

After adding Avaya Breeze® platform nodes to the cluster, you must edit the cluster and select this check box.

For a description of Cluster Attributes, see *Administering Avaya Breeze® platform*.

6. On the Cluster Editor page, select the **Services** tab.

   The system automatically adds CallEventControl and EventingConnector SVARs to the Assigned Services list.

7. In the Available Services list, click the plus sign **(+)** on the following SVARs to add the SVARs to Avaya Oceana® Cluster 5:

   - CRMGateway
   - ZangSmsConnector
   - OceanaMonitorService

8. Click **Commit**.

   The system prompts you to ensure that you restart all Avaya Breeze® platform nodes before placing the cluster into the Accept New Service state.

9. Click **OK**.

Creating Provisioning Cluster

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, click **New**.
3. On the Cluster Editor page, select the **General** tab.
4. In the Basic section, perform the following steps:
   a. In the **Cluster Profile** field, select **Customer Engagement**.
   b. In the **Cluster Name** field, enter a unique cluster name.

      The name must be a string of Alphanumeric characters. For example, `ProvisioningCluster`.

   c. In the **Cluster Group** field, select a cluster group.

      Important:

      Select the same cluster group for all clusters of Avaya Oceana® and ensure that you do not use the selected cluster group for any non-Avaya Oceana® cluster.

   d. Leave the **Cluster IP** field blank.
   e. Leave the **Cluster Fully Qualified Domain Name** field blank.
   f. In the **Description** field, enter a description for the cluster.

Note:

Provisioning Cluster does not require any Avaya Breeze® platform node. Therefore, you must skip the **Servers** tab.

5. On the Cluster Editor page, select the **Services** tab.

   The system automatically adds the CallEventControl and EventingConnector SVARs to the Assigned Services list.

6. In the Available Services list, click the plus sign **(+)** on the OceanaConfiguration SVAR to add the SVAR to Provisioning Cluster.
7. Click **Commit**.

   The system prompts you to ensure that you restart all Avaya Breeze® platform nodes before placing the cluster into the Accept New Service state.

8. Click **OK**.

Setting OceanaConfiguration attributes

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In the **Cluster** field, select **ProvisioningCluster**.
   b. In the **Service** field, select **OceanaConfiguration**.
3. Configure OceanaConfiguration attributes.
4. Click **Commit**.

   You can also configure the attributes of each service of Avaya Oceana® individually. For information about the attributes of the services that you install on Avaya Oceana® clusters, see Service attributes overview on page 756.

Important:

When you configure an attribute through OceanaConfiguration, System Manager overrides the snap-in attribute value already set at the service level.

OceanaConfiguration attributes

Deployment

Name	Description
Deployment Type	The type that determines the deployment size for the installation. • For an Avaya Oceana® deployment that supports up to 4500 active agents, select `3X Large`. • For an Avaya Oceana® deployment that supports up to 2000 active agents, select `Extra Large`. • For an Avaya Oceana® deployment that supports up to 1000, 500, or 250 active agents, select `Large`. • For an Avaya Oceana® deployment that supports up to 100 active agents, select `Small`.
Locale	The locale or language for the installation.
Secure Communications	The attribute that enables or disables the secure communications across the clusters in the installation. For Https-only and wss-only connections across the clusters, select `Enabled`.
Allow Tokenless Access	This is used to allow requests to access resource end-points, even if there is no Authorization token. Set to false if all clients must have an Authorization Token

Clusters

Name	Description
Common Cluster	To set this attribute, select Avaya Oceana® Cluster 1.
Context Store Cluster	The cluster that hosts Context Store services. To set this attribute, select Avaya Oceana® Cluster 1.
Co-Browse Cluster	The cluster that hosts the CoBrowse service. To set this attribute, select Avaya Oceana® Cluster 4.
OCP Cluster	The cluster that hosts Omnichannel Provider services. To set this attribute, select Avaya Oceana® Cluster 3.

Table continues…

Name	Description
Customer Management Cluster	The cluster that hosts the CustomerManagement service. To set this attribute, select Avaya Oceana® Cluster 1.
Chatbot Cluster	The cluster that hosts the BotConnector service. • For an Avaya Oceana® deployment that supports up to 100 active agents, select Avaya Oceana® Cluster 1. • For an Avaya Oceana® deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, select Avaya Oceana® Cluster 2.
Unified Agent Cluster	The cluster that hosts Unified Agent services. • For an Avaya Oceana® deployment that supports up to 100 active agents, select Avaya Oceana® Cluster 1. • For an Avaya Oceana® deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, select Avaya Oceana® Cluster 2.
Authorization Services Address	The Fully Qualified Domain Name or IP of the cluster where Authorization Service is installed. **Note:** This is a mandatory attribute.

Monitoring

Name	Description
Cluster Monitor 1	The first cluster that you want to monitor through OceanaMonitorService. To set this attribute, select Avaya Oceana® Cluster 1.
Cluster Monitor 2	The second cluster that you want to monitor through OceanaMonitorService. To set this attribute, select Avaya Oceana® Cluster 2.
Cluster Monitor 3	The third cluster that you want to monitor through OceanaMonitorService. To set this attribute, select Avaya Oceana® Cluster 3.

Table continues…

Name	Description
Cluster Monitor 4	The fourth cluster that you want to monitor through OceanaMonitorService. To set this attribute, select Avaya Oceana® Cluster 4.
Cluster Monitor 5	The fifth cluster that you want to monitor through OceanaMonitorService. Do not select any value for this attribute.
EASG authorization enabled in Oceana Monitor	The attribute that enables or disables EASG authorization for the Oceana Monitor. • To enable EASG authentication, keep the default value `true`. • To disable EASG authentication, select `false`. Restart the snap-in for the changes to reflect.
Voice Channel	If the Avaya Oceana® deployment has the Voice Channel feature, select `true`.
Video Channel	If the Avaya Oceana® deployment has the Video Channel feature, select `true`.
Chat Channel	If the Avaya Oceana® deployment has the Chat Channel feature, select `true`.
Email Channel	If the Avaya Oceana® deployment has the Email Channel feature, select `true`.
SMS Channel	If the Avaya Oceana® deployment has the SMS Channel feature, select `true`.
Social Channel	If the Avaya Oceana® deployment has the Social Channel feature, select `true`.
Generic Channel	If the Avaya Oceana® deployment has the Generic Channel feature, select `true`.
Asynchronous Messaging Channel	If the Avaya Oceana® deployment has the Asynchronous Messaging Channel feature, select `true`.
Customer Journey	If the Avaya Oceana® deployment has the Customer Journey feature, select `true`.
Reporting	If the Avaya Oceana® deployment has the Reporting feature, select `true`.
Outbound	If the Avaya Oceana® deployment has the Outbound Channel feature, select `true`.
Automation	If the Avaya Oceana® deployment has the Automation feature, select `true`.

Geo-Redundancy

Name	Description
Disaster Recovery Mode	The geo-redundancy mode for this system. For a standalone deployment, set this to Standalone. For a geographical disaster recovery deployment, set this attribute to Geo Primary on the primary site, and Geo Secondary on the secondary site.
Geo-Redundant Common Cluster	A mandatory attribute configured on a geographical disaster recovery deployment.
Keystore file name	Certificate name of the geo-redundancy keystore.
Keystore password	The password of the geo-redundancy keystore.

Voice

Name	Description
Voice Provider Id	The name of the Voice provider (Type:CM) that you plan to configure in Avaya Control Manager.
Application Enablement Services' IP addresses	The IP address of the Application Enablement Services server that you plan to connect to Communication Manager through a TSAPI link. If two instances of Application Enablement Services are used for HA, click the plus sign (**+**) and add the second instance of Application Enablement Services.
Communication Manager Connection Name on Application Enablement Services	The name of the Communication Manager switch connection that you plan to configure on Application Enablement Services. If two instances of Application Enablement Services are used for HA, the same name must be configured for both instances.
AES user	The user name of the Application Enablement Services account. If two instances of Application Enablement Services are used for HA, the same user name must be configured for both instances.
AES user password	The password of the Application Enablement Services account. If two instances of Application Enablement Services are used for HA, the same password must be configured for both instances.

Multimedia

Name	Description
Omnichannel Database Address	The FQDN or IP address of Omnichannel Database.
Username for the Omnichannel Database	The user name for Omnichannel Database. The default user name for Omnichannel Database is `mmJava`.
Password for the Omnichannel Database	The password for Omnichannel Database. The default password for Omnichannel Database is `mmJav`. **Important:** If you change the password for Omnichannel Database through Cache Management Portal, you must also enter the same password in the field.
Secure Connections to Omnichannel Database	The attribute that toggles a secure connection to Omnichannel Database. To set this attribute, select `true`.
Public OCP FQDN/IP Address	The Fully Qualified Domain Name or IP address of the Omnichannel Provider (OCP).

Video

Name	Description
Default Web Voice SIP address	The number that you plan to configure in Engagement Designer Event Mapper to trigger the Web Voice workflow.
Default Video SIP address	The number that you plan to configure in Engagement Designer Event Mapper to trigger the Web Video workflow.
Fully Qualified Domain Name (FQDN) for the Avaya Aura Web Gateway	The FQDN of Avaya Aura® Web Gateway. **Important:** Do not enter an IP address in this field.

Unified Agent Client

Name	Description
Log Upload Location	The location of the shared network folder that all Unified Agent clients can access to upload the logs when the agents select the Upload option. Unified Agent clients are the clients that are running remotely on the agent's computer.
AADS FQDN	The Avaya Aura® Device Services (AADS) FQDN, which the Avaya Workspaces address book uses to search for enterprise directory contacts using LDAP.

External Data Mart

Name	Description
External Data Mart Persistence Type	The attribute that specifies how the Context Store data is stored in the EDM. For more information, see the *External Data Mart persistence* section in the *Avaya Context Store Snap-in Reference* guide. The options are: • **Audit**: Enables persistence of Audit context data to EDM. • **Journey**: Enables persistence of Customer Journey and Context Resurrection related data to EDM. **Important:** Avaya Oceana® deployments must use a persistence type of Journey.
External Data Mart Database Type	The type of the EDM database. The available value for both upgrading to Avaya Oceana® Release 3.8 and new Avaya Oceana® Release 3.8 deployment is Microsoft SQL Server.
External Data Mart FQDN	The FQDN of the EDM database. **Important:** For MS SQL Always On HA, use the FQDN of the Availability Group listener.
External Data Mart Port	The port number of the EDM database.
External Data Mart Database Name	The name of the EDM database.
External Data Mart Username	The user name of the EDM database.

Table continues…

Name	Description
External Data Mart Password	The password for the user specified in the External Data Mart Username attribute.
Secure Connections to EDM	Specifies if communications between the Context Store and the EDM should use a secure connection. The default value is true. **Note:** For unsecured connections from Avaya Oceana® to EDM, you must set the value to false. Unsecured EDM connections are for lab use only. They are not intended for Avaya Oceana® instances that conform to security policies.
EDM: TLS version	The version of TLS to use when connecting to EDM. The supported versions are: • TLSv1.2 • TLSv1.1 • TLSv1.0
Disable persistence of personally identifiable data	When you set this attribute to `true`, External Data Mart (EDM) stops storing the following types of data: • Any digits collected during self-service • Custom data entered in the in the **Data** field. EDM stops storing these types of personally identifiable data to comply with data privacy laws.

Engagement Designer

Name	Description
Delete instances on completion	The attribute that enables or disables the deletion of completed instances. For Avaya Oceana®, select `true`.
Media Server Inclusion	The attribute that enables or disables the inclusion of Avaya Aura® Media Server. To configure Avaya Oceana® for Web Voice/Video, select `true`.
Chatbot Site Identifier	A comma separated string of BotConnector Site IDs in the `Site Id:Friendly Name` format.

Messaging Connection Service

Name	Description
Snap-in Service 1 Name	The name of the first MessagingConnector snap-in service.
Snap-in 1 Key	The database key for the first snap-in account, which is obtained after setting up data in Omnichannel Database. For example, if you set this attribute for SMS, you must enter the name of the snap-in that you create while configuring the SMS gateway.
Snap-in 1 Cluster	The cluster that hosts the first MessagingConnector snap-in service.
Snap-in Service 2 Name	The name of the second MessagingConnector snap-in service.
Snap-in 2 Key	The database key for the second snap-in account, which is obtained after setting up data in Omnichannel Database.
Snap-in 2 Cluster	The cluster that hosts the second MessagingConnector snap-in service.
Snap-in Service 3 Name	The name of the third MessagingConnector snap-in service.
Snap-in 3 Key	The database key for the third snap-in account, which is obtained after setting up data in Omnichannel Database.
Snap-in 3 Cluster	The cluster that hosts the third MessagingConnector snap-in service.

SMS Vendor

Name	Description
Oceana Messaging Service IP or FQDN	The URL of the cluster where the MessagingService is installed.
Oceana Messaging Service key	The Snap-in field configured in Omnichannel Database Administration client.

Co Browse

Name	Description
Multimedia CoBrowse Database Username	The user name for the Co-Browse database. To set this attribute, type the user name as `Cobrowse`.

Table continues…

Name	Description
Multimedia CoBrowse Database Password	The password for the Co-Browse database. To set this attribute, type the password as `Oceana16`.
Multimedia CoBrowse Database Name	The name of the Co-Browse database.

Oceana Event Reporting

Name	Description
Oceana Eventing	The attribute that enables or disables event notifications to be sent out to subscribed services. You must enable this attribute if you use Avaya Analytics™.

Important:

For Work Assignment and Engagement Designer attributes, administrators must examine the individual attributes in Service attributes overview on page 756.

OBCService

Name	Description
POM Server	The FQDN or IP address of the POM server that is to be serviced by Outbound Connector.
POM Server Port	The port number that the POM server uses to connect to Outbound Connector.

Zang SMS Connector

Name	Description
Enable Zang SMS Connector Tokenless Access	The attribute that enables the requests to access resource end-points without any authorization token. To enable tokenless access, retain the default value `true`. This feature is available for Avaya Oceana® mode only.
Maintenance Mode	The attribute to enable the maintenance mode. The supported values are true and false. The default value is false. This feature is available for Avaya Oceana® mode only.
Oceana Mode	The attribute to enable or disable Avaya Oceana® support for ZangSmsConnector.

Table continues…

Name	Description
Key for Oceana Messaging Service	The attribute used for polling the Avaya Oceana® SMS snap-in for accounts information. This attribute is mandatory to support the Oceana mode.
Oceana Messaging Service IP	The Avaya Oceana® cluster that hosts the MessagingService snap-in. This option is mandatory for the Oceana mode.
Oceana Messaging Service Name	The name of the MessagingService snap-in. This option is mandatory to support the Avaya Oceana® mode.

Oceana Data Viewer

Name	Description
CustomerControllerService Cluster	The cluster that hosts the CustomerControllerService.

Adding nodes to Avaya Oceana® Cluster 1

Before you begin

For an Avaya Oceana® deployment that supports 100 active agents or less, you must install the CentralizedLoggingService SVAR on Avaya Oceana® Cluster 1. Therefore, you must identify the WebSphere and Security Module HTTPS certificates for all nodes of Avaya Oceana® Cluster 1 and ensure that the certificates are signed by the same CA. You must also ensure that these certificates have different Common Name (CN).

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, select the check box for the cluster and click **Edit**.
3. On the Cluster Editor page, select the **Servers** tab.

   The system displays all the Avaya Breeze® platform nodes in the Unassigned Servers section.
4. In the Unassigned Servers section, click the plus sign **(+)** on each of the three nodes to add the three Avaya Breeze® platform nodes to Avaya Oceana® Cluster 1.

   The system adds the three Avaya Breeze® platform nodes to the Assigned Servers section.

   Important:

   Do not add additional Avaya Breeze® platform nodes to the cluster.
5. On the Cluster Editor page, select the **General** tab.

6. Select the **Is load balancer enabled** check box.
7. Click **Commit**.

   The system prompts you to ensure that you restart all Avaya Breeze® platform nodes before placing the cluster into the Accept New Service state.
8. Click **OK**.
9. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
10. On the Cluster Administration page, click **Show** on the new cluster to verify whether the system has added the nodes to the cluster.

    The system displays the Avaya Breeze® platform nodes as part of Avaya Oceana® Cluster 1.
11. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
12. On the Services page, verify that the state of the SVARs is `Installing`.

    The state changes to `Installed` when the installation is complete.
13. Wait until the services are installed on the Avaya Breeze® platform nodes.
14. Restart the Avaya Breeze® platform nodes that are added to the cluster.

Adding nodes to Avaya Oceana® Cluster 2

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, select the check box for the cluster and click **Edit**.
3. On the Cluster Editor page, select the **Servers** tab.

   The system displays all the Avaya Breeze® platform nodes in the Unassigned Servers section.
4. In the Unassigned Servers section, click the plus sign **(+)** on each of the two nodes to add the two Avaya Breeze® platform nodes to Avaya Oceana® Cluster 2.

   The system adds the two Avaya Breeze® platform nodes to the Assigned Servers section.

   Important:

   Do not add additional Avaya Breeze® platform nodes to the cluster.
5. On the Cluster Editor page, select the **General** tab.
6. Select the **Is load balancer enabled** check box.
7. Click **Commit**.

   The system prompts you to ensure that you restart all Avaya Breeze® platform nodes before placing the cluster into the Accept New Service state.

8. Click **OK**.
9. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
10. On the Cluster Administration page, click **Show** on the new cluster to verify whether the system has added the nodes to the cluster.

    The system displays the Avaya Breeze® platform nodes as part of Avaya Oceana® Cluster 2.
11. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
12. On the Services page, verify that the state of the SVARs is `Installing`.

    The state changes to `Installed` when the installation is complete.
13. Wait until the services are installed on the Avaya Breeze® platform nodes.
14. Restart the Avaya Breeze® platform nodes that are added to the cluster.

Adding nodes to Avaya Oceana® Cluster 3

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, select the check box for the cluster and click **Edit**.
3. On the Cluster Editor page, select the **Servers** tab.

    The system displays all the Avaya Breeze® platform nodes in the Unassigned Servers section.
4. In the Unassigned Servers section, click the plus sign **(+)** on each of the two nodes to add the two Avaya Breeze® platform nodes to Avaya Oceana® Cluster 3.

    The system adds the two Avaya Breeze® platform nodes to the Assigned Servers section.

    Important:

    Do not add additional Avaya Breeze® platform nodes to the cluster.
5. On the Cluster Editor page, select the **General** tab.
6. Select the **Is load balancer enabled** check box.
7. Click **Commit**.

    The system prompts you to ensure that you restart all Avaya Breeze® platform nodes before placing the cluster into the Accept New Service state.
8. Click **OK**.
9. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.

10. On the Cluster Administration page, click **Show** on the new cluster to verify whether the system has added the nodes to the cluster.

    The system displays the Avaya Breeze® platform nodes as part of Avaya Oceana® Cluster 3.

11. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
12. On the Services page, verify that the state of the SVARs is `Installing`.

    The state changes to `Installed` when the installation is complete.

13. Wait until the services are installed on the Avaya Breeze® platform nodes.
14. Restart the Avaya Breeze® platform nodes that are added to the cluster.

Adding nodes to Avaya Oceana® Cluster 4

Before you begin

For an Avaya Oceana® deployment that supports more than 100 active agents, you must install CentralizedLoggingService on Avaya Oceana® Cluster 4. Therefore, you must identify the WebSphere and Security Module HTTPS certificates for all nodes of Avaya Oceana® Cluster 4 and ensure that the certificates are signed by the same CA. You must also ensure that these certificates have different Common Name (CN).

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, select the check box for the cluster and click **Edit**.
3. On the Cluster Editor page, select the **Servers** tab.

   The system displays all the Avaya Breeze® platform nodes in the Unassigned Servers section.

4. In the Unassigned Servers section, click the plus sign **(+)** on each of the nodes to add the required number of Avaya Breeze® platform nodes to Avaya Oceana® Cluster 4.

   The system adds the Avaya Breeze® platform nodes to the Assigned Servers section.

   Important:

   Do not add additional Avaya Breeze® platform nodes to the cluster.

5. On the Cluster Editor page, select the **General** tab.
6. Select the **Is load balancer enabled** check box.
7. Click **Commit**.

   The system prompts you to ensure that you restart all Avaya Breeze® platform nodes before placing the cluster into the Accept New Service state.

8. Click **OK**.

9. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
10. On the Cluster Administration page, click **Show** on the new cluster to verify whether the system has added the nodes to the cluster.

    The system displays the Avaya Breeze® platform nodes as part of Avaya Oceana® Cluster 4.
11. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
12. On the Services page, verify that the state of the SVARs is `Installing`.

    The state changes to `Installed` when the installation is complete.
13. Wait until the services are installed on the Avaya Breeze® platform nodes.
14. Restart the Avaya Breeze® platform nodes that are added to the cluster.

Adding nodes to Avaya Oceana® Cluster 5

Before you begin

For an Avaya Oceana® deployment that supports more than 100 active agents, you install Avaya CRMGateway snap-in and ZangSmsConnector on Avaya Oceana® Cluster 5. Therefore, you must identify the WebSphere and Security Module HTTPS certificates for all nodes of Avaya Oceana® Cluster 5 and ensure that the certificates are signed by the same CA. You must also ensure that these certificates have different Common Name (CN).

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, select the check box for the cluster and click **Edit**.
3. On the Cluster Editor page, select the **Servers** tab.

   System Manager displays all the Avaya Breeze® platform nodes in the Unassigned Servers section.
4. In the Unassigned Servers section, click the plus sign **(+)** on each of the nodes to add the required number of Avaya Breeze® platform nodes to Avaya Oceana® Cluster 5.

   System Manager adds the Avaya Breeze® platform nodes to the Assigned Servers section.

   Important:

   Do not add additional Avaya Breeze® platform nodes to the cluster.
5. On the Cluster Editor page, select the **General** tab.
6. Select the **Is load balancer enabled** check box.
7. Click **Commit**.

   System Manager prompts you to ensure that you restart all Avaya Breeze® platform nodes before placing the cluster into the Accept New Service state.

8. Click **OK**.
9. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
10. On the Cluster Administration page, click **Show** on the new cluster to verify whether the system has added the nodes to the cluster.

    System Manager displays the Avaya Breeze® platform nodes as part of Avaya Oceana® Cluster 5.
11. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
12. On the Services page, verify that the state of the SVARs is `Installing`.

    The state changes to `Installed` when the installation is complete.
13. Wait until the services are installed on the Avaya Breeze® platform nodes.
14. Restart the Avaya Breeze® platform nodes that are added to the cluster.

Verifying the status of Avaya Breeze® platform nodes

About this task

Verify the status of Avaya Breeze® platform nodes. For detailed information, see *Deploying Avaya Breeze® platform*.

Procedure

1. Identify the Avaya Breeze® platform nodes where you want to install the snap-in services.
2. On the System Manager web console, navigate to **Services** > **Replication** and verify that all Avaya Breeze® platform nodes are in the synchronized state.
3. Perform the following steps to verify that all Avaya Breeze® platform nodes pass the maintenance tests:
    a. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **System Tools and Monitoring** > **Maintenance Tests**.
    b. In the **Select Avaya Breeze to test** field, select the Avaya Breeze® platform node for which you want to perform maintenance tests.
    c. Click **Execute All Tests**.
    d. Verify that the **Test Result** column for all tests displays the result as `Success`.
    e. Repeat step b through d for the other Avaya Breeze® platform nodes.
4. Perform the following steps to check the system state of all Avaya Breeze® platform nodes:
    a. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Server Administration**.
    b. Ensure that the **System State** column for all Avaya Breeze® platform nodes displays the state as `Denying`.

Setting Cluster State to Accepting

About this task

Use this procedure to set the cluster state of all clusters to Accepting, so that they can accept http or https requests.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.

   System Manager displays the Cluster Administration page.
2. Select the check box for Avaya Oceana® Cluster 1.
3. In the **Cluster State** field, select **Accept New Service**.
4. In the Warning: Accept New Service dialog box, click **Continue**.
5. Verify that the Cluster State column for the cluster displays `Accepting [x/x]`.
6. Repeat Step 2 to Step 5 for Avaya Oceana® Cluster 2, Avaya Oceana® Cluster 3, Avaya Oceana® Cluster 4, and Avaya Oceana® Cluster 5.

Enabling CORS for clusters

About this task

Use this procedure to enable Cross-origin Resource Sharing (CORS) for Avaya Oceana® Cluster 1, Avaya Oceana® Cluster 2, Avaya Oceana® Cluster 3, Avaya Oceana® Cluster 4, and Avaya Oceana® Cluster 5. CORS is a mechanism by which restricted resources on a node can be requested from another domain outside the domain from which the resource originated.

Note:

Allowing HTTP/HTTPS requests to the **Avaya Breeze®** from any untrusted host address is a serious security risk. Therefore, you must decide whether to allow connections from all domains into your own networks.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **HTTP Security**.
2. On the HTTP Security page, perform the following steps:
   a. In the **Cluster** field, select the cluster.
   b. Select the **HTTP CORS** tab.
   c. Select the **Allow Cross-origin Resource Sharing for all** check box.
   d. Click **Commit**.

Automated installation checklist

Use the following checklist for new automated installation of Avaya Oceana® SVARs and Avaya Breeze® platform upgrades:

Note:

Skip this installation if you have already installed Avaya Oceana® snap-ins using the manual installation method.

No.	Task	Description	✔
1	Create Avaya Oceana® clusters.	See: • Creating Avaya Oceana Cluster 1 on page 105 • Creating Avaya Oceana Cluster 2 on page 108 • Creating Avaya Oceana Cluster 3 on page 110 • Creating Avaya Oceana Cluster 4 on page 113 • Creating Avaya Oceana Cluster 5 on page 114	
2	Create Provisioning Cluster.	See Creating Provisioning Cluster on page 116.	
3	Set OceanaConfiguration attributes.	See Setting OceanaConfiguration attributes on page 117.	
4	Add Avaya Breeze® platform nodes to clusters.	See: • Adding nodes to Avaya Oceana Cluster 1 on page 127 • Adding nodes to Avaya Oceana Cluster 2 on page 128 • Adding nodes to Avaya Oceana Cluster 3 on page 129 • Adding nodes to Avaya Oceana Cluster 4 on page 130 • Adding nodes to Avaya Oceana Cluster 5 on page 131	
5	Verify the status of Avaya Breeze® platform nodes.	See Verifying the status of Avaya Breeze platform nodes on page 132.	

Table continues…

No.	Task	Description	✔
6	Check the replication status of Avaya Breeze® platform nodes.	See Checking the replication status of Avaya Breeze platform nodes on page 135.	
7	Set the state of all clusters to Denying.	See Setting Cluster State to Denying on page 135.	
8	Run the upgradeSolution script.	See Running the upgradeSolution script on new installations on page 136.	
9	Verify the status of Avaya Breeze® platform nodes.	See Verifying the status of Avaya Breeze platform nodes on page 132.	
10	Check the replication status of Avaya Breeze® platform nodes.	See Checking the replication status of Avaya Breeze platform nodes on page 135.	
11	Set the state of all clusters to Accepting.	See Setting Cluster State to Accepting on page 133.	
12	Enable CORS for clusters.	See Enabling CORS for clusters on page 133.	

Checking the replication status of Avaya Breeze® platform nodes

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. On the Replica Groups page, verify the following:
   - All Avaya Breeze® platform nodes are replicating and are highlighted in green.
   - None of the Avaya Breeze® platform nodes is in the `Audit` state.
   - Validate that the replication status shows a timestamp in the last five minutes. If the timestamp is older, that is, 24 hours, perform a manual replication status check to synchronize the System Manager with all the Avaya Breeze® platform nodes.

Setting Cluster State to Denying

About this task

Use this procedure to set the cluster state of all clusters to Denying, so that they do not accept any requests.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.

   The System Manager displays the Cluster Administration page.
2. Select the check box for Avaya Oceana® Cluster 1.

3. In the **Cluster State** field, select **Deny New Service**.
4. In the Warning: Deny New Service dialog box, click **Continue**.
5. Verify that the Cluster State column for the cluster displays `Denying [x/x]`.
6. Repeat Step 2 to Step 5 for Avaya Oceana® Cluster 2 and Avaya Oceana® Cluster 3.

Running the upgradeSolution script on new installations

About this task

Use this procedure to run the `upgradeSolution` script to do the following:

- Upgrades all Avaya Breeze® platform nodes to latest hotfixes and patches.
- Loads the latest versions of all Avaya Oceana® snap-ins in System Manager.
- Install Avaya Oceana® snap-ins to their relevant clusters.

Important:

Ensure that all Avaya Oceana® nodes are deployed on the same version of VMware ESX.

Before you begin

Download the `Oceana<Release_number>.zip` artifacts file from PLDS.

Procedure

1. Copy the `Oceana<Release_number>.zip` artifacts file to the `/swlibrary` location on System Manager.
2. Log in to the new System Manager virtual machine using an SSH client application, such as PuTTy.
3. Run the following command as a cust user:

   ```
   upgradeSolution /swlibrary/Oceana<Release_number>.zip -cg <N>
   <Configuration Package> <OPTION>
   ```

   In this command:

   - Replace <*N*> with the Cluster Group number of the Oceana nodes being upgraded. There are 2 cluster group numbers for DR solutions. Ensure that you choose the correct cluster group number when using this command.
   - Replace <*Configuration Package*> with the configuration type to match with the deployment type. For example, Combined-4500 for Oceana_Large.
   - Replace <*OPTION*> with space-separated values depending on the required configuration to include non-mandatory snap-ins. For example, Chat GenericChannel Social AMC.

   For detailed information about these parameters, see Avaya Breeze platform upgrade script parameters on page 137.

   Important:

   - The current version of the command provides validation of these parameters.

- Ensure that you carefully type all option values in the **upgradeSolution** command.
- During the installation, the script tries to determine the names of the current Avaya Oceana® clusters and the current snap-ins installed on them. The script prompts for a confirmation if each cluster name corresponds to a specific cluster. For example, "Is Cluster 1 name Cluster1_CC (y/n)". If the prompted cluster name is incorrect and you press `n`, the script prompts again until you get the correct cluster name and press `y`.
- You can view the upgrade logs in the `solution-upgrade.log` file in the `/var/log/Avaya` folder on System Manager.
- You must run the script only when all Avaya Oceana® clusters are in a denying state.

Avaya Breeze® platform upgrade script parameters

Number	Description	Configuration value	OPTION value choices	Sample command
1	Avaya Oceana® 3.5.x or newer release Voice and Digital with agent sizes greater than 100 up to maximum of 4500 agents	Combined-4500	AMC AvayaChat Messaging Chat CoBrowse GenericChannel Social SMS POM CRMgateway ZangSmsConnect or DataView PacketMetric	upgradeSolution *<path To OceanaXXXX.zip file>* -cg N Combined-4500 AMC AvayaChat Messaging Chat CoBrowse GenericChannel Social SMS POM CRMgateway ZangSmsConnector DataView PacketMetric
2	Avaya Oceana® 3.5.x or newer release Voice and Digital with 100 agents	Combined-100	AMC AvayaChat Messaging Chat GenericChannel Social SMS POM CoBrowse ZangSmsConnect or CRMgateway DataView PacketMetric	upgradeSolution *<path To OceanaXXXX.zip file>* -cg N Combined-100 AMC AvayaChat Messaging Chat CoBrowse GenericChannel Social SMS ZangSmsConnector DataView POM CRMgateway PacketMetric
3	Avaya Oceana® 3.5.x or newer release Voice only with agent sizes greater than 100 up to maximum of 4500 agents	VoiceOnly-4500	AMC POM CoBrowse CRMgateway ZangSmsConnect or CRMgateway PacketMetric	upgradeSolution *<Path To OceanaXXXX.zip file>* -cg N VoiceOnly-4500 AMC POM CoBrowse CRMgateway ZangSmsConnector CRMgateway PacketMetric

Table continues…

Number	Description	Configuration value	OPTION value choices	Sample command
4	Avaya Oceana® 3.5.x or newer release Voice only with 100 agents	VoiceOnly-100	AMC POM CoBrowse ZangSmsConnector CRMgateway PacketMetric	upgradeSolution <*Path To OceanaXXXX.zip file*> -cg N VoiceOnly-100 AMC POM CoBrowse ZangSmsConnector CRMgateway PacketMetric
5	Avaya Oceana® 3.5.x or newer release Digital only with agent sizes greater than 100 up to maximum of 4500 agents	DigitalOnly-4500	AvayaChat Messaging SMS Chat GenericChannel Social CoBrowse CRMgateway ZangSmsConnector DataView PacketMetric	upgradeSolution <*Path To OceanaXXXX.zip file*> -cg N DigitalOnly-4500 AvayaChat Messaging SMS Chat GenericChannel Social CoBrowse CRMgateway ZangSmsConnector DataView PacketMetric
6	Avaya Oceana® 3.5.x or newer release Digital only with 100 agents	DigitalOnly-100	AvayaChat Messaging SMS Chat GenericChannel Social CoBrowse ZangSmsConnector DataView PacketMetric	upgradeSolution <*Path To OceanaXXXX.zip file*> -cg N DigitalOnly-100 AvayaChat Messaging SMS Chat GenericChannel Social CoBrowse ZangSmsConnector DataView PacketMetric

Note:

Remove any or all of the options if you do not have those snap-ins installed on your system.

You do not need to remove AMC from service profile if you do not use WebRTC/Video.

The following table lists the snap-ins included in each SnapInGroup OPTION:

SnapInGroup OPTION	Snap-ins included
Messaging	MessagingService
SMS	SMSVendorSnapin
AMC	AvayaMobileCommunications
AvayaChat	BotConnector
Chat	AutomationController
CoBrowse	CoBrowse
GenericChannel	GenericChannelAPI
Social	SocialConnector
POM	OBCService
DataView	DataViewer
PacketMetric	Packetbeat and Metricbeat

Note:

The Logging and PacketMetric snap-ins are optional regardless of which channels are used.

Configuration changes in Avaya Oceana® clusters for NGINX and High Availability

For NGINX and High Availability, Avaya Oceana® clusters require the following configuration changes:

Avaya Oceana® Cluster 1

On the Cluster Editor page of Avaya Oceana® Cluster 1:

- Set the **HTTP Load Balancer backend server max failure response timeout period (seconds)** field to `60`.
- Set the **Max number of failure responses from HTTP Load Balancer backend server** field to `2`.
- Set the **Network connection timeout to HTTP Load Balancer backend server (seconds)** field to `3`.

Avaya Oceana® Cluster 2

On the Cluster Editor page of Avaya Oceana® Cluster 2:

- Set the **HTTP or HTTPS traffic rate limit in bytes/sec per client** field to `5000000`.
- Set the **HTTP Load Balancer backend server max failure response timeout period (seconds)** field to `60`.
- Set the **Max number of failure responses from HTTP Load Balancer backend server** field to `2`.
- Set the **Network connection timeout to HTTP Load Balancer backend server (seconds)** field to `3`.

Avaya Oceana® Cluster 3

On the Cluster Editor page of Avaya Oceana® Cluster 3:

- Set the **HTTP Load Balancer backend server max failure response timeout period (seconds)** field to `60`.
- Set the **Max number of failure responses from HTTP Load Balancer backend server** field to `2`.
- Set the **HTTP or HTTPS limit on connections per client** field to `8000`.
  - For a 100-agent deployment, set the **HTTP or HTTPS limit on connections per client** field to `6000`.
- Set the **Network connection timeout to HTTP Load Balancer backend server (seconds)** field to `3`.

Other Avaya Oceana® clusters

On the Cluster Editor page of the other Avaya Oceana® clusters:

- Set the **Max number of failure responses from HTTP Load Balancer backend server** field to `2`.
- Set the **Network connection timeout to HTTP Load Balancer backend server (seconds)** field to `3`.

The upgrade script automatically applies these changes. However, the new customers who perform a manual installation must manually apply these changes.

Note:

These changes also apply to the 100-agent deployments where you deploy Avaya Oceana® Cluster 2 on Avaya Oceana® Cluster 1.

However, for 100-agent deployments, you must set the **HTTP or HTTPS limit on connections per client** field to `6000`.

Viewing Oceana Monitor Service pages

Procedure

1. To view the Oceana Services Overview page, enter the following URL in your web browser:

   `https://<Cluster IP>/services/OceanaMonitorService/services.html`

2. To view the Monitor Service page, enter the following URL in your web browser:

   `https://<Cluster IP>/services/OceanaMonitorService/monitor.html`

   On the Monitor Service page, click the cluster node to view the information about the cluster.

Monitor Service page

The Monitor Service page provides the following information about each cluster of Avaya Oceana®:

- Name of the cluster.
- IP address of the cluster.
- Number of nodes in the cluster.
- IP address of each node of the cluster.
- Cluster view of the snap-ins installed.
- View of snap-in lifecycle messages.

Monitor Service page field descriptions

When you click the cluster node, the Monitor Service page displays the following buttons:

Button name	Description
Show Node Details	Displays information about the nodes of the cluster.
Show Grid Info	Displays the following information about the processing units of the cluster: • Name of the processing unit • Embedded space of the processing unit • Number of instances • Type of the processing unit • Status of the processing unit
Show Cluster Messages	Displays the service messages for all the snap-ins installed on the cluster.
Show Service Details	Displays the following information about each of the snap-ins installed on the cluster: • Name of the snap-in • Version of the snap-in • Service messages of the snap-in

Oceana Services Overview page

The Oceana Services Overview page provides the following information about each snap-in of Avaya Oceana®:

- Name of the snap-in.
- Symbol specifying whether Oceana Monitor Service has detected the snap-in:
  - ✔ indicates that Oceana Monitor Service has detected the snap-in.
  - ✖ indicates that Oceana Monitor Service has not detected the snap-in.
- Version of the snap-in.
- Name of the cluster where the snap-in is installed.
- Latest Heartbeat message of the snap-in.

  The Heartbeat message includes the node reporting the Heartbeat, the status level of the Heartbeat (OK, WARN, ERROR), and the time since the last update. The Heartbeat background indicates the status of the Heartbeat.

Oceana Dashboard overview

Oceana Dashboard provides a consolidated view of the health of Avaya Oceana® services. The dashboard also provides access to context-sensitive troubleshooting documentation for any active problems. The Traffic Light view displays different functions of Avaya Oceana® covering Channels, Agent Operations, Authorization, LDAP connection health, Engagement Designer health, and EDM connectivity health.

The list of channels and features that the Oceana Dashboard monitors is configured using the OceanaConfiguration service, and values are pushed down to all instances of Dashboard service

located on all clusters. Changes using the configuration service are dynamic and do not require reboot.

Avaya Oceana® The Oceana Dashboard page provides information about the service status and displays the current high-level state of Avaya Oceana® features. Each feature is displayed as a color-coded card based on the state of the services which that feature requires. Each feature card contains colored boxes representing the status of a service which that feature requires to operate. Clicking on one of the cards, automatically filters the service list to only display the services which are required for the selected service.

The Oceana Dashboard page displays the following:

- The name of the service.
- The time that the last heartbeat
- The name of the cluster where the service is installed.
- The name of the node inside the cluster.
- The latest heartbeat message.

  The heartbeat message includes the node reporting the heartbeat, the status level of the heartbeat, and the time since the last update.

  There are four levels of colors displayed for each service:

  - Green: Indicates that all nodes running the service has returned a healthy heartbeat.
  - Yellow: Indicates that one or more service nodes in the cluster returned a warn heartbeat.
  - Orange: Indicates that one or more service nodes either returned an error heartbeat, or is not responding. There are some service nodes remaining in operation which can provide partial service.
  - Red: Indicates that all the nodes for a service are either reporting an error or not responding, indicating that the entire service is down.
- A link to the troubleshooting guide for the service.

Viewing Oceana Dashboard

About this task

The Oceana Dashboard service gets deployed when you install Oceana Monitor service.OceanaMonitor supports adding custom elements to OceanaDasboard. It is useful when we need to add the custom features to the dashboard. Overload Status and Certificate Status blocks are added. The Overload Status shows if the Breeze system is overloaded and Certificate Status displays the status of different certificates on the Breeze system. Dashboard is available on all clusters that have Oceana Monitor service. Authentication is not required to view the Dashboard.

Procedure

1. In your web browser, enter the following URL to view the Oceana Dashboard page:

   `https://<Cluster IP>/services/OceanaMonitorService/dashboard.html`

The dashboard displays the channels which you want to monitor and the associated services. The channels and services are indicated in different colors. You can hover over each service to view the monitor status of the service.

2. On the Oceana Dashboard page, click **Filter** to sort the services based on the monitor status.

   You can filter based on the four color-coded status levels displayed for each service:

   - **Red status**
   - **Orange status**
   - **Yellow status**
   - **Green status**
   - **None**

3. **(Optional)** Click **Automatically update dashboard (every 60 seconds)** to update the dashboard every minute.

Viewing Oceana Manager

About this task

Using Oceana Manager, you can set the status for all clusters at once. On this page, you can set a group of clusters to standby, active, and open the Gigaspace Viewer page for a specific node.

Procedure

1. In your web browser, enter the following URL to view the Oceana Manager page:

   `https://<Cluster IP>/services/OceanaMonitorService/manager.html`

2. Log in to the Authorization Service page as an administrator user.
3. To set the status of the clusters, do the following:
   - To set a Deny status for all clusters, click **Set Cluster Group to Standby**.
   - To set an Accept status for all clusters, click **Set Cluster Group to Active**.
   - To open the Gigaspace Viewer for a specific node, click **Show Node Details**, select a cluster, and click **Open Gigaspace Viewer**.

Viewing Stuck Contact Tool

About this task

Use the Stuck Contact tool if you have an Agent who is stuck on a contact. The Stuck Contact tool helps to clear contacts that are stuck due to some unknown error.

Procedure

1. In your web browser, enter the following URL to view the Oceana Stuck Contact Tool page:

   `https://<Cluster IP>/services/OceanaMonitorService/contacttool.html`

2. Log in to the Authorization Service page.
3. To find all the contacts currently assigned to an agent, enter the Agent username (agent ID) and press **Enter**.
4. Press the **Synchronize** button.

   If successful, the contact transitions to After Call Work (ACW). The agent might need to clean up the ACW interaction/card manually.

   Note:

   It is possible to get a failed attempt here if the providers do not clean the contact or if the request times out. In such cases, when the synchronization fails, click the **Destroy** button.

   This is a last resort, so use it only when you are sure the contact is not cleared. It is possible that the contact may be re-created later by the provider even after you click **Destroy**.

Chapter 10: Deploying External Data Mart

Deploy External Data Mart overview

The EDM can be deployed in one of the following supported configurations:

- *Standalone EDM non-DB HA*: EDM is deployed alone on one SQL Server.
- *Standalone EDM DB HA*: EDM is deployed alone on two SQL Servers.
- *EDM/ACM co-res DB HA*: EDM is deployed co-res with the ACM databases on two SQL Servers.

Note:

The co-resident deployment of Avaya Control Manager databases and the EDM is not supported in a non-DB HA configuration (one SQL Server per Datacenter) in production environments.

Avaya Oceana® provides High Availability (HA) of Context Store External Data Mart (EDM) when:

- EDM is installed co-resident with Avaya Control Manager databases on Microsoft SQL Server using Microsoft SQL Server Enterprise Edition and Windows AlwaysOn Advanced Availability Groups (AAG).
- EDM is installed standalone on Microsoft SQL Server without Avaya Control Manager databases using Microsoft SQL Server Standard Edition and Windows AlwaysOn Basic Availability Group (BAG).

Important:

- For a non-DB HA configuration in production environments, the co-resident deployment of Avaya Control Manager and EDM is not supported.
- In an availability group, you must have a maximum of two EDM replicas.

The following version combinations are tested for the co-resident deployment using AAG:

Microsoft SQL Server		Database Encryption at REST Support
Version	**Edition**	
2019	**Enterprise**	Supported through TDE (Transparent Data Encryption). See Transparent Data Encryption (TDE) on External Data Mart on page 182.

Table continues…

Microsoft SQL Server		Database Encryption at REST Support
Version	**Edition**	
2017	**Enterprise**	Supported through either vCenter Encryption or TDE (Transparent Data Encryption). See Transparent Data Encryption (TDE) on External Data Mart on page 182.
2016	**Enterprise Edition SP2**	Supported through vCenter Encryption

The following version combinations are tested for the standalone EDM using BAG:

Microsoft SQL Server		Database Encryption at REST Support
Version	**Edition**	
2019	**Standard**	Supported through either vCenter Encryption or TDE (Transparent Data Encryption). See Transparent Data Encryption (TDE) on External Data Mart on page 182.
2016	**Standard**	Not supported

Note:

Avaya Oceana® also supports the External Data Mart database running the specified Microsoft SQL Server versions in the table above on any supported version of Windows Operating System.

For supported version combinations, see the following:

- SQL Server 2019: https://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server-ver15?view=sql-server-ver15.
- SQL Server 2016 and 2017: https://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server?view=sql-server-ver15.

Deploy External Data Mart on Avaya Control Manager SQL Server

Avaya Control Manager-External Data Mart co-resident deployment overview

Avaya Oceana® supports Avaya Control Manager and Context Store External Data Mart (EDM) deployment on the same Microsoft SQL Server. With the end of support of Oracle, Microsoft SQL Server is the only supported database platform for EDM.

Database migration

From Avaya Oceana® 3.8 and later versions, a new migration script facilitates the migration of the EDM data from:

- Oracle to Microsoft SQL Server
- Postgres to Microsoft SQL Server
- Old schema-based Microsoft SQL Server to the new schema-based Microsoft SQL Server

For more information on migration, see *Upgrading Avaya Oceana®* .

Footprint reduction

The co-resident deployment of Avaya Control Manager and EDM provides the following reductions in the overall hardware requirement of each separate database server:

- Memory requirement reduces from 28 GB to 24 GB.
- vCPU/node requirement reduces from 16 to 12.
- Hard disk requirement reduces as follows:
  - Avaya Control Manager databases require 700 GB.
  - EDM database requires a variable amount of disk space based on the Avaya Oceana® deployment size.

The following table displays information about the hardware of co-resident deployment of Avaya Control Manager and EDM:

Component	Platform	Requirement	Avaya Oceana®					
Avaya Control Manager Database co-resident with Avaya Context Store External Data Mart and Customer Journey Database	Windows	Number of nodes	2	2	2	2	2	2
		Memory/ node	24 GB	24 GB	24 GB	24 GB	24 GB	24 GB
		Minimum disk size/ node	3500 GB	2405 GB	2405 GB	2405 GB	2405 GB	515 GB
		vCPUs/ node	12	12	12	12	12	12
		IOPs	750	750	750	750	750	750

Note:

EDM requires 8 GB hard disk space per million contacts closed. The requirement does not include the disk space required for SQL transaction logs or database backups. Therefore, configure SQL Server Agent jobs to take regular (hourly is recommended) EDM transaction log backups, full EDM backups (daily at a quiet time is recommended), and clean up old backup files. Since Oceana 3.8.2.0, you can download SampleSQLServerAgentScripts.zip from https://support.avaya.com/ or https://www.devconnectprogram.com/. For more information on configuring the SampleSQLServerAgentScripts, see the *Configuring automated SQL Server Agent jobs* topic in the *Deploying Avaya Oceana®* document.

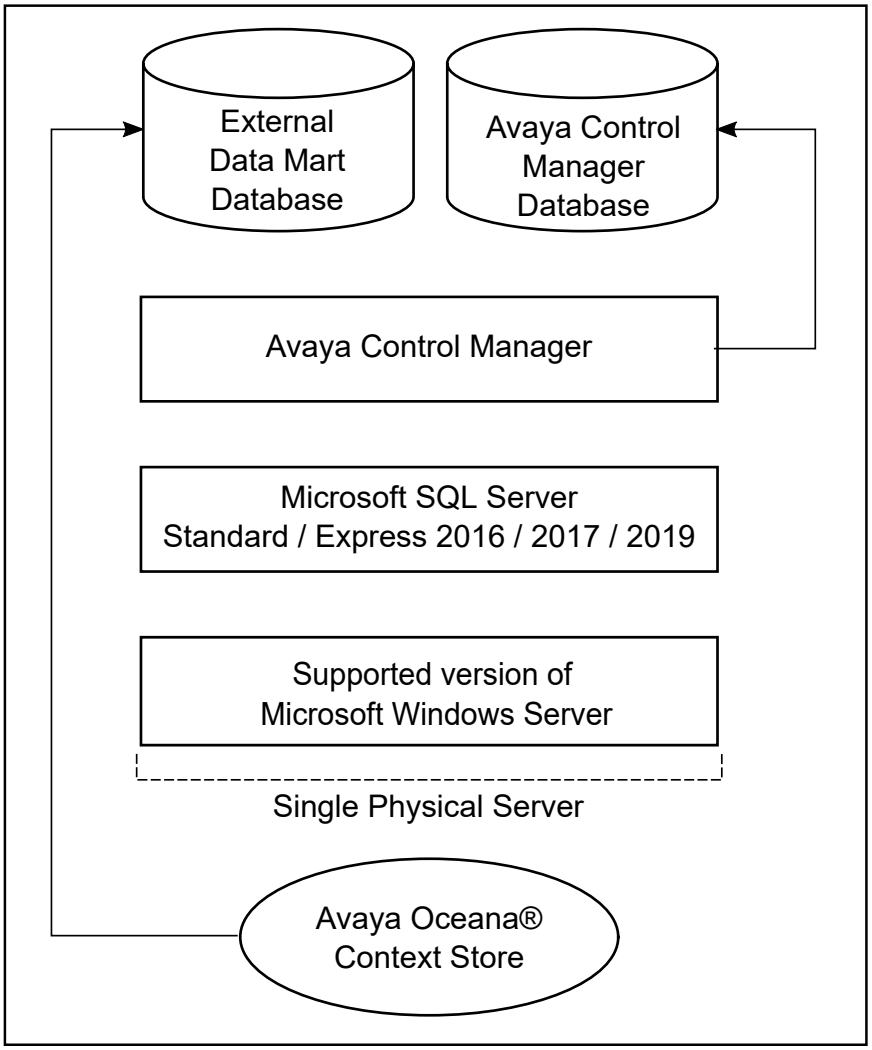
Licensing cost reduction

The co-resident deployment reduces the cost of separate Microsoft SQL Server licenses for Avaya Control Manager and EDM.

Supported configurations for the co-resident deployment of Avaya Control Manager and External Data Mart

Lab site single-server non-DB HA

The following diagram depicts the architecture of a lab site single-server non-DB HA deployment:

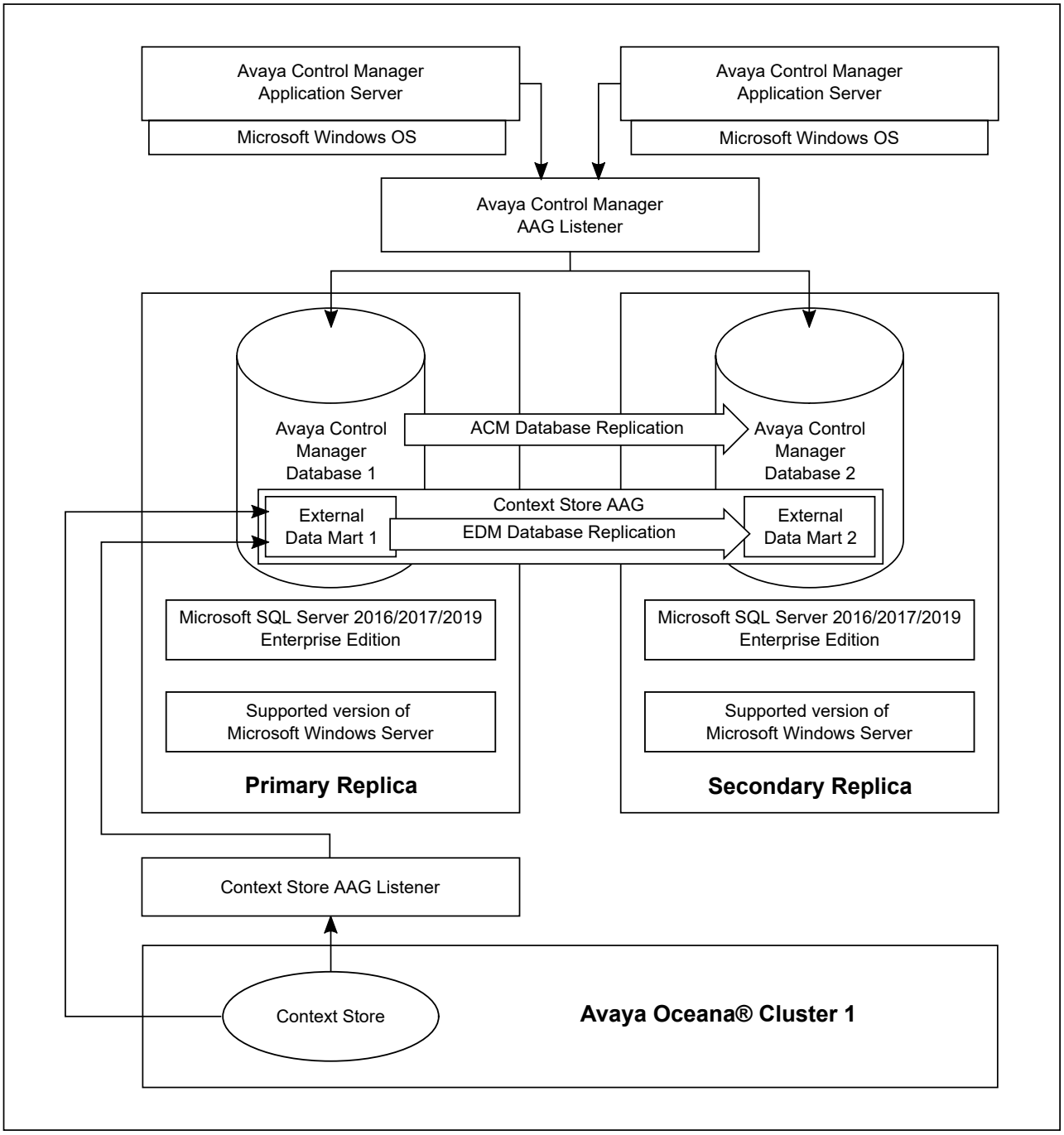


This deployment requires a single server with 24 GB RAM, 12 vCPUs, and 700 GB hard disk space. You can use this deployment for development labs with the following limitations:

- No traffic testing
- Bulk updates might take a longer time
- No customer UAT
- No use for production environments
- Less than 50 agents
- The database size of Microsoft SQL Server Express Edition limited to ~10 GB

Single-site Campus HA

The following diagram depicts the architecture of a single-site Campus HA deployment:



In this diagram, two Avaya Control Manager application servers connect to two Avaya Control Manager databases. You can deploy one or two Avaya Control Manager application servers.

Checklist for the co-resident deployment of Avaya Control Manager and EDM

Note:

This checklist is for new Avaya Oceana® customers only.

For upgrading from a previous version of Oceana and migrating your database, see *Upgrading Avaya Oceana®*.

No.	Task	Description	✔
1	Get the vCPU, memory, and hard disk space required for Microsoft SQL Server based on your Avaya Oceana® deployment size.	See Avaya Oceana hardware requirements on page 51.	
2	Deploy Avaya Control Manager and configure the Avaya Control Manager database SQL Server cluster.	See *Installing Avaya Control Manager for Enterprise - Multiplex High Availability*.	
3	Create database tables for External Data Mart (EDM).	See Creating database tables for External Data Mart on page 153.	
4	Create an optional non-system administrator user on the primary Avaya Control Manager SQL Server.	See Creating a user on the primary Avaya Control Manager SQL Server on page 154.	
5	Create the EDM Advanced Availability Group on Avaya Control Manager SQL Server.	See Creating the EDM Advanced Availability Group on Avaya Control Manager SQL Server on page 156.	
6	Create an optional non-system administrator user on the secondary Avaya Control Manager SQL Server.	See Creating an EDM user on the secondary Avaya Control Manager SQL Server on page 158.	
7	Generate certificates from System Manager to secure the connection between Context Store and Microsoft SQL Servers.	See Generating certificates to enable SSL connections fromContext Store to a cluster of two SQL Servers hosting EDMs configured in an AlwaysOn High Availability group on page 159.	
8	Change the SQL server to use the new certificate by configuring MS SQL Server for forced encryption.	See Configuring MS SQL Server for forced encryption on page 732.	

Table continues…

No.	Task	Description	✔
9	Enable Transparent Data Encryption (TDE) on EDM. **Note:** TDE is an alternative to using VMWare encryption when VMWare encryption is not possible. For example, a CPOD deployment.	See Transparent Data Encryption (TDE) on External Data Mart on page 182	
10	Configure automated SQL Server Agent jobs.	See Configuring automated SQL Server Agent jobs on page 189	
11	Load a JDBC-compatible driver jar file, configure the driver on System Manager, and then install the driver on the Context Store cluster.	See Loading JDBC driver to System Manager on page 162	
12	Configure the OceanaConfiguration and ContextStoreManager attributes in System Manager to enable connection from Context Store to EDM.	See Setting attributes to enable connection from Context Store to EDM on page 180.	

Note:

When installing SQL Server on virtual machines, Avaya recommends reading VMware's best practices published at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/sql-server-on-vmware-best-practices-guide.pdf. A summary of these recommendations includes:

- Store database Log files and database Data files on separate disks. This avoids I/O contention and improves performance.
- Install SQL Server and the Windows operating system on the same disk.

Finding the Avaya Control Manager SQL Server domain user

About this task

Use this procedure to find the Avaya Control Manager SQL Server domain user with administrative rights for all machines in the cluster.

Procedure

1. Log in to the Avaya Control Manager server.

2. Click and locate and open **Microsoft SQL Server *N*** > **SQL Server Configuration Manager** where *N* is the installed version of MS SQL.
   - Alternatively: Press +R and enter `compmgmt.msc` to start **Computer Management**. Expand **Services and Applications** and locate **SQL Server Configuration Manager**.
3. Click **SQL Server Services**.
4. Locate the **Log On As** column entry for the **SQL Server** service.
5. Note the user name of the SQL Server domain user.

Creating the External Data Mart database

About this task

Use this procedure to create the External Data Mart (EDM) database.

Note:

Context Store database tables store all data in ASCII format. To enable Context Store EDM to store a language that uses Unicode characters, the database administrator must set the correct collation type for the desired language on the database. You must configure the collation type before creating the EDM schema.

Procedure

1. Log in to the primary Avaya Control Manager SQL Server.
   - You must log as the Avaya Control Manager SQL Server domain user with administrative rights for all machines in the Avaya Control Manager database cluster. To check the user name, see Finding the Avaya Control Manager SQL Server domain user on page 151.
2. Click **Start** > **Microsoft SQL Server** > **Open SQL Server Management Studio**.
3. In the Object Explorer pane, click **Connect** > **Database Engine**.

   SQL Server Management Studio displays the Connect to Server dialog box.
4. In the **Server name** field, select the local instance of SQL Server.
5. In the **Authentication** field, select **SQL Server Authentication**.
6. In the **Login** and **Password** fields, enter the system administrator credentials.

   The system administrator is usually the default sa user created during SQL Server installation.
7. Click **Connect**.
8. In the Object Explorer pane, expand **Databases**.

   Important:

   Do not point your Avaya Oceana® to the new EDM until EDM configuration and migration is complete. EDM configuration and migration also include creating an

optional non-sa user and adding the EDM into Windows AlwaysOn Advanced Availability Group (AAG).

9. Right-click **Databases** and click **New Database**.

   SQL Server Management Studio displays the New Database dialog box.

10. In the navigation pane, click **General**.
11. In the **Database name** field, enter a name for the EDM database.
12. In the **Database files** section, do the following:

    a. For **File Type = ROWS Data**, click the three dots to the right of the **Path** field.

    b. Browse to the correct folder and click **OK**.

    To change the initial size for the EDM Data file, click the arrows to the right of the **Initial Size (MB)** value for **File Type = ROWS Data** and change the default value. For example, for 300 GB, enter 307200.

13. In the **Database files** field, do the following:

    a. For **File Type = LOG**, click the three dots to the right of the **Path** field.

    b. Browse to the correct folder and click **OK**.

    To change the initial size for the EDM Log file, click the arrows to the right of the **Initial Size (MB)** value for **File Type = LOG** and change the default value. For example, for 20 GB, enter 20480.

    Ensure that hourly transaction log backups are taken. You can download the SampleSQLServerAgentScripts.zip from https://support.avaya.com/ or https://www.devconnectprogram.com/. For more information on configuring the SampleSQLServerAgentScripts, see the *Configuring automated SQL Server Agent jobs* topic in the *Deploying Avaya Oceana®* document.

    You must also create the same paths and folders for EDM data files and log files on the secondary SQL replica before adding the EDM to AAG.

14. In the navigation pane, click **Options**.
15. In the **Collation** field, select the appropriate option or leave as default.
16. In the **Recovery model** field, select **Full**.
17. Click **OK**.

Creating database tables for External Data Mart

About this task

To use the External Data Mart feature, you must use the supported databases, the respective supported versions, and create the required database tables.

Note:

The Microsoft SQL database user configured for the EDM feature must have database ownership or system administrator privileges for this connection to be successful. Also, from the security profile of the database user, you must set the Context Store database as the default database.

Procedure

1. Download the `ContextStoreSchemaCreationScripts-SQLServer.zip` file from Avaya Support.
2. Copy the zip file to the server running the MS SQL Server.
3. Extract the zip file and locate the SQL script: `CreateEDMschema.sql`.
4. Open SQL Server Management Studio and do the following:.
   a. On the **File** menu, click **Open** to open the file.
   b. Click **Execute** or click **Query** > **Execute** to run the file.
5. Create database tables for External Data Mart by executing the `CreateEDMschema.sql` script.

Creating a user on the primary Avaya Control Manager SQL Server

About this task

Use this procedure to create an optional non-system administrator user on the primary Avaya Control Manager SQL Server.

Procedure

1. Log in to the primary Avaya Control Manager SQL Server.
   - You must log as the Avaya Control Manager SQL Server domain user with administrative rights for all machines in the Avaya Control Manager database cluster. To check the user name, see Finding the Avaya Control Manager SQL Server domain user on page 151.
2. Click **Start** > **Microsoft SQL Server** > **Open SQL Server Management Studio**.
3. In the Object Explorer pane, click **Connect** > **Database Engine**.

   SQL Server Management Studio displays the Connect to Server dialog box.
4. In the **Server name** field, select the local instance of SQL Server.
5. In the **Authentication** field, select **SQL Server Authentication**.
6. In the **Login** and **Password** fields, enter the system administrator credentials.

   The system administrator is usually the default sa user created during SQL Server installation.
7. Click **Connect**.
8. In the Object Explorer pane, right-click the SQL Server instance and click **New Query**.

9. In the content pane, run the following command to create a new login:

```
USE [master]
GO
CREATE LOGIN <<loginName>> WITH PASSWORD = '<<password>>', CHECK_POLICY=OFF
```

For example:

```
USE [master]
GO
CREATE LOGIN csEDMLogin WITH PASSWORD = 'myPassword1', CHECK_POLICY=OFF
```

10. Run the following command to select the security identifier (SID) for the new login:

```
SELECT sid, name FROM syslogins where name = '<<loginName>>'
```

For example:

```
SELECT sid, name FROM syslogins where name = 'csEDMLogin'
shows SID = 0x0589627E7A96D447865135449C41E53B
```

Important:

Note the SID. The SID is required when setting up the secondary SQL server.

11. In the Object Explorer pane, click **Security** > **Logins**.
12. Right-click the newly created login name and click **Properties**.

SQL Server Management Studio displays the Login Properties dialog box.

13. In the navigation pane, click **General**.
14. In the **Default database** field, select the EDM database name.
15. In the navigation pane, click **User Mapping**.
16. Select the **Map** check box for the EDM database.
17. Click **OK**.
18. In the Object Explorer pane, click **Databases** > ***<EDM Database>*** > **Security** > **Users**.
19. Verify that the newly created login name is available in the list of users.
20. In the Object Explorer pane, right-click the EDM database and click **New Query**.
21. In the content pane, run the following commands to grant permissions to the newly created user:

```
GRANT SELECT, INSERT, UPDATE, DELETE ON CS_OPERATION TO <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON CS_PROVISION TO <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON GENERATED_KEYS TO <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON INTERACTION_NOTE to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON INTERACTION_PARTICIPANT to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON SERVICE_ATTRIBUTE to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON SERVICE_ATTRIBUTE_GROUP to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON ROUTING_SERVICE to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON CUSTOM_DETAIL to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON INTERACTION to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON LINK to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON TOPIC to <<loginName>>;
GRANT SELECT, INSERT, UPDATE, DELETE ON ENGAGEMENT to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON OUTCOME to <<loginName>>;
```

```
GRANT SELECT, INSERT, UPDATE ON SENTIMENT_RATING to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON TENANT to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON INTERACTION_STATUS to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON INTERACTION_SUBSTATUS to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON CHANNEL_SUBTYPE to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON CHANNEL_TYPE to <<loginName>>;
GRANT SELECT, INSERT, UPDATE, DELETE ON CS_RESURRECT to <<loginName>>;
```

Creating the EDM Advanced Availability Group on Avaya Control Manager SQL Server

About this task

Use this procedure to create the EDM Advanced Availability Group on Avaya Control Manager SQL Server.

Before you begin

Perform steps 1 through 4 from Checklist for the co-resident deployment of Avaya Control Manager and EDM on page 150 before you perform this procedure.

Procedure

1. Log in to the primary Avaya Control Manager SQL Server.
   - You must log as the Avaya Control Manager SQL Server domain user with administrative rights for all machines in the Avaya Control Manager database cluster. To check the user name, see Finding the Avaya Control Manager SQL Server domain user on page 151.
2. Click **Start** > **Microsoft SQL Server** > **Open SQL Server Management Studio**.
3. In the Object Explorer pane, click **Connect** > **Database Engine**.

   SQL Server Management Studio displays the Connect to Server dialog box.
4. In the **Server name** field, select the local instance of SQL Server.
5. In the **Authentication** field, select **SQL Server Authentication**.
6. In the **Login** and **Password** fields, enter the system administrator credentials.

   The system administrator is usually the default sa user created during SQL Server installation.
7. Click **Connect**.
8. In the Object Explorer pane, click **Databases** > ***<EDM Database>***.
9. Right-click the EDM database and click **Tasks** > **Back Up**.

   SQL Server Management Studio displays the Back Up Database dialog box.
10. In the navigation pane, click **General**.
11. In the **Backup type** field, select **Full**.
12. In the **Destination** area, click **Add**.

13. In the Select Backup Destination dialog box, select the path to the backup folder location, specify the backup file name with the `.bak` extension, and click **OK**.

    Ensure that the SQLService User login (services.msc) has full permissions on the backup folder.

14. To provide full permissions to the SQLService User login, do the following:
    a. Go to the backup folder location.
    b. Right-click the backup folder and click **Properties**.
    c. On the Security tab, select the SQLService User login and click **Edit**.
    d. In the **Permissions** area, select the **Full control** check box.
    e. Click **OK**.
15. Click **OK**.
16. In the Object Explorer pane, click **Always On High Availability**.
17. Right-click **Availability Groups** and click **New Availability Group Wizard**.

    SQL Server Management Studio displays the New Availability Group dialog box.

18. In the navigation pane, click **Specify Options**.
19. In the **Availability group name** field, enter a name for the Context Store availability group.
20. In the **Cluster type** field, select **Windows Server Failover Cluster**.
21. Select the **Database Level Health Detection** check box.
22. Select the **Per Database DTC Support** check box.
23. Click **Next**.
24. In the **Select user databases for the availability group** field, select the EDM database.
25. Click **Next**.
26. Click **Add Replica**, specify the other SQL Server as the secondary replica and connect to the database engine of the other SQL Server.

    To connect to the database engine, use SQL Server Authentication and System Administrator login credentials.

27. Do the following for each replica:
    a. Select the **Automatic Failover** check box.
    b. Select the **Synchronous Commit** check box.
    c. Set the **Readable Secondary** field to No.
28. On the Backup Preferences tab, select **Prefer Secondary**.
29. On the Listener tab, select **Create an Availability Group Listener** and do the following:

    In the **Listener DNS Name** field, enter the full FQDN of the listener that you use to access AAG from Context Store.

For more information, on the Microsoft Documentation website, see Configure a listener for an Always On availability group.

Leave the **Port** field as blank.

30. Click **Next**.
31. In the **Select your data synchronization preference** field, select **Automatic seeding**.

    It creates the EDM database on the secondary SQL Server.

    While creating the Availability Group for EDM, you might get an error message asking you to check the disk configuration. To resolve the error, ensure that the locations for EDM data and log files on the primary replica match the drive letters for the EDM data and log files locations on the secondary replica.

    The time taken to replicate Context Store EDM data from the primary to secondary SQL Server is approximately 1 minute/GB.
32. Click **Next**.
33. Validate the AAG and click **Next**.
34. Check the summary and click **Finish**.
35. To test a manual failover of the Availability Group, do the following:
    a. On the primary or secondary SQL Server, click **Always On High Availability** > **Availability Groups**.
    b. Right-click the EDM Availability Group and click **Failover**.

Creating an EDM user on the secondary Avaya Control Manager SQL Server

About this task

Use this procedure to create an optional non-system administrator user on the secondary Avaya Control Manager SQL Server with the same name and SID that you use for the user created on the primary Avaya Control Manager SQL Server.

Procedure

1. Log in to the secondary Avaya Control Manager SQL Server.
2. Click **Start** > **Microsoft SQL Server** > **Open SQL Server Management Studio**.
3. In the Object Explorer pane, click **Connect** > **Database Engine**.

   SQL Server Management Studio displays the Connect to Server dialog box.
4. In the **Server name** field, select the local instance of SQL Server.
5. In the **Authentication** field, select **SQL Server Authentication**.
6. In the **Login** and **Password** fields, enter the system administrator credentials.

   The system administrator is usually the default sa user created during SQL Server installation.

7. Click **Connect**.
8. In the Object Explorer pane, right-click the SQL Server instance and click **New Query**.
9. In the content pane, run the following command to create a new login:

   ```
   USE [master]
   GO
   CREATE LOGIN <<same login name as created on the primary EDM>> WITH PASSWORD =
   '<<password>>', sid = <<same SID as the primary EDM login name>>,
   CHECK_POLICY=OFF
   ```

   For example:

   ```
   USE [master]
   GO
   CREATE LOGIN csEDMLogin WITH PASSWORD = 'myPassword1', sid =
   0x0589627E7A96D447865135449C41E53B, CHECK_POLICY=OFF
   ```

10. Do the following to manually failover the secondary SQL Server:
    a. Click **Always On High Availability** > **Availability Groups**.
    b. Right-click the EDM Availability Group and click **Failover**.
11. In the Object Explorer pane, click **Security** > **Logins**.
12. Right-click the newly created login name and click **Properties**.

    SQL Server Management Studio displays the Login Properties dialog box.
13. In the navigation pane, click **General**.
14. In the **Default database** field, select the EDM database name.
15. In the navigation pane, click **User Mapping**.
16. Select the **Map** check box for the EDM database.
17. Click **OK**.
18. In the Object Explorer pane, click **Databases** > ***<EDM Database>*** > **Security** > **Users**.
19. Verify that the newly created login name is available in the list of users.

Generating certificates to enable SSL connections fromContext Store to a cluster of two SQL Servers hosting EDMs configured in an AlwaysOn High Availability group

About this task

Use this procedure to generate certificates from System Manager to secure the connection between Context Store and Microsoft SQL Servers.

Important:

- Ensure that a separate SSL certificate is issued from System Manager for each SQL Server in the AlwaysOn Availability Group.

- The procedures in this section are applicable when you use System Manager as a Certificate Authority (CA) for solution elements. For a third-party CA, the procedure to create the certificate might be different.

Procedure

1. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
2. In the navigation pane, in the RA Functions section, click **Add End Entity**.
3. In the **End Entity Profile** field, select `INBOUND_OUTBOUND_TLS`.
4. In the **Username** field, enter a unique name to identify the certificate being created.
5. In the **Password (or Enrollment Code)** field, enter a password.

   For each end entity, the password is mandatory for authentication of the certificate generation request.

   Note:

   Note the username and password as they are required in the next steps.
6. In the **Confirm Password** field, re-enter the password.
7. Complete any other fields that you want in your certificate.
8. In the **CN, Common name** field, enter the FQDN of the SQL Server node where you need to install the certificate.

   The Common Name is case-sensitive.
9. In the **Subject Alternative Name** area, in the first **DNS Name** field, enter the FQDN of the other SQL Server node in the AlwaysOn Availability Group.
10. In the second **DNS Name** field, enter the FQDN of the AlwaysOn Availability Group Listener IP.
11. Leave the **IP Address** field as blank.
12. In the **Token** field, select `P12 file`.
13. Click **Add**.

    The system displays the `End Entity <username> added successfully` message.

Downloading Transport Layer Security certificate from System Manager

About this task

To import a Transport Layer Security (TLS) certificate from System Manager to your server, download the certificate to your local machine.

Before you begin

Create a TLS certificate in System Manager.

Procedure

1. Log in to System Manager.
2. Click **Services** > **Security** > **Certificates** > **Authority**.
3. On the left navigation pane, click **Public Web**.

   System Manager displays the public EJBCA pages.
4. On the left navigation pane, click **Create Browser Certificate**.

   System Manager displays the Certificate Enrollment page.
5. To generate your token, do the following:
   a. In the **Username** field, enter the user name that you enter while creating an end entity.
   b. In the **Enrollment code** field, enter the password that you enter while creating an end entity.
   c. Click **OK**.

   System Manager displays the EJBCA Token Certificate Enrollment page.
6. In the **Key length** field, select **4096 bits**, and click **Enroll**.

   System Manager downloads the `p12` certificate to your downloads folder.

Importing the TLS certificate from System Manager to Microsoft SQL Servers

About this task

Use this procedure to import Transport Layer Security (TLS) certificate from System Manager to Microsoft SQL Servers to enable AlwaysOn EDM DB HA.

Procedure

1. Log in to the primary Avaya Control Manager SQL Server.
   - You must log as the Avaya Control Manager SQL Server domain user with administrative rights for all machines in the Avaya Control Manager database cluster. To check the user name, see Finding the Avaya Control Manager SQL Server domain user on page 151.
2. Copy the relevant P12 certificate file from System Manager to a folder on the SQL Server node.
3. Navigate to the folder containing the `P12` file.
4. To open the Certificate Import Wizard page, do one of the following:
   - Double-click the `P12` file.
   - Type `certlm.msc` in the Windows Search window. On the Certificates-Local Computer page, right-click **Personal** and click **All Tasks** > **Import**.

   The Certificate Import Wizard page opens.

5. On the Certificate Import Wizard page, do the following:
   a. Select **Local Machine** and click **Next**.
   b. Click **Browse**, specify the file to import, and click **Next**.
   c. To maintain the private key security, in the **Password** field, enter the password that you use while creating an end entity in System Manager.
   d. Select the **Include all extended properties** check box and click **Next**.
   e. To select the personal certificate store where you save the certificate, select **Certificate Store Selected by User**.
   f. Click **Finish**.
6. On the Certificates-Local Computer page, right-click **Personal** > **Certificates**.
7. Double-click the required certificate.
8. Click the **Details** tab.
9. Click **Edit Properties** and enter a name for the certificate.

   Tip:

   You must save only one certificate in the personal folder of your Microsoft SQL Server so that you can choose this certificate instantly while enforcing the TLS connection.
10. Repeat Steps 1 to 17 for the secondary SQL Server.

    Follow these steps using a unique certificate created for each server as mentioned in Downloading Transport Layer Security certificate from System Manager on page 160.

Database drivers

For Context Store to communicate with the External Data Mart, you must load a JDBC-compatible driver jar file, configure it on System Manager, and then install the driver on the Context Store cluster.

Loading JDBC driver to System Manager

Before you begin

Ensure you download the JDBC driver `.jar` file compatible with the database version you want to use from the database vendor website. Ensure you are using the correct `.jar` file and the implementation class for that `.jar` file.

MS SQL server database supports the following `.jar` files:

Database	.jar file
MS SQL Server	`mssql-jdbc-7.4.1.jre8.jar` or higher **Note:** You must use the JRE8 version, because the Avaya Breeze® platform runs only on Java 8, and not other versions, such as Java 11.

Procedure

1. On the System Manager web console, click **Home** > **Elements** > **Avaya Breeze®** > **Configuration** > **JDBC Providers**.
2. Click **New** and do the following:
   - In the **Name** field, type the name of your JDBC driver, which is displayed as a service name.

     For example, `MS-SQL-JDBC-Driver`
   - In the **Class Name** field, type the name of the JDBC driver class.

     For example, the MS SQL driver class is `com.microsoft.sqlserver.jdbc.SQLServerDriver`
   - **Optional:** In the **Description** field, type a description of the JDBC driver.
3. To select the jar file, click **Choose file** and select the JDBC jar file.

   The driver appears on the list of **Available JDBC drivers**.
4. On the System Manager web console, click **Avaya Breeze®** > **Service Management** > **Services**.
5. Select the driver.
6. Click **Install** and select the Context Store cluster.
7. Click **Commit** to install the jar file to the cluster.

   Restart the Context Store cluster after installing the driver.

Deploy External Data Mart on standalone SQL Server

External Data Mart standalone deployment overview

The EDM can be deployed in one of the following supported configurations:

- *Standalone EDM non-DB HA*: EDM is deployed alone on one SQL Server.
- *Standalone EDM DB HA*: EDM is deployed alone on two SQL Servers.

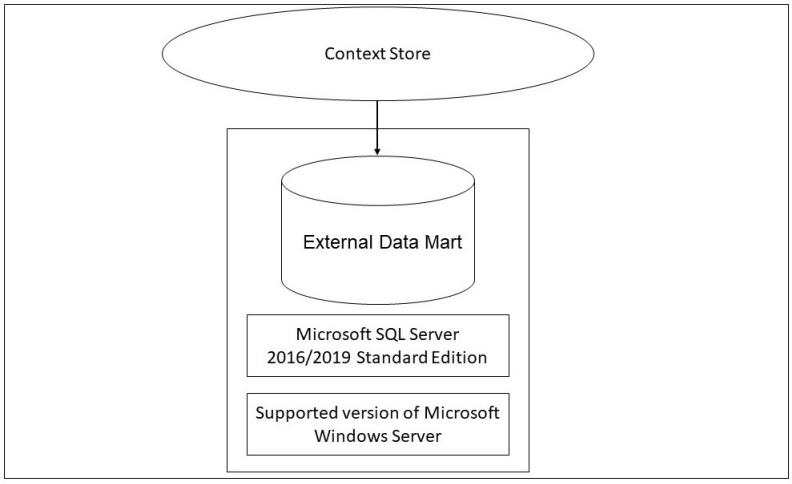
Avaya Oceana® supports High Availability (HA) of Context Store External Data Mart (EDM) in the standalone deployment. The standalone deployment specifies that you use Microsoft SQL Server Standard Edition and Windows AlwaysOn Basic Availability Group (BAG) to deploy EDM on Microsoft SQL Server without Avaya Control Manager databases.

The EDM DB HA through BAG has some limitations compared to AAG. For example, Microsoft does not support Backup on a secondary replica for BAG.

Supported configurations for the standalone deployment of External Data Mart

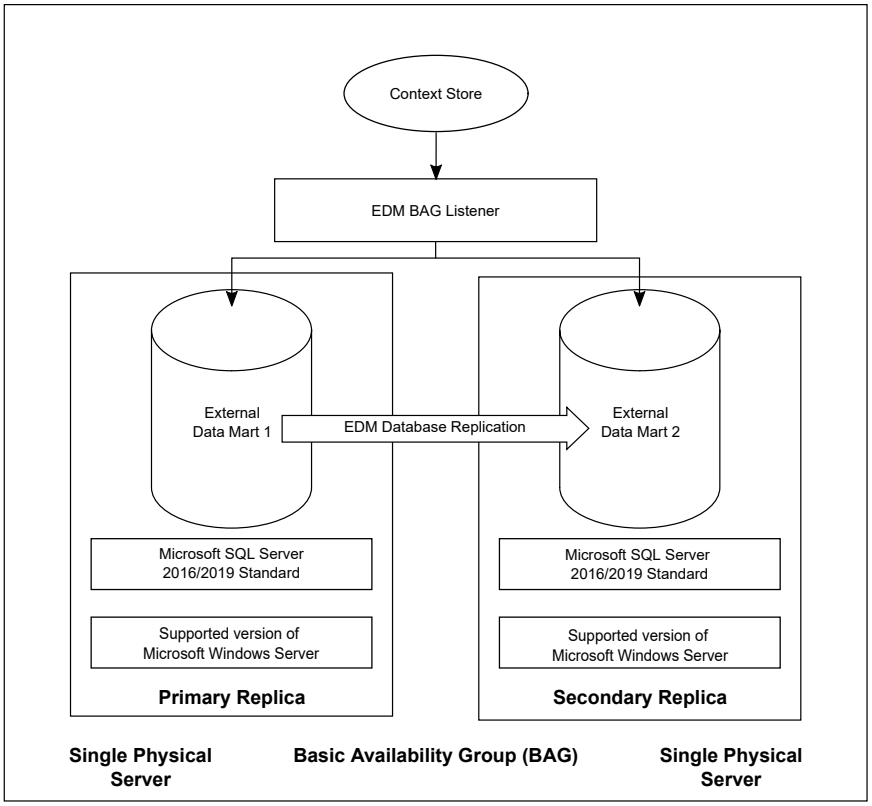
Single-site External Data Mart Non-DB HA

The following diagram depicts the architecture of a single-site non-DB HA deployment:



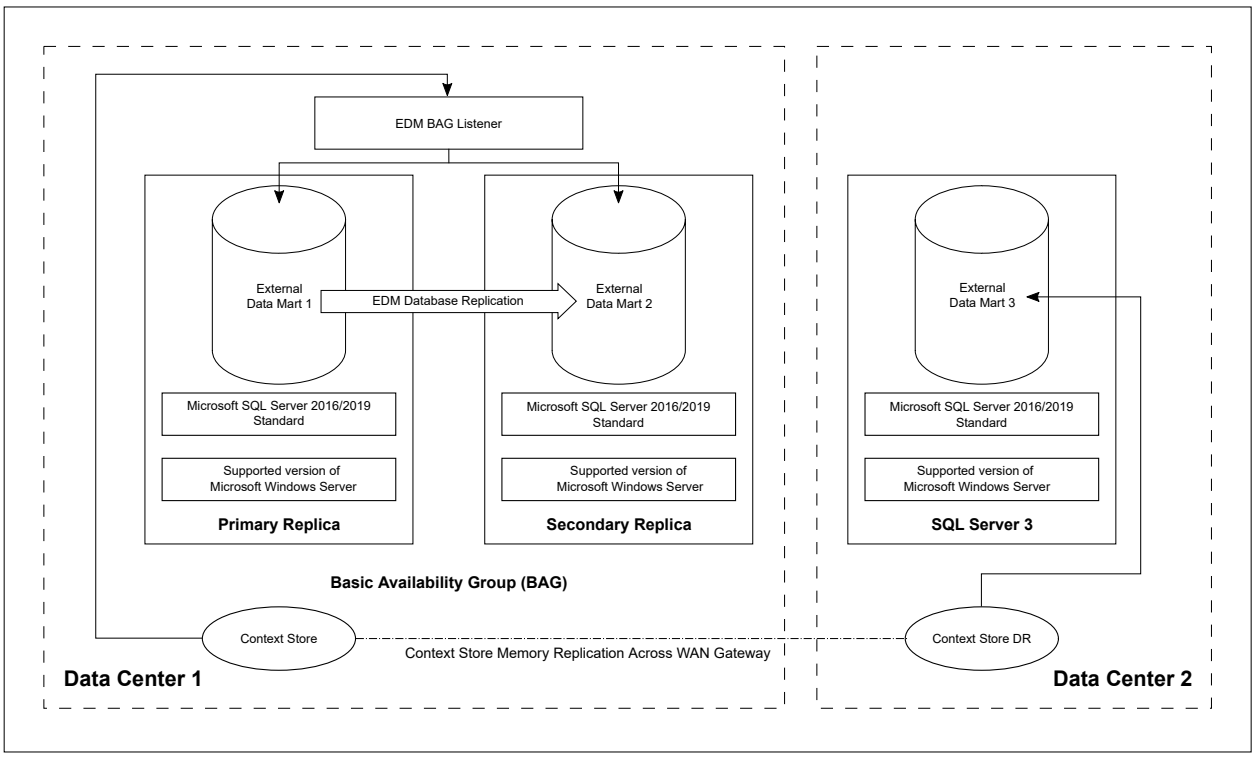
Single-site External Data Mart with Windows AlwaysOn Basic Availability Group (BAG)

The following diagram depicts the architecture of a single-site deployment:



Single-site Campus High Availability (HA) and Disaster Recovery (DR) with Windows AlwaysOn Basic Availability Group (BAG)

The following diagram depicts the architecture of a single-site Campus HA and DR deployment:



Checklist for the standalone deployment of External Data Mart

No.	Task	Description	✔
1	Configure the required hardware. For EDM non-DB HA, deploy one virtual machine. For EDM DB HA, deploy two virtual machines.	• Memory: 16 GB • vCPUs: 8 • Hard disk space: See the *Avaya Context Store External Data Mart and Customer Journey Database* details in the *Avaya Oceana hardware requirements* section in *Deploying Avaya Oceana®*.	
2	Install a supported version of the Microsoft Windows Server software on the virtual machine(s).	After installing the Windows Server, run the Microsoft Windows Update program to install any recent updates to the core software. Hostnames of the EDM database server(s) must follow the Microsoft requirements mentioned on https://support.microsoft.com/en-us/help/909264/.	

Table continues…

No.	Task	Description	✔
3	Configure a Windows Server Failover Cluster to include both Windows virtual machines. **Note:** This step is applicable only when configuring EDM DB HA.	See Configure Windows Server Failover Cluster on page 167.	
4	Install and configure a supported version of Microsoft SQL Server Standard Edition.	See Install Microsoft SQL Server Standard Edition on page 169.	
5	Create the External Data Mart (EDM) database.	See Creating the External Data Mart database for the standalone deployment on page 171.	
6	Create database tables for External Data Mart (EDM).	See Creating database tables for External Data Mart on page 153.	
7	Create an optional non-system administrator user on the primary EDM SQL Server for Context Store connections to Microsoft SQL Server.	See Creating a user on the primary External Data Mart SQL Server on page 173.	
8	Configure EDM DB HA using Microsoft SQL Server AlwaysOn software to create a Basic Availability Group (BAG). **Note:** This step is applicable only when configuring EDM DB HA.	See Creating the Basic Availability Group on External Data Mart SQL Server on page 175.	
9	Create an optional non-system administrator user on the secondary EDM SQL Server for Context Store connections to Microsoft SQL Server. **Note:** This step is applicable only when configuring EDM DB HA.	See Creating a user on the secondary External Data Mart SQL Server on page 177.	

Table continues…

No.	Task	Description	✔
10	Configure and install SSL certificates from System Manager to Microsoft SQL Servers. **Note:** This step is applicable only when configuring EDM DB HA. For EDM non-DB HA, see the *Transport Layer Security encryption checklist* section in the *Avaya Context Store Snap-In Reference Guide*.	See Generating certificates to enable SSL connections fromContext Store to a cluster of two SQL Servers hosting EDMs configured in an AlwaysOn High Availability group on page 159.	
11	Change the SQL server to use the new certificate by configuring MS SQL Server for forced encryption.	See Configuring MS SQL Server for forced encryption on page 732.	
12	Enable Transparent Data Encryption (TDE) on EDM. **Note:** TDE is an alternative to using VMWare encryption when VMWare encryption is not possible. For example, a CPOD deployment.	See Transparent Data Encryption (TDE) on External Data Mart on page 182	
13	Configure automated SQL Server Agent jobs.	See Configuring automated SQL Server Agent jobs on page 189	
14	Load a JDBC-compatible driver jar file, configure the driver on System Manager, and then install the driver on the Context Store cluster.	See Loading JDBC driver to System Manager on page 162	
15	Configure the OceanaConfiguration and ContextStoreManager attributes in System Manager to enable connection from Context Store to EDM.	See Setting attributes to enable connection from Context Store to EDM on page 180.	

Configure Windows Server Failover Cluster

The High Availability (HA) deployment of the External Data Mart (EDM) Basic Availability Group (BAG) requires Microsoft SQL Server AlwaysOn software and the Windows Server Failover Clustering (WSFC) feature on each Microsoft Windows Server operating system. You must install the supported Microsoft SQL Server AlwaysOn software and WSFC feature on each database host in the deployment.

The following four unused IP addresses are required in the same domain and network:

- One IP address for the primary database server
- One IP address for the secondary database server
- One IP address for the BAG Listener
- One IP address for WSFC

Creating an administrator user for Windows Server Failover Cluster

About this task

Use this procedure to create a single domain user with administrative rights on all machines in the cluster. This user is used for logging in to the SQL Servers and configuring all related AlwaysOn features.

Procedure

1. Log in to the Domain Controller.
2. Click **Start** > **Administrative Tools** > **Active Directory Users and Computers**.
3. In the navigation pane, expand the domain that you create for the users.
4. Right-click the **Users** folder and click **New** > **User**.
5. In the **New Object - User** dialog box, do the following:
    a. In the **First name** field, enter the first name of the user.
    b. In the **Last name** field, enter the surname of the user.
    c. In the **User logon name** field, enter the user name.
    d. Click **Next**.
    e. In the **Password** field, enter a password for the user.
    f. In the **Confirm Password** field, re-enter the password.
    g. Clear the **User must change password at next logon** check box.
    h. Select the **Password never expires** check box.
    i. Click **Next**.
    j. Click **Finish**.

    The server displays the new user in the list in the content pane.
6. On each SQL Server, do the following:
    a. Click **Control Panel** > **User Accounts** > **User Accounts** > **Manager User Accounts**.
    b. In the Users dialog box, click **Add**.
    c. On the Add a user screen, click **Browse**.
    d. On the Select User screen, click **Locations** and select the domain where you created the domain user.

e. Click **OK**.

f. On the Select User screen, click **Advanced** > **Find Now**.

g. In the Search results window, select the domain user and click **OK**.

The server displays the domain user in the **Enter the object name to select** box.

h. Click **OK**.

i. On the Add a user screen, verify the user name and domain of the user and click **Next**.

j. On the What level of access do you want to grant this user screen, select **Administrator** and click **Finish**.

Use this user to log in to each Windows server when configuring WSFC and SQL Server.

Configuring a Windows Server Failover Cluster

About this task

Use this procedure to configure a Windows Server Failover Cluster (WSFC).

Procedure

1. Log in to each Windows Server to check if the Windows Failover Cluster Feature is installed.
2. Click **Server Manager** > **Tools**.
3. Check for the **Failover Cluster Manager** option.
4. If the **Failover Cluster Manager** option is not available, do the following to add the option:

   Click **Server Manager** > **Manage** > **Add roles and features**.
5. Keep clicking **Next** until the Features screen.
6. Select **Failover Clustering** and click **Install**.
7. To configure a WSFC, follow the steps on the https://social.technet.microsoft.com/wiki/contents/articles/36143.sql-server-2016-step-by-step-creating-alwayson-availability-group.aspx#Windows_Failover_Clustering_Configuration_for_Always_On_Availability_Groups link.

Install Microsoft SQL Server Standard Edition

Prerequisites

- Download a supported version of Microsoft SQL Server Standard Edition software to the database servers.
- Verify that none of the systems used in the cluster is a domain controller.
- Verify that each computer is on the same network.
- Verify that each computer is operating on a supported version of Microsoft Windows Server.
- Open port 5022 and port 1433 in the firewall settings on each Microsoft Windows Server. See Opening a port in the Windows Firewall for TCP access on page 170.

- When installing SQL Server on virtual machines, read VMware's best practices published at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/sql-server-on-vmware-best-practices-guide.pdf. A summary of these recommendations includes:
  - Store the database log files on a separate disk than the disk where you store database data files. It avoids I/O contention for the disk because the contention leads to poor performance.
  - Install SQL Server on to the same disk where you install the Windows operating system.

Installation

- Follow the installation instructions in the Microsoft SQL Server Installation Guide at https://docs.microsoft.com/en-us/sql/database-engine/install-windows/install-sql-server?view=sql-server-ver15.
- During the installation, select the New SQL Server standalone installation or add features to an existing installation option.
- Do not select the New SQL Server failover cluster installation option.
- SQL Server Failover Cluster Installation is not supported for External Data Mart HA.
- Ensure that you install Microsoft SQL Server Standard Edition on both SQL Servers.

Post-installation

- Install SQL Server Management Studio on both SQL Servers. For installation instructions, go to https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?redirectedfrom=MSDN&view=sql-server-ver15.
- Enable the AlwaysOn Availability Groups feature on both SQL Servers.

Opening a port in the Windows Firewall for TCP access

About this task

Use this procedure to open a port in the Windows Firewall for TCP access.

Procedure

1. Log in to the Microsoft Windows Server.
2. Click **Start** > **Run**.
3. In the Run dialog box, type `WF.msc` and click **OK**.

   The server displays the Windows Firewall with Advanced Security screen.
4. In the navigation pane, right-click **Inbound Rules** and click **New Rule** in the Actions pane.
5. On the Rule Type screen, select **Port** and click **Next**.
6. On the Protocol and Ports screen, select **TCP**.
7. Select **Specific local ports** and type the port number of the instance of the database engine. 1433 and 5022 for the default instance.
8. Click **Next**.
9. On the Action screen, select **Allow the connection** and click **Next**.

10. On the Profile screen, select any profiles that describe the computer connection environment to connect to the database engine, and then click **Next**.
11. On the Name screen, type a name and description for this rule, and then click **Finish**.
12. Repeat Steps 1 to 11 for the second Microsoft Windows Server.

Enabling the Always On Availability Groups feature

About this task

You must enable the **Always On Availability Groups** feature on every SQL Server instance in the cluster.

Procedure

1. Log in to the EDM server.
2. Click **Start** > **Microsoft SQL Server** > **SQL Server Configuration Manager**.
3. In the navigation pane, click **SQL Server Services**.
4. In the content pane, right-click the SQL Server instance, and then click **Properties**.

   The SQL Server Properties dialog box opens.
5. Select the **Always On Availability Groups** tab (**AlwaysOn High Availability** in SQL Server 2016):
   a. In the **Windows Server Failover Cluster** field (**Windows failover cluster name** in SQL Server 2016), ensure the correct Windows Server Failover Cluster is selected.
   b. Select the **Enable Always On Availability Groups** check box (**Enable AlwaysOn Availability Groups** in SQL Server 2016).
6. On the **Log On** tab, select **This account**, and enter the account name and password of the domain user that was used to create the Windows Server Failover Cluster.

   Ensure that you include the domain in the account name. For example, `myDomain\myUsername`.
7. Click **OK**.
8. In the content pane, right-click the SQL Server instance and click **Restart**.
9. Repeat the process for each SQL Server instance in the cluster.

Creating the External Data Mart database for the standalone deployment

About this task

Use this procedure to create the External Data Mart (EDM) database for the standalone deployment EDM.

Procedure

1. Log in to the primary EDM SQL Server.
2. Open the SQL Server Management Studio on the SQL Server that needs to become the primary replica.

3. In the Object Explorer pane, click **Connect** > **Database Engine**.

   SQL Server Management Studio displays the Connect to Server dialog box.

4. In the **Server name** field, select the local instance of SQL Server.
5. In the **Authentication** field, select **SQL Server Authentication**.
6. In the **Login** and **Password** fields, enter the system administrator credentials.

   The system administrator is usually the default sa user created during SQL Server installation.

7. Click **Connect**.
8. In the Object Explorer pane, expand **Databases**.

   Important:

   Do not point your Avaya Oceana® to the new EDM until EDM configuration and migration is complete. EDM configuration and migration also include creating an optional non-sa user and adding the EDM into the Basic Availability Group (BAG).

9. Right-click **Databases** and click **New Database**.

   SQL Server Management Studio displays the New Database dialog box.

10. In the navigation pane, click **General**.
11. In the **Database name** field, enter a name for the EDM database.
12. In the **Database files** section, do the following:

    a. For **File Type = ROWS Data**, click the three dots to the right of the **Path** field.

    b. Browse to the correct folder and click **OK**.

    To change the initial size for the EDM Data file, click the arrows to the right of the **Initial Size (MB)** value for **File Type = ROWS Data** and change the default value. For example, for 300 GB, enter 307200.

13. In the **Database files** field, do the following:

    a. For **File Type = LOG**, click the three dots to the right of the **Path** field.

    b. Browse to the correct folder and click **OK**.

    To change the initial size for the EDM Log file, click the arrows to the right of the **Initial Size (MB)** value for **File Type = LOG** and change the default value. For example, for 20 GB, enter 20480.

    Ensure that hourly transaction log backups are taken. You can download the SampleSQLServerAgentScripts.zip from https://support.avaya.com/ or https://www.devconnectprogram.com/. For more information on configuring the SampleSQLServerAgentScripts, see the *Configuring automated SQL Server Agent jobs* topic in the *Deploying Avaya Oceana®* document.

    You must also create the same paths and folders for EDM data files and EDM log files on the secondary SQL replica before adding the EDM to BAG.

14. In the navigation pane, click **Options**.
15. In the **Collation** field, select the appropriate option or leave it as default.
16. In the **Recovery model** field, select **Full**.
17. Click **OK**.

Creating database tables for External Data Mart

About this task

To use the External Data Mart feature, you must use the supported databases, the respective supported versions, and create the required database tables.

Note:

The Microsoft SQL database user configured for the EDM feature must have database ownership or system administrator privileges for this connection to be successful. Also, from the security profile of the database user, you must set the Context Store database as the default database.

Procedure

1. Download the `ContextStoreSchemaCreationScripts-SQLServer.zip` file from Avaya Support.
2. Copy the zip file to the server running the MS SQL Server.
3. Extract the zip file and locate the SQL script: `CreateEDMschema.sql`.
4. Open SQL Server Management Studio and do the following:.
   a. On the **File** menu, click **Open** to open the file.
   b. Click **Execute** or click **Query** > **Execute** to run the file.
5. Create database tables for External Data Mart by executing the `CreateEDMschema.sql` script.

Creating a user on the primary External Data Mart SQL Server

About this task

Use this procedure to create an optional non-system administrator user on the primary External Data Mart (EDM) SQL Server.

Procedure

1. Log in to the primary EDM SQL Server.
2. Click **Start** > **Microsoft SQL Server** > **Open SQL Server Management Studio**.
3. In the Object Explorer pane, click **Connect** > **Database Engine**.

   SQL Server Management Studio displays the Connect to Server dialog box.
4. In the **Server name** field, select the local instance of SQL Server.
5. In the **Authentication** field, select **SQL Server Authentication**.

6. In the **Login** and **Password** fields, enter the system administrator credentials.

   The system administrator is usually the default sa user created during SQL Server installation.

7. Click **Connect**.
8. In the Object Explorer pane, right-click the SQL Server instance and click **New Query**.
9. In the content pane, run the following command to create a new login:

   ```
   USE [master]
   GO
   CREATE LOGIN <<loginName>> WITH PASSWORD = '<<password>>', CHECK_POLICY=OFF
   ```

   For example:

   ```
   USE [master]
   GO
   CREATE LOGIN csEDMLogin WITH PASSWORD = 'myPassword1', CHECK_POLICY=OFF
   ```

10. Run the following command to select the security identifier (SID) for the new login:

    ```
    SELECT sid, name FROM syslogins where name = '<<loginName>>'
    ```

    For example:

    ```
    SELECT sid, name FROM syslogins where name = 'csEDMLogin'
    shows SID = 0x0589627E7A96D447865135449C41E53B
    ```

    Important:

    SID is used when creating the user if using a pair of SQL Servers for database high availability.

11. In the Object Explorer pane, click **Security** > **Logins**.
12. Right-click the newly created login name and click **Properties**.

    SQL Server Management Studio displays the Login Properties dialog box.

13. In the navigation pane, click **General**.
14. In the **Default database** field, select the name for the EDM database.
15. In the navigation pane, click **User Mapping**.
16. Select the **Map** check box for the EDM database.
17. Click **OK**.
18. In the Object Explorer pane, click **Databases** > ***<EDM Database>*** > **Security** > **Users**.
19. Verify that the newly created login name is available in the list of users.
20. In the Object Explorer pane, right-click the EDM database and click **New Query**.
21. In the content pane, run the following commands to grant permissions to the newly created user:

    ```
    GRANT SELECT, INSERT, UPDATE, DELETE ON CS_OPERATION TO <<loginName>>;
    GRANT SELECT, INSERT, UPDATE ON CS_PROVISION TO <<loginName>>;
    GRANT SELECT, INSERT, UPDATE ON GENERATED_KEYS TO <<loginName>>;
    GRANT SELECT, INSERT, UPDATE ON INTERACTION_NOTE to <<loginName>>;
    ```

```
GRANT SELECT, INSERT, UPDATE ON INTERACTION_PARTICIPANT to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON SERVICE_ATTRIBUTE to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON SERVICE_ATTRIBUTE_GROUP to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON ROUTING_SERVICE to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON CUSTOM_DETAIL to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON INTERACTION to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON LINK to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON TOPIC to <<loginName>>;
GRANT SELECT, INSERT, UPDATE, DELETE ON ENGAGEMENT to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON OUTCOME to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON SENTIMENT_RATING to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON TENANT to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON INTERACTION_STATUS to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON INTERACTION_SUBSTATUS to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON CHANNEL_SUBTYPE to <<loginName>>;
GRANT SELECT, INSERT, UPDATE ON CHANNEL_TYPE to <<loginName>>;
GRANT SELECT, INSERT, UPDATE, DELETE ON CS_RESURRECT to <<loginName>>;
```

Creating the Basic Availability Group on External Data Mart SQL Server

About this task

Use this procedure to create the Basic Availability Group (BAG) on External Data Mart (EDM) SQL Server.

Procedure

1. Log in to the primary EDM SQL Server.
2. Click **Start** > **Microsoft SQL Server** > **Open SQL Server Management Studio**.
3. In the Object Explorer pane, click **Connect** > **Database Engine**.

   SQL Server Management Studio displays the Connect to Server dialog box.
4. In the **Server name** field, select the local instance of SQL Server.
5. In the **Authentication** field, select **SQL Server Authentication**.
6. In the **Login** and **Password** fields, enter the system administrator credentials.

   The system administrator is usually the default sa user created during SQL Server installation.
7. Click **Connect**.
8. In the Object Explorer pane, click **Databases** > ***<EDM Database>***.
9. Right-click the EDM database and click **Tasks** > **Back Up**.

   SQL Server Management Studio displays the Back Up Database dialog box.
10. In the navigation pane, click **General**.
11. In the **Backup type** field, select **Full**.
12. In the **Destination** area, click **Add**.
13. In the Select Backup Destination dialog box, select the path to the backup folder location, specify the backup file name with the `.bak` extension, and click **OK**.

Ensure that the SQLService User login (services.msc) has full permissions on the backup folder.

14. To provide full permissions to the SQLService User login, do the following:
    a. Go to the backup folder location.
    b. Right-click the backup folder and click **Properties**.
    c. On the Security tab, select the SQLService User login and click **Edit**.
    d. In the **Permissions** area, select the Full control check box.
    e. Click **OK**.
15. Click **OK**.
16. In the Object Explorer pane, click **Always On High Availability**.
17. Right-click **Availability Groups** and click **New Availability Group Wizard**.

    SQL Server Management Studio displays the New Availability Group dialog box.
18. In the navigation pane, click **Specify Options**.
19. In the **Availability group name** field, enter a name for the Context Store availability group.
20. In the **Cluster type** field, select **Windows Server Failover Cluster**.
21. Select the **Database Level Health Detection** check box.
22. Select the **Per Database DTC Support** check box.
23. Click **Next**.
24. In the **Select user databases for the availability group** field, select the EDM database.
25. Click **Next**.
26. Click **Add Replica**, specify the other SQL Server as the secondary replica, and connect to the database engine of the other SQL Server using SQL Server Authentication and System Administrator login credentials.
27. Do the following for each replica:
    a. Select the **Automatic Failover** check box.
    b. Select the **Synchronous Commit** check box.
    c. Set the **Readable Secondary** field to No.
28. On the Listener tab, select **Create an Availability Group Listener** and do the following:

    In the **Listener DNS Name** field, enter the name of the listener to access the BAG from Context Store.

    You must adhere to the specific requirements for the DNS Name of an Availability Group Listener mentioned in the Configure a listener for an Always On availability group on the Microsoft Documentation website.

    In the **Port** field, type `1433`.

29. Click **Next**.
30. In the **Select your data synchronization preference** field, select **Automatic seeding**.

    It creates the EDM database on the secondary SQL Server.

    While creating the Availability Group for EDM, you might get an error asking you to check the disk configuration. To resolve the error, ensure that the locations for EDM data and log files on the primary replica match the drive letters for the EDM data and log files locations on the secondary replica.

    The time taken to replicate Context Store EDM data from the primary to secondary SQL Server is approximately 1 minute/GB.
31. Click **Next**.
32. Validate the BAG and click **Next**.
33. Check the summary and click **Finish**.
34. To view the Availability Group status, do the following:
    a. On the primary or secondary SQL Server, click **Always On High Availability** > **Availability Groups**.
    b. Right-click the EDM Availability Group and click **Show Dashboard**.

Creating a user on the secondary External Data Mart SQL Server

About this task

Use this procedure to create an optional non-system administrator user on the secondary External Data Mart (EDM) SQL Server with the same name and SID that you use for the user created on the primary EDM SQL Server.

Procedure

1. Log in to the secondary EDM SQL Server.
2. Click **Start** > **Microsoft SQL Server** > **Open SQL Server Management Studio**.
3. In the Object Explorer pane, click **Connect** > **Database Engine**.

   SQL Server Management Studio displays the Connect to Server dialog box.
4. In the **Server name** field, select the local instance of SQL Server.
5. In the **Authentication** field, select **SQL Server Authentication**.
6. In the **Login** and **Password** fields, enter the system administrator credentials.

   The system administrator is usually the default sa user created during SQL Server installation.
7. Click **Connect**.
8. In the Object Explorer pane, right-click the SQL Server instance and click **New Query**.

9. In the content pane, run the following command to create a new login:

```
USE [master]
GO
CREATE LOGIN <<same login name as created on the primary EDM>> WITH PASSWORD =
'<<password>>', sid = <<same SID as the primary EDM login name>>,
CHECK_POLICY=OFF
```

   For example:

```
USE [master]
GO
CREATE LOGIN csEDMLogin WITH PASSWORD = 'myPassword1', sid =
0x0589627E7A96D447865135449C41E53B, CHECK_POLICY=OFF
```

10. Do the following to manually failover the secondary SQL Server:
    a. Click **Always On High Availability** > **Availability Groups**.
    b. Right-click the EDM Availability Group and click **Failover**.
11. In the Object Explorer pane, click **Security** > **Logins**.
12. Right-click the newly created login name and click **Properties**.

    SQL Server Management Studio displays the Login Properties dialog box.
13. In the navigation pane, click **General**.
14. In the **Default database** field, select the EDM database name.
15. In the navigation pane, click **User Mapping**.
16. Select the **Map** check box for the EDM database.
17. Click **OK**.
18. In the Object Explorer pane, click **Databases** > ***<EDM Database>*** > **Security** > **Users**.
19. Verify that the newly created login name is available in the list of users.

Database drivers

For Context Store to communicate with the External Data Mart, you must load a JDBC-compatible driver jar file, configure it on System Manager, and then install the driver on the Context Store cluster.

Loading JDBC driver to System Manager

Before you begin

Ensure you download the JDBC driver `.jar` file compatible with the database version you want to use from the database vendor website. Ensure you are using the correct `.jar` file and the implementation class for that `.jar` file.

MS SQL server database supports the following `.jar` files:

Database	.jar file
MS SQL Server	`mssql-jdbc-7.4.1.jre8.jar` or higher **Note:** You must use the JRE8 version, because the Avaya Breeze® platform runs only on Java 8, and not other versions, such as Java 11.

Procedure

1. On the System Manager web console, click **Home** > **Elements** > **Avaya Breeze®** > **Configuration** > **JDBC Providers**.
2. Click **New** and do the following:
   - In the **Name** field, type the name of your JDBC driver, which is displayed as a service name.

     For example, `MS-SQL-JDBC-Driver`
   - In the **Class Name** field, type the name of the JDBC driver class.

     For example, the MS SQL driver class is `com.microsoft.sqlserver.jdbc.SQLServerDriver`
   - **Optional:** In the **Description** field, type a description of the JDBC driver.
3. To select the jar file, click **Choose file** and select the JDBC jar file.

   The driver appears on the list of **Available JDBC drivers**.
4. On the System Manager web console, click **Avaya Breeze®** > **Service Management** > **Services**.
5. Select the driver.
6. Click **Install** and select the Context Store cluster.
7. Click **Commit** to install the jar file to the cluster.

   Restart the Context Store cluster after installing the driver.

Generating certificates to enable SSL connections fromContext Store to a cluster of two SQL Servers hosting EDMs configured in an AlwaysOn High Availability group

About this task

Use this procedure to generate certificates from System Manager to secure the connection between Context Store and Microsoft SQL Servers.

Important:

- Ensure that a separate SSL certificate is issued from System Manager for each SQL Server in the AlwaysOn Availability Group.

- The procedures in this section are applicable when you use System Manager as a Certificate Authority (CA) for solution elements. For a third-party CA, the procedure to create the certificate might be different.

Procedure

1. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
2. In the navigation pane, in the RA Functions section, click **Add End Entity**.
3. In the **End Entity Profile** field, select `INBOUND_OUTBOUND_TLS`.
4. In the **Username** field, enter a unique name to identify the certificate being created.
5. In the **Password (or Enrollment Code)** field, enter a password.

   For each end entity, the password is mandatory for authentication of the certificate generation request.

   Note:

   Note the username and password as they are required in the next steps.
6. In the **Confirm Password** field, re-enter the password.
7. Complete any other fields that you want in your certificate.
8. In the **CN, Common name** field, enter the FQDN of the SQL Server node where you need to install the certificate.

   The Common Name is case-sensitive.
9. In the **Subject Alternative Name** area, in the first **DNS Name** field, enter the FQDN of the other SQL Server node in the AlwaysOn Availability Group.
10. In the second **DNS Name** field, enter the FQDN of the AlwaysOn Availability Group Listener IP.
11. Leave the **IP Address** field as blank.
12. In the **Token** field, select `P12 file`.
13. Click **Add**.

    The system displays the `End Entity <username> added successfully` message.

Setting attributes to enable connection from Context Store to EDM

About this task

Use this procedure to configure the OceanaConfiguration attributes in System Manager to enable connection from Context Store to External Data Mart (EDM).

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In the **Cluster** field, select **ProvisioningCluster**.
   b. In the **Service** field, select **OceanaConfiguration**.
3. For **External Data Mart Database Type**, do the following:
   a. Select **Override Default**.
   b. In the **Effective Value** field, select **Microsoft SQL Server**.
4. For **External Data Mart FQDN**, do the following:
   a. Select **Override Default**.
   b. In the **Effective Value** field, do one of the following:
      - For EDM DB HA, enter the FQDN of the Availability Group Listener.
      - For EDM non-DB HA, enter the FQDN of Microsoft SQL Server.
5. For **External Data Mart Port**, do the following:
   a. Select **Override Default**.
   b. In the **Effective Value** field, type `1433`.

      It is the default port number.
6. For **External Data Mart Database Name**, do the following:
   a. Select **Override Default**.
   b. In the **Effective Value** field, enter the same name that you use when creating the EDM database.
7. For **External Data Mart Username**, do the following:
   a. Select **Override Default**.
   b. In the **Effective Value** field, enter the sa or non-sa user name to access the EDM database.
8. For **External Data Mart Password**, do the following:
   a. Select **Override Default**.
   b. In the **Effective Value** field, enter the password to access the EDM database.
9. For **External Data Mart Persistence Type**, do the following:
   a. Select **Override Default**.
   b. In the **Effective Value** field, select **Journey**.

      Only the Journey persistence type is supported in Avaya Oceana®.

10. Click **Commit**.

Transparent Data Encryption (TDE) on External Data Mart

Transparent Data Encryption (TDE) prevents the theft of sensitive data stored in the Context Store External Data Mart (EDM) on the SQL server as part of the Avaya Oceana® solution. TDE encrypts EDM data which includes all EDM files and backups. Support for TDE of EDM data is an alternative to VMWare encryption, particularly for CPOD deployments, where VMWare encryption is impossible.

Important:

TDE can be enabled on the EDM when the EDM is installed on either one SQL server or in a cluster of two SQL servers.

For more information about TDE, see https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-ver15.

Supported Configurations

Avaya Oceana® supports Transparent Data Encryption (TDE) on the Context Store (CS) EDM in the following configurations:

- *EDM/ACM co-res*: EDM is deployed co-resident with the ACM databases on two SQL servers (DB HA).

  Note:

  The supported SQL server versions in the following table are also supported when the EDM is installed on a single SQL server (no DB HA, no AlwaysOn High Availability). However, enabling TDE on a single SQL server for ACM/EDM co-res is only supported as a lab deployment and not a production deployment.

SQL Server		Type of Always On High Availability (SQL Server DB HA)
Version	**Edition**	
2019	Enterprise	Advanced Availability Group (AAG)
2017	Enterprise	Advanced Availability Group (AAG)

- *Standalone EDM*: EDM is deployed alone without ACM DBs on one SQL server (non-DB HA) or EDM is deployed alone on two SQL servers (DB HA).

SQL Server		Type of AlwaysOn High Availability (SQL Server DB HA)
Version	**Edition**	
2019	Standard	Basic Availability Group (BAG)

Note:

TDE for Standalone EDM is applicable only for Oceana deployments. TDE is not supported for standalone Context Store deployments (non-Oceana deployments).

Enabling TDE on an EDM installed on a cluster of SQL servers

About this task

Use this procedure to enable Transparent Data Encryption (TDE) on the Context Store External Data Mart when it is deployed in a database HA configuration using AlwaysOn Availability Groups.

You can enable TDE on EDM when it is deployed:

- Co-resident with the Avaya Control Manager databases in a cluster of two SQL servers using an AlwaysOn Advanced Availability Group (AAG).
- Standalone (no ACM DBs installed on the SQL server) in a cluster of two SQL servers using an AlwaysOn Basic Availability Group (BAG).

Before you begin

Ensure that the EDM is added to the Availability Group.

Procedure

1. Do the following on the Primary SQL server:
   a. Log in to the local instance of SQL server in SQL Server Management Studio (SSMS) as the domain user configured to use the SQL server service.

      The domain user can be found in the **Log On As** column under **SQL Server Services**. For more information on finding the domain user, see Finding the Avaya Control Manager SQL Server domain user on page 151.

   b. In the Object Explorer pane, right-click the local SQL server instance and click **New Query**.

   c. To create the master key for the SQL server, run the following T-SQL commands and click **Execute**:

```
USE MASTER
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<enter strong password>'
GO
```

      Note:

      If a master key is already created on the SQL server, an error is displayed. If you know the password for the existing master key, continue to the next step. If you do not know the password, see Creating a new master key with a known password on page 186.

   d. To create a certificate for the EDM and also a backup certificate and private key, run the following T-SQL commands and click **Execute**:

      Note:

      It is recommended to save the backup certificate and the private key off the SQL server.

      For example,

```
CREATE CERTIFICATE <name of new EDM certificate>
WITH SUBJECT = '<enter any subject e.g. CSEDM TDE Certificate for the EDM
```

```
Availability Group>'
USE MASTER
GO
BACKUP CERTIFICATE <name of new EDM certificate>
TO FILE = '<enter file location, for example C:><name of new EDM
certificate>_File.cer'
WITH PRIVATE KEY (FILE = '<enter file location, for example C:><name of new
EDM certificate>_Key.pvk' ,
ENCRYPTION BY PASSWORD = '<enter strong password>' )
GO
```

e. Copy `<enter file location, for example C:><name of new EDM certificate>.cer` and `<enter file location, for example C:><name of new EDM certificate>.pvk` from the primary to the secondary SQL server.

2. Do the following on the Secondary SQL server:

   a. Log in to the local instance of the SQL server in SQL Server Management Studio (SSMS) as the domain user configured to use the SQL server service.

      The domain user can be found in the **Log On As** column under SQL **Server Services**. For more information on finding the domain user, see Finding the Avaya Control Manager SQL Server domain user on page 151.

   b. In the Object Explorer pane, right-click the local SQL server instance and click **New Query**.

   c. To create the master key for the SQL server, run the following T-SQL commands and click **Execute**:

```
USE MASTER
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<strong password>'
GO
```

      Note:

      If a master key is already created on the SQL server, an error is displayed. If you know the password for the existing master key, continue to the next step. If you do not know the password, see Creating a new master key with a known password on page 186.

   d. To create a certificate for the EDM, run the following T-SQL commands and click **Execute**:

```
USE MASTER
GO
CREATE CERTIFICATE <name of new EDM certificate as used on the Primary SQL
Server>
FROM FILE = '<enter file location, for example C:><name of new EDM
certificate as used on the Primary SQL Server>.cer'
WITH PRIVATE KEY (FILE = '<enter file location, for example C:><name of new
EDM certificate as used on the Primary SQL Server>.pvk',
DECRYPTION BY PASSWORD = '<strong password (same password used to encrypt
the private key on the Primary SQL Server>' );
```

3. To enable encryption on the Primary SQL server, run the following commands to create the encryption key of the EDM:

Note:

Run these commands only on the Primary SQL server.

```
USE <name of EDM DB>
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_256
ENCRYPTION BY SERVER CERTIFICATE <name of new EDM certificate>
GO
```

4. To enable TDE on the EDM, run the following T-SQL commands:

   Note:

   Run this command only on the Primary SQL server.

   ```
   ALTER DATABASE <name of EDM DB>
   SET ENCRYPTION ON
   ```

   Note:

   It takes approximately one hour to encrypt a 300 GB EDM data file.

5. To check if the encryption was successful, run the following T-SQL commands on the primary and secondary SQL servers:

   ```
   SELECT
   db.name,
   db.is_encrypted,
   dm.encryption_state,
   dm.percent_complete,
   dm.key_algorithm,
   dm.key_length
   FROM sys.databases db
   LEFT OUTER JOIN sys.dm_database_encryption_keys dm
   ON db.database_id = dm.database_id;
   ```

   The preceding commands return a number that represents the `encryption_state` for the EDM (0-6). For more information about the encryption state codes, see https://docs.microsoft.com/en-us/sql/relational-databases/system-dynamic-management-views/sys-dm-database-encryption-keys-transact-sql?view=sql-server-ver15.

   For more information on enabling TDE on ACM databases, see *Maintaining and Troubleshooting Avaya Control Manager*.

   Note:

   Keep valid backups of the following files in case of disaster:

   - The certificate that encrypts the DEK
   - The password to the private key of the TDE certificate
   - The password to decrypt the master key in the master database
   - A healthy backup of the system and user databases

   For information on recovering a TDE enabled database when the user does not have various combinations of the master key password, a backup of the master database,

backups of the certificate and private key, password for the private key, or password to decrypt master database, see: https://techcommunity.microsoft.com/t5/sql-server-support-blog/recover-tde-databases-in-disaster-recover-steps-for-3-common/ba-p/2963600.

Creating a new master key with a known password

About this task

If a master key is already created on the SQL server, an error is displayed if a user attempts to create another master key. If you do not know the password for the existing master key, you must decrypt all databases, then drop all the certificates associated with the master key and create a new master key with a known password.

You need to recreate any of the certificates that were dropped but are still required for encryption. Then, re-encrypt the databases with the new certificates.

Note:

Ensure that you store the master key password in a secure location for future use.

Procedure

1. To view all certificates, run the following command:

```
SELECT name, certificate_id, principal_id, pvt_key_encryption_type_desc,
start_date, expiry_date
FROM sys.certificates;
```

2. To drop a certificate, run the following command:

```
DROP CERTIFICATE <nameOfCert>
```

If the certificate cannot be dropped because it is in use with a database encryption key, drop the database encryption key.

3. To drop the database encryption key, run the following command:

```
USE <name of database >
GO
DROP DATABASE ENCRYPTION KEY
GO
```

If a database encryption key cannot be dropped, turn off encryption for that database.

Note:

Turning off encryption can take a significant amount of time. For example, decrypting 100GB of data can take approximately one hour.

4. To turn off encryption for the database, run the following command:

```
ALTER DATABASE <name of database > SET ENCRYPTION OFF;
```

5. To drop the master key, run the following command:

```
DROP MASTER KEY
```

Enabling TDE on an EDM installed on a single SQL server

About this task

Use this procedure to enable Transparent Data Encryption (TDE) on the Context Store External Data Mart when it is it is deployed standalone on a single SQL server.

This can be either one of the following configurations:

- *Standalone EDM non-DB HA*: EDM is deployed alone on one SQL server (within an Oceana deployment only).
- *Co-resident with ACM*: EDM is deployed on only one SQL server (lab deployment only, not supported in production).

Follow this procedure for enabling TDE on the EDM when it is installed on only one SQL server.

Procedure

1. Establish a remote desktop connection to the SQL server.
2. Log in to the local instance of SQL server in SQL Server Management Studio (SSMS) as the domain user configured to use the SQL server service.

   The domain user can be found in the **Log On As** column under **SQL Server Services**. For more information on finding the domain user, see Finding the Avaya Control Manager SQL Server domain user on page 151.
3. In the Object Explorer pane, right-click the local SQL server instance and click **New Query**.
4. To create the master key for the SQL Server, run the following T-SQL commands and click **Execute**:

   ```
   USE MASTER
   GO
   CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<enter strong password>'
   GO
   ```

   Note:

   If a master key is already created on the SQL server, an error is displayed. If you know the password for the existing master key, continue to the next step. If you do not know the password, see Creating a new master key with a known password on page 186.
5. To create a new certificate for the EDM and also a backup certificate and private key, run the following T-SQL commands and click **Execute**:

   Note:

   It is recommended to save the backup certificate and the private key off the SQL server.

   For example,

   ```
   CREATE CERTIFICATE <name of new EDM certificate>
   WITH SUBJECT = '<enter any subject e.g. CSEDM TDE Certificate>'
   GO
   USE MASTER
   GO
   BACKUP CERTIFICATE <name of new EDM certificate>
   ```

```
TO FILE = '<enter file location, for example C:><name of new EDM
certificate>_File.cer'
WITH PRIVATE KEY (FILE = '<enter file location, for example C:><name of new EDM
certificate>_Key.pvk' ,
ENCRYPTION BY PASSWORD = '<enter strong password>' )
GO
```

6. To enable encryption on the SQL server, run the following commands to create the encryption key of the EDM:

```
USE <name of EDM DB>
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_256
ENCRYPTION BY SERVER CERTIFICATE <name of new EDM certificate>
GO
```

7. To enable TDE on the EDM, run the following T-SQL commands:

```
ALTER DATABASE <name of EDM DB>
SET ENCRYPTION ON
GO
```

8. To check if the encryption was successful, run the following T-SQL commands on the SQL server:

```
SELECT
db.name,
db.is_encrypted,
dm.encryption_state,
dm.percent_complete,
dm.key_algorithm,
dm.key_length
FROM sys.databases db
LEFT OUTER JOIN sys.dm_database_encryption_keys dm
ON db.database_id = dm.database_id;
```

The preceding commands return a number that represents the `encryption_state` for the EDM (0-6). For more information about the encryption state codes, see https://docs.microsoft.com/en-us/sql/relational-databases/system-dynamic-management-views/sys-dm-database-encryption-keys-transact-sql?view=sql-server-ver15.

For more information on how to enable TDE on ACM databases, see *Maintaining and Troubleshooting Avaya Control Manager*.

Note:

Keep valid backups of the following files in case of disaster:

- The certificate that encrypts the DEK
- The password to the private key of the TDE certificate
- The password to decrypt the master key in the master database
- A healthy backup of the system and user databases

For information on recovering a TDE enabled database when the user does not have various combinations of the master key password, a backup of the master database, backups of the certificate and private key, password for the private key, or password to

decrypt master database, see: https://techcommunity.microsoft.com/t5/sql-server-support-blog/recover-tde-databases-in-disaster-recover-steps-for-3-common/ba-p/2963600.

Troubleshooting TDE issues

For information on recovering a TDE enabled database when the user does not have various combinations of the master key password, a backup of the master database, backups of the certificate and private key, password for the private key, or password to decrypt master database, see https://techcommunity.microsoft.com/t5/sql-server-support-blog/recover-tde-databases-in-disaster-recover-steps-for-3-common/ba-p/2963600.

Configuring automated SQL Server Agent jobs

About this task

Use this procedure to configure automated SQL Server Agent jobs after the EDM has been deployed and configured to persist data from Context Store.

Note:

The Sample SQL Server Agent Scripts are applicable to both EDM co-resident with ACM and EDM installed alone on SQL Server(s).

Procedure

1. Log in to the SQL server which is used to take regular EDM transaction log backups and EDM full backups.

   Note:

   If using SQL Server Enterprise Edition, it is possible to use the secondary SQL server for this task.

   If using SQL Server Standard Edition, it is not possible to use the secondary SQL server for this task. In such cases, you must use the primary SQL server.

2. Log into the local instance of SQL Server Management Studio.
3. In the Object Explorer pane, if SQL Server Agent is not enabled (red icon visible), right-click **SQL Server Agent** > **Start**.

   Note:

   If SQL Server Agent is required to start up automatically on reboot of the SQL Server, ensure that the Start Mode for the SQL Server Agent service is set to **Automatic** in **SQL Server Configuration Manager** > **SQL Server Services**.

4. Right-click **Jobs** > **New Job**.
5. On the General page, enter a name for the Job.

   For example, EDMTransactionLogBackup

6. On the Steps page, do the following:
   a. Click **New** and enter a name for the step. For example, `Backup EDM`.

b. Copy and paste a sample script into the command window.

   For more information on how to customize the Sample SQL Server Agent script, see the *ReadMe* file included in the SampleSQLServerAgentScripts.zip file.

c. Click **OK**.

7. On the Schedules page, click **New** and enter a name for the schedule.

   For example, Hourly EDM Transaction Log Backup.

8. In the Frequency section, in the **Occurs** field, select the appropriate option. For example, **Daily**.

9. In the **Daily Frequency** section, select either **Occurs once at:** or **Occurs every:**, enter appropriate value(s), and click **OK**.

   For example, for an hourly transaction log backup, select **Occurs every:** and enter `1 hour`.

10. **(Optional)** Enable **Notifications** to get notifications with the status of the job.

11. Click **OK** to save the new job.

Chapter 11: Deploy Engagement Designer tasks and workflows

Deploying Engagement Designer tasks

Before you begin

- Download the latest versions of the following files:
  - `EngagementDesignerTasks.svar`
  - `ContextStoreTasks.svar`
  - `WATasks.svar`
  - `OceanaTasks.svar`
- In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Note:

You can skip this step, if you have already configured the DNS correctly, and the Windows desktop uses the same DNS as Avaya Breeze® platform nodes.

Procedure

1. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

2. On the Bundles tab, click **Upload**.
3. On the Choose bundle file to upload dialog box, click **Choose File**.
4. Browse to the `EngagementDesignerTasks.svar` file and click **Upload**.
5. Select the bundle and click **Deploy**.

   After the bundle is deployed successfully, ensure that:

   - The **Deployed** column for the bundle displays the value `Yes`.
   - The **Deployed Nodes** column for the bundle contains all nodes of Avaya Oceana® Cluster 1.

When you open or refresh the Designer Console of Engagement Designer, the system displays the drawers and tasks associated with the tasks bundle.

6. Repeat steps 2 to 5 to deploy Context Store, Work Assignment, and Oceana tasks.

Verifying Engagement Designer tasks

About this task

To deploy Engagement Designer workflows, you must first verify the successful installation of Engagement Designer tasks.

Procedure

1. In your web browser, enter the following URL to open the Designer Console of Engagement Designer::

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. On the Designer Console, verify the following task blocks in the navigation pane:

Task block	Installed by Tasks Bundle
Notification	EngagementDesignerTasks
Telephony Communications	EngagementDesignerTasks
Media Communications	EngagementDesignerTasks
Transformation	EngagementDesignerTasks
Oceana	OceanaTasks
Context Store	ContextStoreTasks
Work Assignment	WATasks
Events	A default task block of Engagement Designer
Gateways	A default task block of Engagement Designer
Integration	A default task block of Engagement Designer

Deploy Engagement Designer workflows

Avaya Oceana® provides the following sample Engagement Designer workflows:

Workflow	Workflow name
Voice workflow	OceanaVoiceAssistedService
Chat workflow	OceanaChatAssistedService

Table continues…

Workflow	Workflow name
Email workflow	OceanaEmailAssistedService OceanaEmailResumeService
SMS workflow	OceanaSMSAssistedService
Web Voice workflow	OceanaWebVoiceAssistedService
Social Media workflow	OceanaSocialAssistedService
Messaging workflow	OceanaMessagingAssistedService
SelfService workflow	OceanaVoiceSelfService
Video workflow	OceanaVideoAssistedService
Generic Channel workflow	OceanaGenericAssistedService
Transfer workflow for Voice	OceanaVoiceTransfer
Transfer workflow for Chat	OceanaChatTransfer
Transfer workflow for Email	OceanaEmailTransfer
Transfer workflow for SMS	OceanaSMSTransfer
Transfer workflow for Web Voice	OceanaWebVoiceTransfer
Transfer workflow for Social Media	OceanaSocialTransfer
Transfer workflow for Messaging	OceanaMessagingTransfer
Transfer workflow for Video	OceanaVideoTransfer
Transfer workflow for Generic Channel	OceanaGenericTransfer

The sample workflows work out-of-the-box. You must get the provided sample workflows working in your solution before you begin to customize them.

For instructions on how to deploy the sample workflow for each channel, see the relevant sections in this document.

Exporting multiple workflows

About this task

Use this procedure to export multiple workflows from the Engagement Designer **Admin Console**.

Procedure

1. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

2. On the Workflows tab, select the workflows that you want to export in bulk.
3. Click **Export Workflow**.

The **Admin Console** displays the Export workflow(s) dialog box listing the selected workflows.

4. Click **OK** to confirm your selection.

   The exported workflows are saved into a zipped file.

Importing multiple workflows

About this task

Use this procedure to import multiple drafted or deployed workflows into the Admin Console of Engagement Designer. After importing deployed workflows, do not deploy the workflow again.

Procedure

1. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

2. On the Workflows tab, click **Import Workflow**.
3. In the Choose work flow file to upload dialog box, click **Choose File**.
4. Navigate to your folder from where you want to import the workflows.

   You cannot import a workflow which is in .xml file format. However, you can import workflows that are in a zipped file format only. You can only import the deployed workflows that are exported from the **Workflows** tab.

5. Click **Import**.

   The **Admin Console** displays the Imported workflow(s) dialog box indicating the number of successfully imported workflows.

   On the Bundles tab, if you **Undeploy** your bundle and then import the workflows, the Engagement Designer displays an error message and the import fails.

Searching an instance in Engagement Designer Admin console

About this task

As a workflow administrator, you can view information about completed instances in the Engagement Designer Admin console. You can also review issues related to errors, successful completion with or without errors, and completed instances. With the **Error Handled** and **UCID/**

WRID options in the **Advanced Search**, you can now search for error handled instances and instances by work request ID.

By default, the Admin console retains 2000 error handled instances for 7 days. However, you can set the values in the **Number of days the user want to retain error instances** and **Maximum limit for the number of error instances to be retained** properties of the EngagementDesigner attribute. The **Treat error handled instances like successfully completed instance** property determines whether the error handled instances are treated like successfully completed instances for delete operation.

Procedure

1. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

2. On the Instances tab, click **Advanced Search**.
3. On the Advanced search on instances dialog box, select **Search On Column**.
4. Select **Active**.
5. Select **Error Handled** or **UCID/WRID** to search error handled instances or instances by work request ID.

   You can also search for instances using the available search attributes.

6. Enter `True`.
7. Click **Search**.

   For error handled instances, the Admin console displays instances in the **Error Handled** column. For UCID/WRID, the Admin console displays instances in the **UCID/WRID** column. For any search attribute, the Admin console displays instances in the respective columns.

Deleting instances in Engagement Designer Admin console

Deleting instances in the Admin console of Engagement Designer depends on the values set in the EngagementDesigner attribute.

Deleting successfully completed instances

- If the **Completed instance to be deleted** property of the EngagementDesigner attribute is set to **true**, then the completed instances are deleted immediately.
- If the **Completed instance to be deleted** property is set to **false**, the completed instances are deleted periodically based on the value set in the **Number of days the user want to retain error instances** property.

Deleting error handled instances

- If the **Treat error handled instances like successfully completed instance** property is set to **true**, then error handled instances are deleted periodically like completed instances based on the value set in the **Number of days the user want to retain error instances** property.

- If the **Treat error handled instances like successfully completed instance** is set to **false**, then error handled instances are deleted periodically like errored instances based on the values set in the following properties:
  - **Number of days the user want to retain error instances**: The error handled instances are deleted after this period.
  - **Maximum limit for the number of error instances to be retained**: If the number of error handled instances count instances are larger than this number, then older instances exceeding this number are deleted regardless of the value in the **Number of days the user want to retain error instances** property. The delete happens during the archival clean up period, set by the **Number of days the user want to retain error instances** property.

Deleting errored instances

- **Number of days the user want to retain error instances**: The errored instances are deleted after this period.
- **Maximum limit for the number of error instances to be retained**: If the number of errored instances count instances are larger than this number, then older instances exceeding this number are deleted regardless of the value in the **Number of days the user want to retain error instances** property. The delete happens during the archival clean up period, set by the **Number of days the user want to retain error instances** property.

Chapter 12: Deploy Omnichannel Windows Server

Deploy Omnichannel Windows Server overview

This section describes how to deploy an Omnichannel Windows Server.

If your solution supports High Availability (HA), you must also install a standby Omnichannel Windows Server. To install the standby server, you must perform the same installation procedures as the primary server and ensure that both servers have the same:

- Operating system version
- Windows patches
- Hard disk partitions
- Network subnet

However, you must install the standby server on a different VMware host.

Avaya recommends that you configure an HA setup for Omnichannel Windows Server. For more information about the HA setup, see Omnichannel Database HA on page 663. For information about the optimum configuration where you configure a HA setup on the local data center and a backup on a remote data center, see *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.

Important:

You must install, run, and patch the Omnichannel server software using a Windows Administrator account with full Administrator privileges. You must run the Oceana Data Management Tool using this same account.

Creating a VMware virtual machine

Procedure

Create a VMware virtual machine for the Omnichannel server. Ensure that you set the VMware virtual machine specifications as required for your deployment. For more information about server specifications, see Avaya Oceana hardware requirements on page 51.

Installing Microsoft Windows Server 2022

About this task

Install the Microsoft Windows Server 2022 (Desktop Experience) Standard or Datacenter edition and configure it to support the Omnichannel software.

Before you begin

- Ensure that you have a newly formatted server that meets the specifications for installing Microsoft Windows Server 2022 (Desktop Experience) Standard or Datacenter edition.
- Ensure that you have a DVD of the Microsoft Windows Server 2022 (Desktop Experience) Standard or Datacenter edition.
- Ensure that you have a product key for Microsoft Windows Server 2022 (Desktop Experience) Standard or Datacenter edition.
- Obtain the IP addresses for the Omnichannel subnet.

Procedure

1. Insert the Microsoft Windows Server 2022 (Desktop Experience) DVD into the DVD drive.
2. Turn on the power to the server.

   The server begins to boot up.
3. On the Windows Setup screen, in the **Language to install** field, select the appropriate language.
4. In **Time and currency format**, select the appropriate time and currency.
5. In **Keyboard or input method**, select an appropriate value.
6. Click **Next**.
7. Click **Install now**.
8. Select a version of Windows Server 2022 that includes a Desktop Experience.
9. Click **Next**.
10. On the Enter the product key to activate Windows screen, enter the operating system product key.
11. Click **Next**.
12. On the Applicable notices and license terms screen, read the notices and terms, and select **I accept the license terms**.
13. Click **Next**.
14. Select **Custom: Install Windows only (advanced)** for a new installation.
15. Click **Next**.
16. Select the disk partition where you want to install Windows Server 2022 (Desktop Experience) Standard or Datacenter edition.

Important:

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

17. Click **Next**.

    The installation proceeds and automatically restarts the server several times.

18. After completing the installation, log on to the server as an administrator by entering and confirming the administrator password.
19. Select **Set time zone** and complete the information as required for your system.
20. Select **Configure Networking** and complete the information for your Network Interface Card (NIC) with the server IP address.
21. Select **Provide computer name and domain** and complete the information for your server name and network settings.
22. Change the DVD drive letter to **E:** and ensure that the correct drive letters are free for the Omnichannel application and database hard disk drives and partitions.
23. Configure the hard disk drives and partitions for this server using the Windows Server 2022 (Desktop Experience) Standard or Datacenter edition.
24. Install other required drivers for your hardware configuration.

Installing the most recent supported operating system service packs

About this task

Avaya recommends installing Operating System Service Packs and Security Hotfixes in a controlled manner during the initial deployment. Installing subsequent Operating System updates must be carefully controlled and tested within a planned Maintenance Window.

Avaya tests the Omnichannel software on Windows servers using the most recent updates to the operating system. However, as Microsoft publishes new Operating System updates monthly, some precautions are necessary to ensure that updates published after the Omnichannel software releasedo not break Oceana features or functions.

Note:

- Install and test the Operating System updates in the Preproduction solution before installing them in the Production solution.
- In Omnichannel Database HA solutions, to minimize the number of server switchovers needed, perform this procedure first on the current backup server and then on the other Omnichannel server.

Before you begin

- Install and configure Microsoft Windows Server 2019 (Desktop Experience) Standard or Datacenter edition on your server.
- Disable Operating System Automatic updates.

Procedure

1. Review the published Microsoft updates to determine the most recent patches or service packs for the Windows Server 2019 (Desktop Experience) Standard or Datacenter OS.
2. Download the appropriate Windows Server 2019 updates for the Omnichannel software installed on this server.
3. Plan a Maintenance Window.
    a. At the start of the Maintenance Window, take a VMware snapshot of the Omnichannel server.
    b. Install the most recent Windows Server 2019 Operating System Updates, following the Microsoft Installation instructions.
    c. Some OS updates and hotfixes might require a reboot of the Omnichannel server.
    d. Do a Sanity test of Oceana to ensure the OS updates and hotfixes have not broken any Oceana feature and function.
    e. If the OS updates and hotfixes break any feature and function, revert to the VM snapshot taken before applying the updates and notify Avaya of the issue.
    f. If the OS updates and hotfixes do not break any feature or function, delete the VM snapshot.
    g. For Omnichannel Database HA solutions, ensure Cache DB Mirroring is working before returning the solution to Production.
4. End the Maintenance Window.

Adding the server to a domain

About this task

Before installing the Omnichannel software, you must add the server to the domain.

Before you begin

- Ensure that the server time and domain controller time are synchronized.
- On the server, configure a preferred Domain Name System (DNS) server on the Network Interface Card (NIC).
- Ask your System Administrator to add a Domain Name System (DNS) static entry for this server.

  Each Omnichannel server in a domain requires a DNS static entry.

Procedure

1. Log on to the server.
2. Click **Start** > **Server Manager**.
3. In the navigation pane, click **Local Server**.
4. In the content pane, in the PROPERTIES section, double-click the **Domain** value.

5. In the System Properties dialog box, click the **Computer Name** tab.
6. Click **Change**.
7. In the Member of dialog box, click **Domain** to add the server to a domain.
8. In **Domain**, type the domain name.

   Provide the fully qualified domain name with the prefix and suffix.
9. Click **OK**.
10. Type the domain administrator username and password.
11. Click **OK**.
12. Restart the server when you are prompted.

Disabling unused network adapters

About this task

Use this procedure to disable all unused network adapters or Network Interface Cards (NICs) to improve network communications and prevent the erroneous configuration of unused NICs during the Omnichannel server commissioning.

Procedure

1. Log on to the server.
2. Click **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center**.
3. In the navigation pane, click **Change adapter settings**
4. Right-click the unused network adapter and click **Disable**.
5. Repeat Step 4 to disable all unused network adapters.

Enabling Microsoft Remote Desktop connection

About this task

Use this procedure to enable Microsoft Remote Desktop connection as your remote access tool. Microsoft Remote Desktop provides remote access for support on the server.

Important:

This procedure is optional. System administrators must determine whether to enable Microsoft Remote Desktop connection.

Procedure

1. Log on to the server with administrator privileges.
2. Click **Start** > **Control Panel** > **System and Security**.
3. In the System section, select **Allow remote access**.
4. Select the **Remote** tab.

5. Select **Allow remote connections to this computer**.
6. Click **Apply**.
7. Click **OK**.

Disabling Admin Approval Mode for Omnichannel Windows Server administrators

About this task

Microsoft Windows Server 2019 implements a security feature known as User Account Control (UAC). By default, this feature causes applications run by local non built-in administrators to behave as if the applications had been run by standard users. Perform this procedure to ensure that local administrators get full privileges for running applications.

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

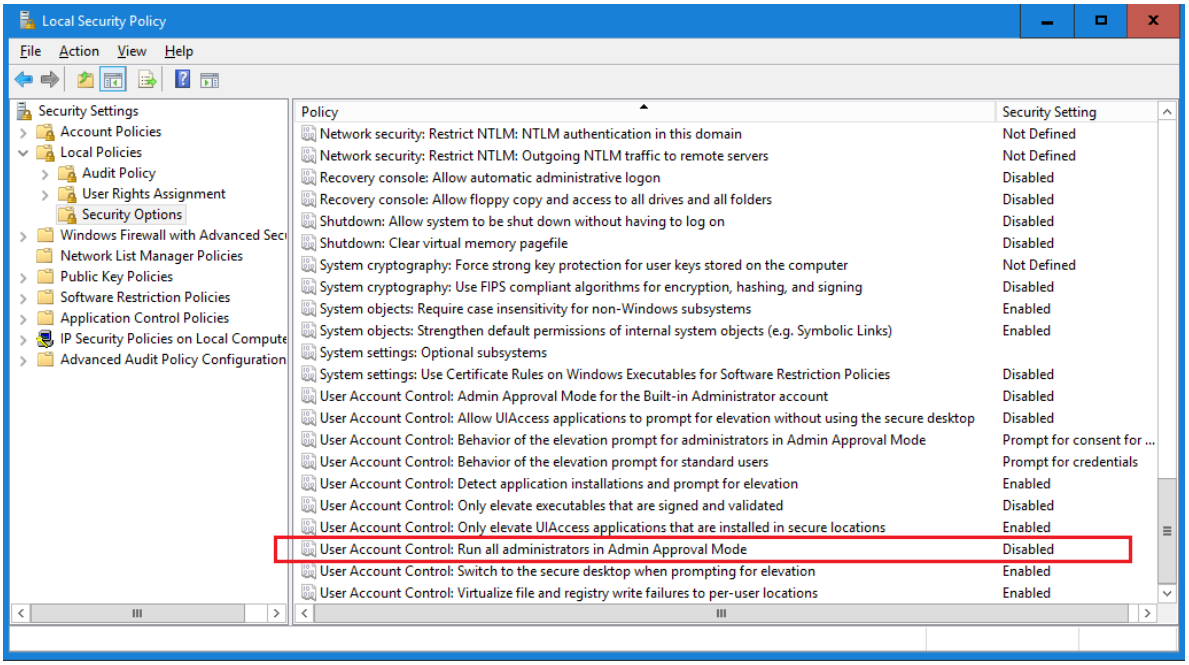
Important:

If you cannot change User Account Control settings on the Omnichannel Windows Server because your Windows user account does not have sufficient privileges, you must contact your local system administrator. Do not install Omnichannel Windows Server software until you resolve this issue.

Procedure

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

   If prompted, restart the server.



Enabling or disabling a scheduled computer maintenance in Windows 2019

About this task

Windows Server 2019 provides a centralized mechanism called Computer Maintenance, for maintaining the operating system, to perform hard disk defragmentation, and Microsoft Windows updates. Computer Maintenance can interfere with the deployment of Contact Center software, resulting in failed installations. You can turn on or off, the scheduled computer maintenance during the software installation.

Procedure

1. Open Windows Control Panel.
2. Navigate to **Troubleshooting** > **Change Settings**.
3. Before an installation Omni Channel Provider (OCP) begins, on the Change troubleshooting settings page, select **Off**.
4. Click **OK**.
5. After the installation process completes, on the Change troubleshooting settings page, select **On (Recommended)**.
6. Click **OK**.

Installing the Omnichannel server software

About this task

Use this procedure to install the Omnichannel server software.

When you install the Omnichannel server software, the installer disables SSL 3.0, TLS 1.0, and TLS 1.1 on the Omnichannel server. Therefore, you must enable them after the installation is complete.

Important:

You must install, run, and patch the Omnichannel server software using a Windows Administrator account with full Administrator privileges. You must run the Oceana Data Management Tool using this same account.

Procedure

1. Log in to the Omnichannel server.
2. Right-click the `OCEANA_x.x.xxx.iso` file and click **Mount**.
3. Double-click the `Setup.exe` file.
4. Click **Accept** to install the Microsoft .NET Framework on the Omnichannel server.

   You must install Microsoft .NET Framework 4.7.2.
5. If the installer prompts you to accept the Microsoft .NET Framework license agreement, click **Accept**.
6. If the installer prompts you to restart the server, click **Yes** and repeat Step 4.

   The installer runs the operating system and hardware checks on the server. If the software installation fails, you must review the logs of System Readiness Check and resolve the problems that caused the failure. You can ignore the warnings that do not impact the operation of the contact center.

   The installer displays the Omnichannel Server Select Destination Drive screen.
7. In the **Product Install Drive** field, select the hard disk partition for the main application.
8. In the **Journal Database Drive** field, select the hard disk partition for the Journal database.
9. In the **Oceana Database Drive** field, select the hard disk partition for the Omnichannel database.
10. Click **Next**.
11. On the AVAYA GLOBAL SOFTWARE LICENSE TERMS screen, click **I ACCEPT THE LICENSE TERMS**.
12. After the installation is complete, click **Restart**.

Removing Server Message Block (SMB) from Omnichannel Server

About this task

Use this procedure to remove the Server Message Block (SMB) from Omnichannel Server.

Important:

- Server Message Block v1 & v2 have significant security vulnerabilities. Avaya recommends removing them.

Procedure

1. Log in to the Omnichannel Microsoft Windows Server 2019 server.
2. On the Server Manager Dashboard, select **Manage** > **Remove roles and features**.
3. On the Before you begin page if shown, click **Next**.
4. On the Select destination server page under **Server Pool**, select the server and click **Next**.
5. On the Remove server roles page, click **Next**.
6. On the Remove features page, clear the check box for **SMB 1.0/CIFS File Sharing Support** and click **Next**.
7. On the Confirm removal selections page, confirm that the feature is listed and select **Remove**.

Removing the IIS Default page

About this task

Use this procedure to remove the IIS Default page.

Important:

The IIS Default page has significant security vulnerabilities. Avaya recommends removing it.

Procedure

1. Log in to the Omnichannel Microsoft Windows Server 2019 server.
2. Click **Start** > **Windows Administrative Tools** > **Internet Information Services (IIS) Manager.**
3. Click the server name.
4. Double click **Default Document**.
5. On the right of the screen, click **Disable**.

Manage Security and TLS certificates

This section describes how to configure secure Chat and Omnichannel Windows Server. This section also describes how to securely create or request security certificates. Secure encrypted communications require a TLS certificate.

To use the certificates so that a browser can securely access a service, see how to install the root certificate. To add a server and certificate to System Manager, see how to create end entities and subsequent sections.

There are two ways to create a certificate:

- Create a p12 keystore for the server.
- Create a private key and Certificate Signing Request using OpenSSL (recommended).

Downloading the root certificate from Avaya Aura® System Manager

About this task

A default root certificate can be generated when Avaya Aura® System Manager is being installed. This section covers how to download and install the default root certificate or any other CA certificate that is loaded in System Manager. System Manager uses a third-party open source application called Enterprise Java Beans Certificate Authority (EJBCA). EJBCA acts as a Certificate Authority for certificate management.

For more information about System Manager, generating the default certificate, and working with certificates, see *Administering Avaya Aura® System Manager*.

Note:

- If you are using System Manager as Certificate Authority (CA) for Avaya Oceana® and Avaya Aura® applications, then the certificate used in the following instructions is the System Manager Root Certificate or CA Certificate.
- If you are using an enterprise or third-party Certificate Authority (CA) and not System Manager as the CA, then the certificate used in the following instructions is the root certificate of the enterprise or third-party CA. The root certificate for the enterprise or third-party CA is obtained from the enterprise or third-party CA and not from System Manager. For more information, consult the enterprise or third-party CA administrator.

Procedure

1. Log in to Avaya Aura® System Manager using your credentials.
2. Navigate to **Services** > **Security** > **Certificates** > **Authority**.
3. On the EJBCA Administration page, on the left pane, click **Public Web**.

   The system displays `Welcome to the public EJBCA pages.`
4. On the public EJBCA screen, on the left pane, in the **Retrieve** section, click **Fetch CA certificates**.
5. To download the certificate, choose any of the following:
   - Download as PEM - To download the certificate `.pem` file.
   - Download to Firefox - To install the certificate in the certificate manager of Firefox browser.
   - Download to Internet Explorer - To install the certificate on a Windows machine containing Microsoft Internet Explorer, Edge, and Chrome browsers.

Installing the root certificate

Before you begin

Download the root certificate.

Procedure

1. Navigate to root certificate location.
2. Right-click the certificate file and click **Install Certificate**.
3. On the Certificate Import Wizard, select **Local Machine** and click **Next**.
4. Select **Place all certificates in the following store** and click **Browse**.
5. Click **Trusted Root Certification Authorities**.
6. Click **OK**.
7. Click **Next**.
8. Click **Finish**.

Verifying to ensure the browser accepts the certificate

Before you begin

Ensure that the certificate is installed.

Procedure

1. Open the Windows hosts file in a text editor such as Notepad.
2. Right-click the text editor and click **Run as Administrator**.
3. Add the host names of the lab to your hosts file in the following format:

   <IP Address> FQDN
4. In your web browser, browse to a known service URL.

   Microsoft Internet Explorer tries to download the JSON response. However, Firefox and Chrome display the result.
5. In your web browser, browse to the chat URL:

   `https://<AvayaOceanaCluster3_Hostname>/services/customer/chat`

   An HTTP 405 error indicates that the request used the wrong method. The error also indicates that the browser has accepted the certificate and can open a WebSocket.

Certificate Profiles

Certificate Profiles determine the specific behavior of a certificate type, mainly through particular extensions. There are default certificate profiles available. This document assumes that you use the built-in ID_CLIENT_SERVER profile.

Creating end entities

About this task

End entities are users such as browsers, email clients, or servers. This section assumes that you want to add a server using the default INBOUND_OUTBOUND_TLS end entity profile. This profile is used for client and server authentication.

You must use this procedure if you use System Manager Certificate Authority (CA).

Procedure

1. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
2. In the navigation pane, in the RA Functions section, click **Add End Entity**.
3. In the **End Entity Profile** field, select `INBOUND_OUTBOUND_TLS`.
4. In the **Username** field, enter a user name.

   Ensure that you make a note of the user name. This user name is required when creating a certificate for this server.
5. In the **Password (or Enrollment Code)** field, enter a password.

   Ensure that you make a note of the password. This password is required when creating a certificate for this server.
6. In the **Confirm Password** field, re-enter the password.
7. In the **CN, Common name** field, enter the FQDN of the Omnichannel Windows server.
8. In the **DNS Name** field, enter the server FQDN.
9. In the **IP Address** field, enter the server IP address.
10. In the **Main certificate data** section, do the following:
    a. In the **Certificate Profile** field, select the appropriate certificate profile.
    b. In the **CA** field, select the appropriate CA.
    c. In the **Token** field, select **User Generated**.
11. Click **Add**.

Creating a Certificate Signing Request

About this task

A Certificate Signing Request (CSR) is used by a server to apply for an SSL/TLS certificate. Use this procedure to create a CSR using OpenSSL.

Note:

This procedure is a worked example that describes how to create a CSR using OpenSSL. You can also create a CSR by using other options.

Procedure

1. Log on to the Microsoft Windows Server 2019 (Desktop Experience) for Omnichannel Provider (OCP).
2. Download a Windows version of OpenSSL to this Microsoft Windows Server 2019 (Desktop Experience).
3. Generate a private key using the OpenSSL genpkey command.
4. Generate a CSR for this key using the OpenSSL req command.

   Sample CSR generation:

```
# generate the private key. This creates a 2048-bit RSA key, which is encrypted
using AES-256.

# The -pass parameter passes in "testing" as the password - consult the OpenSSL
documentation for other ways of doing this.

openssl genpkey -algorithm RSA -out mmdev1.key -aes-256-cbc -pass pass:testing
-pkeyopt rsa_keygen_bits:2048

# generate the CSR.
# The value of the -passin parameter MUST match the password for the private key.
# This generates a CSR called mmdev1.csr.

openssl req -new -in mmdev1.key -key mmdev1.key -passin pass:testing -out
mmdev1.csr
```

Creating a certificate from a CSR

Procedure

1. Connect to Omnichannel Windows Server.
2. Open the CSR file in a text editor such as Notepad.
3. In your web browser, enter the following URL for the System Manager installation of EJBCA:

   `https://<SMGR FQDN>/ejbca`

4. In the navigation pane, in Enroll section, click **Create Certificate from CSR**.
5. In the **Username** field, enter the user name.
6. In the **Enrollment code** field, enter the password or enrollment code.
7. From the text editor, copy the content of the CSR file that is present between the `---BEGIN CERTIFICATE REQUEST---` and `---END CERTIFICATE REQUEST---` lines.
8. Paste the copied content into the list.
9. Click **OK**.

Creating a keystore to identify users

Procedure

1. Ensure that you have an end entity configured with a username and password or enrollment code.

   In this example, the username is mmdev1.

2. In your web browser, enter the following URL for the System Manager installation of EJBCA:

   `https://<SMGR FQDN>/ejbca`

3. In the navigation pane, in the Enroll section, click **Create Keystore**.
4. In the **Username** field, enter your user name.

   For example, mmdev1

5. In the **Password** field, enter the password or enrollment code.
6. Click **OK**.
7. Follow the on-screen instructions to download and install the keystore as a certificate.

   You can install it in the same manner as a root certificate. However, you must add it as a personal certificate rather than as a trusted root authority certificate.

Configuring the security setting in Firefox

About this task

Use this procedure to configure the security setting in Firefox to use the certificate manager of the operating system.

Procedure

1. In the Firefox browser address bar, enter the following text:

   `about:config`

2. On the Warning page, click **Accept the Risk and Continue**.
3. In the **Search** field, type `security.enterprise_roots`.
4. Set the value of the **security.enterprise_roots.enabled** row to `true`.

Configuring Caché to use TLS

Omnichannel Windows Server contains a Caché database. This section describes how to configure the database to use TLS connectivity.

Generating a private key and certificate

Procedure

1. Add an End Entity for the Windows server through System Manager.

2. Generate a private key for Caché using the version of OpenSSL that you downloaded and installed earlier.
3. Generate a Certificate Signing Request (CSR) for this private key.
4. Create a certificate from CSR through System Manager.
5. Copy the certificate into a folder onto the Windows server. For example, `C:/CacheCerts`.
6. Move the private key into the same folder.

Configuring Caché Superserver to use TLS

About this task

Use this procedure to configure Caché Superserver to use TLS on Data Center 1 and Data Center 2.

Important:

The system does not retain this configuration on upgrade. Therefore, you must do this configuration after every upgrade.

Procedure

1. Navigate to `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
2. Run the `OceanaDataManagementTool.exe` configuration file.
3. Go to **Configuration** and enter **SSL info** details.
4. In the **File containing this configuration's X.509 certificate** field, browse and select **Server Certificate**.
5. In the **File containing associated private key** field, browse and select the key.
6. In the **Private key password** field, enter the new password.
7. Click **Save**.
8. In your web browser, enter the following URL to open **Caché Management Portal**:

   `http://<ServerIP>:57772/csp/sys/UtilHome.csp`

   <ServerIP> is the IP address of the server where you installed Omnichannel Database.
9. On the **Caché Management Portal** login page, do the following:
   a. In the **User Name** field, type `_admin`.
   b. In the **Password** field, type `Oceana16`.
   c. Click **LOGIN**.
10. Navigate to **System Administration** > **Security** > **SSL/TLS Configurations**.
11. On the **%SuperServer** row, click **Edit**.
12. Replace the **Enabled ciphersuites** text with the following:

    `TLSv1:TLSv1.1:TLSv1.2:!ADH:!LOW:!EXP:@STRENGTH`

Configuring Java clients to use TLS

Procedure

In the following services, set the **Secure Connections to Omnichannel Database** attribute to `true` to enable a secure connection:

- AgentControllerService
- AutomationController
- CustomerControllerService
- EmailService
- MessagingService
- OCPDataServices
- ORCRestService
- OceanaDataViewer

Important:

- For any of these services, if you do not see the **Secure Connections to Omnichannel Database** attribute in System Manager, then it specifies that the service does not currently support a secure connection to Omnichannel Database.
- The JDBC connection to Omnichannel Database remains unaffected even if Avaya Oceana® Cluster 3 is configured to only support secure connections.
- Irrespective of the TLS version set on Avaya Oceana® Cluster 3, all services use TLS 1.2 to access Omnichannel Database.

Changing the Omnichannel Database password

About this task

Use this procedure to change the Omnichannel Database password. The procedure describes the steps to change the password for the mmJava user in Omnichannel Database. You can perform the similar steps to change the password for the _admin user.

Important:

For a High Availability pair of databases:

- Change the password in both databases
- Specify the same password for the mmJava user in both databases

  For the _admin user, you can specify different passwords in both databases.

Procedure

1. In your web browser, enter the following URL to open Caché Management Portal:

   `http://<ServerIP>:57772/csp/sys/UtilHome.csp`

   <*ServerIP*> is the IP address of the server where you installed Omnichannel Database.

2. On the Caché Management Portal login page, do the following:
   a. In the **User Name** field, type `_admin`.
   b. In the **Password** field, type `Oceana16`.
   c. Click **LOGIN**.
3. Click **System Administration** > **Security** > **Users**.
4. In the list of users, locate the mmJava user and click **Profile**.
5. On the User Profile page, click **Edit User**.
6. On the Edit User page, do the following:
   a. On the **General** tab select **Enter new password**.
   b. In the **Password** field, enter the new password.
   c. In the **Password (confirm)** field, reenter the password.

      Caution:

      You must remember the new password.
   d. Click **Save**.
7. Log on to System Manager.
8. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
9. On the Service Clusters tab, do the following:
   a. In the **Cluster** field, select Provisioning Cluster.
   b. In the **Service** field, select **OceanaConfiguration**.
10. In the Multimedia area, specify this new password in the **Password for the Omnichannel Database** attribute.

Database encryption

Database encryption overview

The Oceana Data Management utility includes the **Encryption** tab. With this tab, you can encrypt and decrypt the data stored in the following databases:

- Omnichannel database
- OFFLINE database
- CoBrowse database

The encryption of databases is important because it makes the data useless if the data is stolen. These databases are encrypted locally. Any interruption during the encryption or decryption process can leave the databases in unusable state. Therefore, you must take a backup of the databases before encrypting them. You must also ensure that you perform the encryption or decryption process during a maintenance window.

Encryption protects databases when they are not being used. Avaya Oceana® is configured to allow Cache to start automatically. The purpose of this configuration is to eliminate any human intervention for providing the encryption credentials every time the server is restarted. Encryption does not change the normal behavior of the Cache terminal or System Management Portal, where normal user credentials are required to connect, regardless of whether or not the databases are encrypted.

Creating and activating an encryption key

About this task

You must create and activate an encryption key to encrypt or decrypt databases.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Encryption**.
4. In the navigation pane, click **Data Encryption**.
5. In the **Key location** field, click **Browse**.
6. Select the directory where you want to store the encryption key.

   The default directory is `C:/Users/<current_user_name>/Documents`.
7. In the Open dialog box, in the **File name** field, do one of the following:
   - To continue with the default name `enc`, click **Open**.
   - To use a new name, type the name for the encryption key and click **Open**.
8. In the **Username** field, type a username for the encryption key.
9. In the **Password** field, type a password for the encryption key.
10. In the **Confirm Password** field, retype the password.
11. Click **Create and activate key**.

    The Oceana Data Management utility displays the following message:

    ```
    Database encryption key successfully enabled.
    ```

Activating the encryption key

About this task

Use this procedure to activate an existing encryption key so that you can use the key to encrypt or decrypt databases.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.

3. In the Oceana Data Management utility, click **Encryption**.
4. In the navigation pane, click **Data Encryption**.
5. In the **Key location** field, click **Browse**.
6. Select the directory containing the encryption key.
7. In the Open dialog box, select the encryption key and click **Open**.
8. In the **Username** field, type the user name of the encryption key.
9. In the **Password** field, type the password of the encryption key.
10. In the **Confirm Password** field, retype the password.
11. Click **Activate key**.

    The Oceana Data Management utility displays the following message:

    ```
    Database encryption key successfully enabled.
    ```

Encrypting databases

About this task

Use this procedure to encrypt the following databases:

- Omnichannel database
- OFFLINE database
- CoBrowse database

Important:

The encryption of the Omnichannel database does not necessitate you to enter encryption keys when performing database operations such as backup and restore.

Before you begin

Create and activate an encryption key.

Important:

Ensure that the key for encryption is activated. If you activate one key and try to perform the encryption using a different key, it provokes an inconsistent state of databases.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Encryption**.
4. In the navigation pane, click **Data Encryption**.
5. In the **Key location** field, click **Browse**.
6. Select the directory containing the encryption key.
7. In the Open dialog box, select the activated encryption key and click **Open**.

8. In the **Username** field, type the user name of the encryption key.
9. In the **Password** field, type the password of the encryption key.
10. In the **Confirm Password** field, retype the password.
11. Click **Encrypt Database**.

    After successful encryption, the Oceana Data Management utility displays the following message:

    ```
    All databases are encrypted
    ```

    If an error occurs in the encryption process, check the details of the error in the logs by using the `*ERROR*` prefix. An Inconsistent Database status indicates that some of the databases are encrypted and some are not.

Decrypting databases

About this task

Use this procedure to decrypt the following databases:

- Omnichannel database
- OFFLINE database
- CoBrowse database

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Encryption**.
4. In the navigation pane, click **Data Encryption**.
5. In the **Key location** field, click **Browse**.
6. Select the directory containing the encryption key.
7. In the Open dialog box, select the activated encryption key and click **Open**.
8. In the **Username** field, type the user name of the encryption key.
9. In the **Password** field, type the password of the encryption key.
10. In the **Confirm Password** field, retype the password.
11. Click **Decrypt Database**.

    After successful decryption, the Oceana Data Management utility displays the following message:

    ```
    No databases are encrypted
    ```

Checklist for encrypting or decrypting databases in a High Availability deployment

Use the following checklist to encrypt or decrypt databases in a High Availability (HA) deployment:

No.	Task	Description	✔
1	Create and activate an encryption key on the active Omnichannel Database server.	See Creating and activating an encryption key on page 214.	
2	Encrypt or decrypt databases on the active Omnichannel Database server.	See Encrypting databases on page 215 or Decrypting databases on page 216.	
3	Copy the encryption key from the active Omnichannel Database server to the standby Omnichannel Database servers.	-	
4	Activate the encryption key on the standby Omnichannel Database servers.	See Activating the encryption key on page 214.	
5	Encrypt or decrypt databases on the standby Omnichannel Database servers.	See Encrypting databases on page 215 or Decrypting databases on page 216.	

Checklist for encrypting or decrypting databases in a Disaster Recovery deployment

Use the following checklist to encrypt or decrypt databases in a Disaster Recovery (DR) deployment:

No.	Task	Description	✔
1	Create and activate an encryption key on the active Omnichannel Database server.	See Creating and activating an encryption key on page 214.	
2	Encrypt or decrypt databases on the active Omnichannel Database server.	See Encrypting databases on page 215 or Decrypting databases on page 216.	

Table continues…

No.	Task	Description	✔
3	Copy the encryption key from the active Omnichannel Database server to the backup Omnichannel Database servers.	-	
4	Activate the encryption key on the backup Omnichannel Database servers.	See Activating the encryption key on page 214.	
5	Encrypt or decrypt databases on the backup Omnichannel Database servers.	See Encrypting databases on page 215 or Decrypting databases on page 216.	

Error scenarios

The following are the error scenarios for which you must be careful during the encryption and decryption processes:

- Ensure that the key used for encryption of databases is the same key that you activated.

  You must also mount the affected databases manually, decrypt all databases, and then encrypt them in the utility.
- Ensure that you use the correct key for decryption of databases.
- Ensure that you provide correct credentials for the encryption key.
- To provide an access to the encryption functionality by SOAP, the utility creates a temporary web application `/csp/encryption`. In the end, the utility deletes the application. If the utility is stopped in an abnormal way and the web application is not deleted, ensure that you manually delete the web application.

Chapter 13: Commission Avaya Control Manager

Commission Avaya Control Manager overview

This section describes how to commission Avaya Control Manager for Avaya Oceana®.

For information on how to install and commission Avaya Control Manager, see *Installing Avaya Control Manager*.

Creating a Communication Manager user for Avaya Control Manager

About this task

Using the Communication Manager web interface, add a Communication Manager user for use by Avaya Control Manager.

Procedure

1. In your web browser, enter the following URL to open the Communication Manager web console:

   `http://<CM IP address or FQDN>`

2. Click **Administration** > **Server (Maintenance)** > **Security** > **Administrator Accounts**.
3. Select **Privileged Administrator**.
4. Click **Submit**.

   Note:

   The Communication Manager account is used when adding Communication Manager in the Avaya Control Manager config.

   The system displays the Administrator Login - Add Login screen.

5. In the **Login name** field, enter an administrator login name.

   The login name:

   - Can have alphabetic characters
   - Can have numbers

- Can have an underscore (_)
- Cannot have more than 31 characters

6. In the **Primary group** field, enter `susers` for a privileged login.
7. In the **Additional group (profile)** field, add an access profile.

   The system automatically populates the values in the Linux shell and the Home directory fields.
8. In the **Enter password** field, enter the password for the login.
9. In the **Re-enter password** field, re-enter the same password.
10. **(Optional)** To change the password after the first login, in the **Force password/key change on next login** field, select **yes**.
11. Click **Submit**.

Logging in to Avaya Control Manager

About this task

Use this procedure to log in to Avaya Control Manager to administer Avaya Oceana® resources.

Before you begin

Install SSL certificates on the Avaya Control Manager server. For more information, see Avaya Control Manager documentation.

Procedure

1. In your web browser, enter the following URL:

   `https://<acccm_hostmame>/ACCCMPortal`

   <acccm_hostname> is the host name of the Avaya Control Manager server.
2. On the Avaya Control Manager login page, perform the following steps:
   a. In the **Username** field, enter the user name.

      The initial user name is `itnv`.
   b. In the **Password** field, enter the password.

      The initial password is `itnv`.
   c. Click **Login**.

      The system prompts you to change the password.
3. Change the password.
4. Log in to Avaya Control Manager using your new credentials.
5. If you receive any errors in Internet Explorer trying to connect to the ACCCM tiles, add the Avaya Control Manager IP address to the local hosts file.

Creating a location for Avaya Oceana®

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Locations**.
2. On the Location List page, click **Add**.
3. On the Location Add page, perform the following steps:
   a. In the **Name** field, enter the name of the location.
   b. In the **Description** field, enter the description of the location.
   c. **(Optional)** In the **Auditing Location** field, leave the value as `False` or select `True` to activate audit logging for the location.
   d. Click **Save**.

Adding Communication Manager to Avaya Control Manager

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Team Engagement**.
2. On the Team Engagement page, select **Communication Manager**.
3. On the Communication Manager List page, click **Add**.
4. On the Communication Manager Edit page, do the following:
   a. In the **CM Alias Name** field, enter the alias name of Communication Manager.
   b. In the **CM IP Address** field, enter the IP address of Communication Manager.
   c. In the **CMS ACD** field, type `1`.
   d. In the **CM Username** field, enter the user name of the Privileged Administrator account that you created earlier.
   e. In the **CM Password** field, enter the password of the Privileged Administrator account that you created earlier.
   f. In the **CM Type** field, select `S8700`.
   g. In the **CM Version** field, select the supported version of Communication Manager.
   h. In the **Terminal Type** field, select `ossi3`.
   i. In the **Is Pin Required** field, select `Yes` or `No` based on your requirement.
   j. In the **Time Of Day tables number** field, type `32`.
   k. In the **Time Zone** field, select the correct time zone.
   l. Click **Save**.

   The Communication Manager List page displays the entry for the Communication Manager.

Adding Communication Manager to the location

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Locations**.
2. On the Location List page, perform the following steps:
   a. Select the location to which you want to add the Communication Manager.
   b. Click **Edit**.
3. On the Location Edit page, perform the following steps:
   a. Select the **Systems** tab.
   b. Click the **+** sign.
   c. In the **System Type** field, select **CM**.

      The **System Name** field populates the name of the newly created Communication Manager.
4. Leave the **Sync Schedule** field blank and click **Save**.
5. Click **Confirm** on the Warning message dialog box.

Adding a site, department, and team to Avaya Control Manager

About this task

Use this procedure to add a site, department, and team in an organization tree. The organizational tree manages users, sites, departments, and teams in an organizational chart.

The following are the organizational hierarchy level:

- Site
- Department
- Team

Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.
3. In the navigation pane, click **Organization tree**.
4. Click the **Expand** icon next to the **Add** button.
5. Click the **Add Organization Chart Items** icon.
6. On the Site tab, enter the information in the following fields:
   a. In the **Site Name** field, enter a name for the site.
   b. In the **Site description** field, enter a description for the site.
   c. In the **Site location** field, select the location that you created in the previous procedures.

d. Click **Save**.
e. Click **Close**.

7. In the navigation pane, click the newly created site.
8. Click the **Expand** icon next to the **Add** button.
9. Click the **Add Organization Chart Items** icon.
10. On the Department tab, enter the information in the following fields:
    a. In the **Department name** field, enter a name for the department.
    b. In the **Department site** field, select the site that you created.
    c. In the **Department description** field, enter a description for the department.
    d. Click **Save**.
    e. Click **Close**.
11. In the navigation pane, click the newly created department.
12. Click the **Expand** icon next to the **Add** button.
13. Click the **Add Organization Chart Items** button.
14. On the Team tab, enter the information in the following fields:
    a. In the **Team name** field, enter a name for the team.
    b. In the **Team department** field, select the department that you created.
    c. In the **Team description** field, enter a description for the team.
    d. Select the **Default Sync Team** check box.
    e. Click **Save**.
    f. Click **Close**.

Synchronizing Avaya Control Manager and Communication Manager

About this task

The initial synchronization process synchronizes all the information from Communication Manager in to the Avaya Control Manager database.

Important:

- Use the initial synchronization process only once. If you use this process multiple times, all data is again pulled into Avaya Control Manager database and duplicate rows appear.
- Perform this procedure on the Avaya Control Manager server.

Procedure

1. Log in to the Avaya Control Manager server.

2. On the Avaya Control Manager server, go to the `<install_path>\Avaya\Avaya Control Manager <version>\Services\ACCCM Synchronizer` folder.
3. Right-click the `NAV360_Synchronizer` file and click **Run as administrator**.
4. Click **Start** to start the synchronization process.
5. Click **Yes** on the confirmation screen.
6. Perform the following steps to verify that the resources are pulled into Avaya Control Manager:
   a. On the Avaya Control Manager webpage, click **Users**.
   b. Select the **Users** tab.
   c. In the navigation pane, select the site that you created in the previous procedure.
   d. Verify that the pulled resources are available in the right pane.

Creating a Manager Server for Unified Collaboration Administration

About this task

Unified Collaboration Administration (UCA) is an Avaya Breeze® platform service that stores the static administration data for Avaya Oceana®. Control Manager uses the UCA REST API to add agent, attribute, provider, and resource information to the Avaya Breeze® platform components in Avaya Oceana®. Therefore, you must configure the Avaya Oceana® server URL connection information for Control Manager.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. On the Oceana Server List page, click **Add**.
4. In the Primary Server tab, perform the following steps:
   a. In the **Alias** field, enter an alias name for the server.
   b. In the **API URL** field, enter the URL of the UCA ReST interface.

      For example: `https://<AvayaOceanaCluster1_FQDN>/services/UCAStoreService/uca`

      Important:

      - If the Avaya Oceana® and Avaya Analytics™ server use the same UCA server (Common setup), the **API URL** configured on both must match, including using matching address formats. For example, you must not use an IP address on one and FQDN on the other.

   c. In the **Version** field, select the Avaya Oceana® release that you are managing through Control Manager.

d. **(Optional)** Select the **Enable Authorization** option. For more information about the **Enable Authorization** option and its related parameters, see Configuring token-based access between Control Manager and Avaya Oceana, Avaya Analytics, or Avaya Workspaces for Call Center Elite on page 228.

e. In the **Deployment type** field, select any of following deployment types that shows correct type for Avaya Oceana® server that you configure. Each deployment type enforces respective guardrails for the total number of attributes assigned to all agents in the system. You can move the mouse over the field and view the guardrail details for the selected deployment type.

5. Click **Save**.
6. Click **Test** to validate the connection details and interoperability configurations required to communicate with the system.

Note:

- After you upgrade Control Manager, the Avaya Oceana® system that you configured sets Blank as the deployment type by default. Ensure that you change the deployment type to the appropriate value.
- Avaya Oceana® 3.8.2 and later supports the 4X Large deployment type. If the 4X Large deployment type is already selected, you cannot select an Avaya Oceana® version earlier than 3.8.2 as they do not support this deployment type.
- There is a guardrail/threshold value for a maximum number of attributes you can assign to an agent. The default value is 500.

  Similarly, there is a guardrail/threshold value for maximum assigned agent attributes in the system. The threshold value depends on the Oceana system's deployment type configured in the location.

  The system restricts the attributes assignment operation if the assigned attributes exceed any of the above threshold values.
- You must assign the system to a location before administering the system through Control Manager.

The following table details the total assigned attributes threshold values:

Deployment Type	Total Assigned Agent Attributes Limit in system
Small	16500
Large	165000
Extra Large	330000
3X Large	742500
4X Large	1237500

Adding an Avaya Oceana® server to a location

About this task

Control Manager supports multiple Avaya Oceana® server instances. Each Avaya Oceana® server must be assigned to a different location in Control Manager.

Control Manager does not support sharing of Avaya Oceana® server across multiple locations. Therefore, add a single server to only one location. The Avaya Oceana® system assigned to a location is not available in the **System Name** drop-down for assigning to other locations.

Note:

Control Manager does not support the sharing of the Avaya Oceana® server across multiple locations. Therefore, add the server to only one location.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Locations**.
3. On the Location List page, perform the following steps:
   a. Select the location to add the Avaya Oceana® server.
   b. Click **Edit** or double-click the location.
4. On the Location Edit page, perform the following steps:
   a. Select the **Systems** tab.
   b. Click the **+** sign.
   c. In **System Type**, select `Avaya Oceana`.

      The **System Name** field displays the name of the newly created Manager Server.
5. Leave **Sync Schedule** blank and click **Save**.
6. Click **Confirm** on the Warning message dialog box.

Synchronizing Avaya Oceana® Server

About this task

After you complete installing the latest version of Control Manager or upgrade from the previous versions of Control Manager, you must synchronize Avaya Oceana® data into the Control Manager system.

Avaya Oceana® data can include:

- Workflow Assignment Objects: Categories, Attributes, and Services
- Work Assignment Properties: Service Excluded, Strategy, Proficiency, and Multiplicity
- User Attributes

- User Prototype
- User Profile Prototype
- Providers
- User Details
- UserGroups Types
- System properties

Procedure

1. Log on to the Windows operating system.
2. Navigate to the `<InstallPath>\Services\ACCCM Synchronizer` folder.
3. To start the synchronizer, right-click the `NAV360_Synchronizer.exe` file and select **Run**.

   Control Manager displays the Synchronizer screen.
4. Select **Oceana** in the **Type Sync** field.
5. Select the options in the **Objects to synchronize** section.
6. Select the **Locations to synchronize**.
7. Click **Start**.

   Note:

   If you have enabled Avaya Oceana® Disaster Recovery support, ensure that the primary Avaya Oceana® server is in an **Active** state before you synchronize data from Avaya Oceana®.

   If data already exists in the Control Manager database for the selected objects and locations that you synchronize, you will overwrite this data when you run subsequent sync operations. The synchronizer application displays a warning message with this information when you run a sync operation.

Adding connectors to Provisioning Server

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Services** > **Provisioning**.
2. On the Provisioning Services List page, perform the following steps:
   a. Select the Provisioning Server.
   b. Click **Edit**, or double-click the location.
3. On the Provisioning Services Edit page, perform the following steps:
   a. Select the **Location** tab.

b. Move the required location from the **Available locations** list to the **Selected locations** list.

c. Select the **Connectors** tab.

d. Enable or disable a connector by selecting **Yes** or **No** from the drop-down list.

e. Click **Save**.

Configuring token-based access between Control Manager and Avaya Oceana®, Avaya Analytics™, or Avaya Workspaces for Call Center Elite

Complete the procedures in this section to configure token-based access between Control Manager and Avaya Oceana®, Avaya Analytics™, or Avaya Workspaces for Call Center Elite.

About this task

Token enforcement requires that the REST API client first requests a token from the Avaya Breeze® platform Authorization Service. The client sends a digitally-signed token request to the service with a list of objects to access. If the Authorization Service recognizes the client and grants access to the resource, the service returns a signed token. The client uses this token in subsequent calls to the target REST service. The service endpoint checks the validity of the token on each request and processes a request only if the token is valid.

For token-based access to work, perform the following procedures:

- Create a trust between Control Manager and Authorization service by:
  1. Obtaining the System Manager root certificate.
  2. Installing the root certificates from the Avaya Breeze® platform cluster to host the Authorization service as a trusted root certificate authority on the Control Manager application server.
  3. Updating the Avaya Oceana® UCA server URL.
- Export the Control Manager public certificate.
- Install the Control Manager public certificates in the Authorization clients list so that the Authorization service recognizes token requests from the Control Manager server.
- Assign Grants to the Control Manager client to define the list of resources that can access the Control Manager server.
- Enable token-based access in Control Manager.
- Configure the Avaya Breeze® platform assigned Client ID for Control Manager in Control Manager.

Note:

For the Multiple HA setup, you must repeat the same procedure on each application server.

Before you begin

- Ensure that you installed the signed certificates on the Control Manager deployment. For information about certificate installation, see *Installing Avaya Control Manager* and *Upgrading Avaya Control Manager* guides.

- On the System Manager web console, click **Services** > **Inventory** > **Manage Elements** and identify the root CA that was used to sign the certificate for one of the nodes in the Avaya Breeze® platform cluster that hosts the Authorization service.

Downloading the root certificate from Avaya Aura® System Manager

About this task

A default root certificate can be generated when Avaya Aura® System Manager is being installed. This section covers how to download and install the default root certificate or any other CA certificate that is loaded in System Manager. System Manager uses a third-party open source application called Enterprise Java Beans Certificate Authority (EJBCA). EJBCA acts as a Certificate Authority for certificate management.

For more information about System Manager, generating the default certificate, and working with certificates, see *Administering Avaya Aura® System Manager*.

Note:

- If you are using System Manager as Certificate Authority (CA) for Avaya Oceana® and Avaya Aura® applications, then the certificate used in the following instructions is the System Manager Root Certificate or CA Certificate.
- If you are using an enterprise or third-party Certificate Authority (CA) and not System Manager as the CA, then the certificate used in the following instructions is the root certificate of the enterprise or third-party CA. The root certificate for the enterprise or third-party CA is obtained from the enterprise or third-party CA and not from System Manager. For more information, consult the enterprise or third-party CA administrator.

Procedure

1. Log in to Avaya Aura® System Manager using your credentials.
2. Navigate to **Services** > **Security** > **Certificates** > **Authority**.
3. On the EJBCA Administration page, on the left pane, click **Public Web**.

   The system displays `Welcome to the public EJBCA pages.`
4. On the public EJBCA screen, on the left pane, in the **Retrieve** section, click **Fetch CA certificates**.
5. To download the certificate, choose any of the following:
   - Download as PEM - To download the certificate `.pem` file.
   - Download to Firefox - To install the certificate in the certificate manager of Firefox browser.
   - Download to Internet Explorer - To install the certificate on a Windows machine containing Microsoft Internet Explorer, Edge, and Chrome browsers.

Adding the System Manager root certificate to the Trusted Root Certification Authorities list

Procedure

1. Log on to the server where Avaya Control Manager is installed.

2. Click **Start** > **Run**.
3. In the Run dialog box, type `mmc` and click **OK**.
4. On the Console screen, click **File** > **Add/Remove Snap-in**.
5. On the Add or Remove Snap-ins screen, select **Certificates** from the **Available snap-ins** list and click **Add >**.
6. On the Certificates Snap-in screen, select **Computer account** and click **Next**.
7. On the Select Computer screen, select **Local computer** and click **Finish**.
8. Click **OK**.
9. On the Console screen, in the navigation pane, expand **Certificates**.
10. Right-click **Trusted Root Certification Authorities** and click **All Tasks** > **Import**.
11. On the Certificate Import Wizard screen, perform the following steps:
    a. Click **Next**.
    b. Browse to the location where you downloaded the System Manager root certificate.

       For more information about obtaining the root certificate from System Manager, see *Downloading the root certificate from System Manager* in this chapter.
    c. Select the certificate and click **Next**.
    d. Select **Place all certificates in the following store** and click **Next**.
    e. Click **Browse** and select **Trusted Root Certification Authorities**.
    f. Click **Next**.
    g. Click **Finish**.

Updating the Avaya Oceana® server URL

About this task

After the root certificate is installed on the Avaya Control Manager server, the Avaya Oceana® server URL that is used for the communication between Control Manager and the Avaya Oceana® server URL can be updated to specify HTTPS usage.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. Either double-click the administered Avaya Oceana® server, or select the administered Avaya Oceana® server and click **Edit**.
4. On the Avaya Oceana Server Edit page, update **API URL** to point to the HTTPS endpoint.

   Important:

   - If the Avaya Oceana® and Avaya Analytics™ server use the same UCA server (Common setup), the **API URL** configured on both must match, including using

matching address formats. For example, you must not use an IP address on one and FQDN on the other.

Exporting Control Manager certificate

Procedure

1. Log on to the server where Avaya Control Manager is installed.
2. Click **Start** > **Run**.
3. In the Run dialog box, type `mmc` and click **OK**.
4. On the Console screen, click **File** > **Add/Remove Snap-in**.
5. On the Add or Remove Snap-ins screen, select **Certificates** from the **Available snap-ins** list and click **Add**.
6. On the Certificates Snap-in screen, select **Computer account** and click **Next**.
7. On the Select Computer screen, select **Local computer** and click **Finish**.
8. Click **OK**.
9. On the Console screen, in the navigation pane, expand **Personal** > **Certificates**.
10. Select the Control Manager certificate that you want to export for authorization.

    See Adding the Authorization client to System Manager on page 231.
11. Right-click on the Control Manager certificate and then select **All Tasks** > **Export**.
12. Click **Next** and then click **Finish**.
13. Open the exported certificate and extract the thumbprint.
14. Open the `Nav360Config.xml` file and locate the following line:

    ```
    <certificates> <stores> <store id="Personal"> <thumbprint id="identity"> </
    thumbprint> </store> </stores>
    ```
15. Insert the thumb print of the exported certificate.

    For example:

    ```
    <certificates> <stores> <store id="Personal"> <thumbprint id="identity">
    1d8294aa33a3b6de8fb49b298c946c50b3ec0eb1</thumbprint> </store> </stores>
    ```
16. Save and close the `Nav360Config.xml` file.
17. Restart the Control Manager server.

Adding the Authorization client to System Manager

Procedure

1. Log on to System Manager.
2. Navigate to **Elements** > **Avaya Breeze®** > **Configuration** > **Authorization**.
3. On the Authorization Configuration page, click **New**.

4. On the New External Authorization Client page, do the following:
   a. In the **Name** field, enter the name of the Control Manager server.
   b. In the **Certificate** field, browse to the Control Manager certificate.

      See Exporting Control Manager certificate on page 231.
   c. Click **Commit**.

      The new client now appears in the list of authorized clients.

Adding Grants to the Control Manager application

Procedure

1. Log on to System Manager.
2. Navigate to **Elements** > **Avaya Breeze®** > **Configuration** > **Authorization**.
3. On the Authorization Configuration page, select the Control Manager client that you added to System Manager.
4. Click **Edit Grants**.
5. On the Edit Grants for Authorization Client page, click **New**.
6. On the Create Grant for Authorization Client page, do the following:
   a. In the **Resource Name** field, select **UCAStoreService**.
   b. In the **Resource Cluster** field, select the cluster that hosts UCAStoreService.
   c. In the **Feature** field, select **ACM**.
   d. In the **Values** field, select the **delete**, **read**, and **write** check boxes.
7. Click **Commit**.
8. On the Edit Grants for Authorization Client page, click **New**.
9. On the Create Grant for Authorization Client page, do the following:
   a. In the **Resource Name** field, select **OCPDataServices**.
   b. In the **Resource Cluster** field, select the cluster that hosts OCPDataServices.
   c. In the **Feature** field, select **access**.
   d. In the **Values** field, select the **read** and **write** check boxes.
10. Click **Commit**.
11. Click **Done**.
12. On the Authorization Configuration page, do the following:
    a. In the **Name** column, locate the entry for the Control Manager client.
    b. In the **Id** column, locate the ID value for the Control Manager client and make a note of the ID value.

       You must use the exact ID value when configuring the Control Manager identity.

Adding Grants to Authorization Service

Procedure

1. Log on to System Manager.
2. Navigate to **Elements** > **Avaya Breeze®** > **Configuration** > **Authorization**.
3. On the Authorization Configuration page, select **AuthorizationService** from the list of clients.
4. Click **Edit Grants**.
5. On the Edit Grants for Authorization Client page, click **New**.
6. On the Create Grant for Authorization Client page, do the following:
    a. In **Resource Name**, select **UCAStoreService**.
    b. In **Resource Cluster**, select the cluster that hosts UCAStoreService.
    c. In **Feature**, select **UserAuthentication**.
    d. In **Values**, select the **read** check box.
7. Click **Commit**.
8. Click **Done**.

Adding Grants to Engagement Designer

Procedure

1. Log on to System Manager.
2. Navigate to **Elements** > **Avaya Breeze®** > **Configuration** > **Authorization**.
3. On the Authorization Configuration page, select **EngagementDesigner** from the list of clients.
4. Click **Edit Grants**.
5. On the Edit Grants for Authorization Client page, click **New**.
6. On the Create Grant for Authorization Client page, do the following:
    a. In the **Resource Name** field, select **UCAStoreService**.
    b. In the **Resource Cluster** field, select the cluster that hosts UCAStoreService.
    c. In the **Feature** field, select **ED**.
    d. In the **Values** field, select the **read** check box.
7. Click **Commit**.
8. Click **Done**.

Configuring the Control Manager identity

Before you begin

Ensure that you added the ID value of the Control Manager client that you noted from the Authorization Configuration page in System Manager in the `NavConfig.xml` file.

Procedure

1. Log on to Control Manager.
2. Select one of the following servers:
   a. For Avaya Oceana®, navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
   b. For Avaya Workspaces for Call Center Elite, navigate to **Configuration** > **Customer Engagement** > **Avaya Workspaces for Elite**.
   c. For Avaya Analytics™, navigate to **Configuration** > **Customer Engagement** > **Avaya Analytics**.
3. Select the respective server and then click **Edit**.
4. On the Connection Details tab, do the following:
   a. Select the **Enable Authorization** check box.
   b. In **Authorization Service URL**, enter the following value:

      `https://`*`BreezeClusterFQDN`*`:9443/services/AuthorizationService/token`

      BreezeClusterFQDN is the FQDN of the cluster that hosts the Authorization service.
   c. From **Breeze alias**, select the alias of the Breeze instance.
5. Click **Save**.

Enabling the token enforcement in UCA

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, select **UCAStoreService**.
3. In the **Advanced** group, set the **Enable Tokenless Access** attribute to **FALSE**.
4. Click **Commit**.

Personal Certificates pools for Breeze authorization

About this task

If more than one certificate is present in the Personal Certificates pool then you must specify the certificate used for authorization service in the `ACCCMUCAProxyService.exe.config` file of the UCA proxy service.

Procedure

1. Stop the UCA Proxy service.
2. Change to the directory to `<install_path>\Services\ACCCM UCA Proxy Service`
3. Open the ACCCMUCAProxyService.exe.config file.
4. Set the valid certificate thumbprint value for "BreezeAuthorizationCertificateThumbnail".

   For example:

   <add key="BreezeAuthorizationCertificateThumbnail" value="783404B433022475F588333B5A19C013021ABB1C"/>
5. Restart the UCA Proxy service.

Assigning a location to the UCA proxy server

About this task

Use this procedure if Avaya Control Manager services are segregated based on the Avaya Control Manager locations.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Services** > **UCA Proxy**.
3. Double-click the administered UCA proxy server or select the administered UCA proxy server and click **Edit**.
4. Select the **Location** tab.
5. Move the location that contains the UCA server from the **Available locations** list to the **Selected locations** list.
6. Click **Save**.

Assigning location to Application Server

About this task

Use this procedure only if Avaya Control Manager services are segregated based on Avaya Control Manager locations.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Services** > **Application Server**.

2. On the Application Server List page, perform the following steps:
    a. Select the Application Server to which you want to assign a location.
    b. Click **Edit**.
3. On the Application Server Edit page, perform the following steps:
    a. Select the **Location** tab.
    b. Move the required location from the **Available locations** list to the **Selected locations** list.

       Ensure that you move the location that contains the UCA server to the relevant Avaya Control Manager services.
    c. Click **Save**.

Assigning location to Synchronizer Service Server

About this task

Use this procedure only if Avaya Control Manager services are segregated based on Avaya Control Manager locations.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Services** > **Synchronizer**.
2. On the Synchronize Services List page, perform the following steps:
    a. Select the Synchronizer Service Server to which you want to assign a location.
    b. Click **Edit**.
3. On the Synchronize Service Edit page, perform the following steps:
    a. Select the **Location** tab.
    b. Move the required location from the **Available locations** list to the **Selected locations** list.

       Ensure that you move the location that contains the UCA server to the relevant Avaya Control Manager services.
    c. Click **Save**.

Testing the UCA REST connection

About this task

Use this procedure to test the UCA REST connection.

Note:

By default, UCA requires an authentication token to be supplied in REST request headers. For testing or troubleshooting purposes, you must enable tokenless access by setting the **Enable Tokenless Access** attribute of UCAStoreService to `TRUE`. The change is effective as soon as System Manager replicates the setting to the nodes. After you complete the testing or troubleshooting, you must reset this attribute to `FALSE`.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

Perform one of the following steps to view all Providers:

1. In your web browser, enter the following URL:

   `https://<AvayaOceanaCluster1_FQDN>/services/UCAStoreService/uca/providers`

2. Perform the following steps:

   a. Install a REST client on your Internet browser. For example, Postman application on Chrome.

   b. In the **Get** field, enter the following request URL:

      `https://<AvayaOceanaCluster1_FQDN>/services/UCAStoreService/uca/providers`

   c. Click **Send**.

   The test returns one of the following results:

   - On a newly created system, the test returns an empty JSON block ([ ]).
   - On a system with providers configured, the test returns the provider information in JSON format.

   Note:

   If the test returns an HTTP error, you must investigate and resolve the error.

Categories, Attributes, and Attribute Sets

Categories

Categories are the ways of grouping attributes. For example, the French and Spanish attributes are in the Language category. Categories are used in Property Management to configure how property values are derived for attribute sets that do not have explicit property values defined.

Attributes

Attributes are the main basis to select from available resources to be assigned work, or to select waiting work to be assigned to the newly available resources. When selecting a resource to be assigned to incoming work, the resource must have the desired attributes specified in the work request. When selecting a waiting work request for a newly available resource, the work request must have attributes that match those of the resource.

Attribute Sets

Attribute Sets are the collections of attributes. Attribute Sets can be configured for a property value, so that each property can have different values depending on which attributes are used. As an example, for the Proficiency property, a resource has high proficiency in the attribute set “English, Sales, Tablets”, low proficiency for the attribute set “English, Service, Laptops”, and low proficiency for the attribute set “Spanish”.

Users, Accounts, and Providers

Users

A user is at the highest level in the hierarchy and represents a human or an object. A user involved in Work Assignment is referred to as Work Assignment Resource.

Resource Account

A user can have one or more Resource Accounts. A Resource Account is an accessible address such as email and phone number.

Account Sources or Providers

A source is a system that hosts the Resource Accounts. For example, Communication Manager, an external Email provider, or a Chat host.

Assignment Management

The assignment of attributes and property values to users.

Property Management

The configuration of property definitions, including their category list and their default values. For example, Multiplicity Count, Proficiency, and Service Exclusion.

Channel Attributes

By default, Work Assignment contains Default Category Channel and several Default Channel attributes such as Email, Voice, and Chat. Channel Attribute is a special type of attribute that is automatically assigned to the user as Resource Accounts are created for that user. The Channel category cannot be edited. Channels can be included in attribute sets for Property Management.

Adding Attribute Categories to Avaya Control Manager

About this task

Add attribute categories to support Avaya Oceana® contact routing.

Important:

To use the sample self-service applications or workflows to validate contact routing, you must the create the Language, Service and Location categories.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™** > **Work Assignment**.

2. On the Attribute Categories tab, click **Add**.
3. On the Attribute Category tab, perform the following steps:
    a. In the **Name** field, enter the name of the category.

       For example, Language.

    b. Click **Save**.

Adding Attributes to Avaya Control Manager

About this task

Add attribute values for categories to support Avaya Oceana® contact routing.

Important:

- To use the sample self-service applications or workflows to validate contact routing, you must add values for the Language, Service, and Location categories. For the Location category, add the ‘Inhouse’ value for the sample workflows to function correctly.
- Avaya Oceana® supports viewing Customer Journey in Avaya Workspaces by topic. A topic is an identifier that you can use to correlate intent across multiple channels. For example, a customer inquiry about an insurance claim can traverse across multiple media channels. Topics can unify those interactions in the customer journey. If no topic value exists when a contact is created, a default value is provided. The default value is a combination of the Language and Service attributes, which demonstrates how to link cross-channel interactions that arrived for a topic. The default value can only be provided if Language and Service attribute values exist.

Before you begin

- Avaya Oceana® Cluster 1 should be in a running and accepting state.
- On the UI page, attributes are listed based on the logged-in user's permissions to view the Avaya Control Manager groups of Avaya Oceana® attributes. Users can only view attributes that belong to assigned attribute groups.
- Avaya Control Manager administrators and supervisors should have appropriate Avaya Control Manager groups of attributes assigned as part of groups to view permissions.
- Avaya Control Manager administrators or supervisors with no groups-to-view permission on attribute groups can view all attributes in the location without restrictions.

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™** > **Work Assignment**.
2. On the Attributes tab, click **Add**.
3. On the Attribute tab, perform the following steps:
    a. In the **Attribute Category** field, select the attribute category that you have created.

       For example, type `Language` or `Location`.

    b. In the **Attribute Value** field, enter a value for the attribute.

       For example, type `English` or `Inhouse`.

c. Click **Save**.

Adding services to Avaya Control Manager

About this task

Use this procedure to add services to Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™** > **Work Assignment**.
2. Click the **Services** tab.
3. On the Services tab, click **Add**.
4. To add a service, do the following:
   a. In the **Service Name** field, enter the name of the service.
   b. Select the **Available for Transfer** check box.

      The system automatically selects the **Agent Display** check box.

      Note:

      You must always check the **Agent Display** check box regardless of this service being a normal routed service or a transfer service.

   c. In the **After Contact Work Timer (Seconds) ***, enter a value (in seconds).

      Important:

      You can set **After Contact Work Timer (Seconds) *** at a channel or at a service basis. If this field is set to 0 and a call comes in on that service, no ACW occurs. If there value is > 0, then this value is used for ACW and it overrides the channel ACW setting. If a call comes in, that does not match a service attributes then the ACW time at a channel level is used.

   d. Move the required attributes from the **Available Attributes** list to the **Included Attributes** list.
   e. Click **Save**.

      When creating service name tags, it is recommended that you use high-level business appropriate designations and do not create a display name for every combination of attributes that can possibly be routed.

      - Recommendation 1: Omit the channel from the **Displayname** of the service. For example, instead of creating:

Displayname	Attributes
ChatSales	Department.Sales, Channel.Chat
EmailSales	Department.Sales, Channel.Email
SMSSales	Department.Sales, Channel.SMS

Create:

Displayname	Attributes
Sales	Department.Sales, Channel.Chat

- Recommendation 2: Omit system or functional attributes from the **Displayname** of the service. For example, instead of creating:

Displayname	Attributes
NoviceSupportGroup	Department.Support, AgentExpertise.Novice, Channel.Chat
RegularSupportGroup	Department.Support, AgentExpertise.Regular, Channel.Email
ExpertSupportGroup	Department.Support, AgentExpertise.Expert, Channel.Chat

Create:

Displayname	Attributes
Support	Department.Support, Channel.Chat

Configuring Properties in Avaya Control Manager

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™** > **Work Assignment**.
2. On the Properties tab, double-click the property that you want to configure.

   For example, Multiplicity.

Note:

- Attributes are listed on the basis of the logged in user's permissions to view the ACM groups of Oceana attributes. Users can view attributes that belong to assigned attribute groups.
- Avaya Control Manager administrators and supervisors must have appropriate ACM groups of attributes assigned as a part of groups to view permissions.

- Avaya Control Manager administrators and supervisors must have permission to view at least one attribute from each category. If you do not have permissions, the system does not displays categories and attribute sets.

  Administrator and supervisor must have permission to view all the selected attributes set in the attributes set if they click on already configured **Proficiency** or **Service exclude** property for editing. If you do not have permissions, the system does not displays categories and attribute sets.

  In order to correct permissions, verify the categories configured in the Work Assignment Properties, the attributes of the respective categories and the attributes of the ACM attribute groups assigned to the Administrator/Supervisor as groups to view.

- Avaya Control Manager administrators or supervisors having no groups-to-view permission on attribute groups can view all attributes in the location without any restriction.

3. On the Property tab, make the required changes in the fields and click **Save**.

   For example, to configure Multiplicity, you can change the value in the **Default Value** field.

Configuring Avaya Oceana® system properties using Control Manager

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. Double-click the administered Avaya Oceana® server, or select the administered Avaya Oceana® server and click **Edit**.
4. Click the **System Properties** tab.
5. Expand **Context Store**.
6. In the **Oceana Core Data Service Collected Digits Key** field, type `CustomerId` or `CollectedDigits`.
7. Expand **Omni Channel**.
8. In the **Omni Channel Database Server** field, enter the name of the Omnichannel Database server as administered in the HTTPS certificate installed on the Omnichannel Database server. The name not only must match the name on the certificate, but the certificate must also be trusted to avoid any certificate errors.
9. In the **Omni Channel Database Server Port Number** field, enter 443.
10. Select the **Https** check box to have a secure communication between Avaya Control Manager and your Omnichannel server.

Important:

Verify that you are able to communicate with the Omnichannel Database server through the web and without any certificate errors.

11. Expand **RONA**.
12. In the **RONA Timer(Seconds)** field, enter the RONA time for non-voice channels in seconds.

    Enter a value in the range of 26 to 100 seconds.
13. Expand **After Contact Work**.
14. Select the **Enable After Contact Work** check box.
15. Select the **Allow agent to extend ACW** check box so that the agents in the After Contact Work state can extend the time they are in After Contact Work.

    If you select this check box, interactions in After Contact Work have an **Extend** button on the work card. Agents can click the **Extend** button to extend the After Contact Work time.
16. Enter the **After Contact Work Timer** value in seconds for each channel.

    Ensure that you enter a value in the range of 0 to 9999 seconds. These fields become disabled or read-only if you uncheck the **Enable After Contact Work** check box.

    Note:

    Avaya Oceana® supports **After Contact Work Timer** per channel settings in version 3.8.1. Avaya Oceana® version 3.8 supports only one global **After Contact Work Timer** setting.

    - After Contact Work Timer for Voice (Seconds)
    - After Contact Work Timer for Email (Seconds)
    - After Contact Work Timer for Chat (Seconds)
    - After Contact Work Timer for Messaging (Seconds)
    - After Contact Work Timer for Short Messaging Service (Seconds)
    - After Contact Work Timer for Social (Seconds)
    - After Contact Work Timer for WebVoice (Seconds)
    - After Contact Work Timer for Video (Seconds)
    - After Contact Work Timer for Generic (Seconds)

    Note:

    POM or outbound channel uses Avaya Control Manager setting of Voice channel.
17. Expand **Workspaces**.

18. In the General area, administer the following options:
    a. In the **Avaya Oceana Workspaces Welcome Page URL** field, enter the URL of an optional web page that is to be presented to agents within the Avaya Workspaces welcome widget.

       This widget is displayed out-of-the-box when the agent logs in or can be added as part of another layout.

       The Welcome page does not support the `X-Frame-Options: deny` HTML tag.

    b. Enter a value in the **Workspaces time-out in seconds** field.

       Use this field to configure the time-out value for an idle agent. Time-out count starts when the browser on agent's screen is disconnected. After the time-out, the status of an agent is set to `Not Ready` with a system code as configured in **Default Not Ready code when browser disconnects** parameter. Work is not routed to an agent when in Not Ready state.

       The maximum value of time-out is 300 seconds. Until Release 3.5, the value was specified in minutes. You must re-enter this value if you are upgrading from Avaya Oceana® Release 3.5 or earlier to a later Avaya Oceana® Release.

    c. Select the **Enable mandatory disposition code for contacts** check box to mandate the disposition codes. The agents must set a disposition code to close an interaction.

    d. Select the **Outgoing Email address is blank by default** checkbox to display a blank **select a value** drop-down in the **Workspaces**.

19. In the Global Screenpop Behaviours area, do the following:
    a. Select the **Launch external Screen-pops on Agent Accept** check box to open external screen pops in new browser windows when an agent answers an interaction.

    b. Select the **Display internal Screen-pops Widget first on Agent Accept** check box to display the screenpop widget instead of the contact type widget when an agent accepts an interaction.

       Important:

       Before enabling this feature, you must configure the Screen-pop widget and verify that the widget is working correctly in Avaya Workspaces. Do not make the Screen Pop tab the default tab until you verify that the screen pops are working correctly.

20. In the Supervisor area, do the following:
    a. Select the **Notify Agent Being Observed by Supervisor** check box to notify an agent that the supervisor is monitoring the agent.

    b. Select the **Supervisor Can Modify Agent State** check box so that all supervisors can modify the state of an agent when the agent is inactive.

    c. In the **Supervisor Custom Link URL** field, enter a custom URL that you can view in Avaya Workspaces.

21. In the Widget Library area, do the following:
    a. Select the **Enable An External Widget Library** check box to enable the external widget library to include additional widgets in Avaya Workspaces.
    b. In the **Workspaces Library URL** field, enter the URL of an external widget library that you want to load in Avaya Workspaces.

    Note:

    This is a mandatory field. Do not leave it blank.
22. In the **Avaya Workforce Engagement Select (AWES)** area, select the **Avaya Workforce Engagement Select Enabled** check box to indicate that Avaya Workforce Engagement Select is available as part of the Avaya Oceana® deployment.
23. Expand **Thresholds**.
24. In the **Short Not Ready** field, enter the appropriate value in seconds.

    Enter a value of zero (0) to 999999999 seconds. This value is used to identify the number of times agents went into the Not Ready state and remained in that state for a duration less than the value configured in this field.

    Important:

    This is a mandatory field. Therefore, you must not leave this field blank.
25. Expand **System Default Codes**.
26. In the **Default Not Ready code when browser disconnects** drop-down list, select a reason code from the available reason codes.

    Important:

    Before using this option, ensure that you have created the **not ready reason** code in **Configuration** > **Avaya Oceana** > **Reason Codes** as the **User Codes** field. The drop-down contains a list of all user codes created in the UCA.
27. Expand **Transfer to User**.
28. Select the **Enable Transfer to User** check box.

    Avaya Control Manager administrators can enable or disable the Transfer to User feature. Based on this configuration, agents or supervisors can view the Transfer to User option in Avaya Workspaces.
29. Expand **Disposition Codes**.

    The following are the channels under Disposition Codes. Using Control Manager, you can make disposition codes mandatory for each of the channels below. If you do not have any disposition code configured for a channel, you cannot make it mandatory.

    - Voice
    - Email

- Social
- Generic
- Messaging
- Short Message Service
- Chat
- Outbound
- Video

30. Click **Save**.

Configuring access to Omnichannel Administration Utility

About this task

Use this procedure to configure access to Omnichannel Administration Utility so that you can open it by clicking the **Launch OC Database Administration Client** option in Avaya Control Manager.

Important:

This procedure is mandatory because it is the only supported method to open Omnichannel Administration Utility.

Before you begin

- Install and commission Avaya Control Manager.

  For more information about how to install Avaya Control Manager, see “Installing Avaya Control Manager” document. For more information on commissioning Avaya Control Manager, see the earlier topics of this chapter.
- Identify the Enterprise Certificate Authority of the Omnichannel windows server by running **`certutil.exe`** command in windows command tool.

  Note:

  The **Name** in the output is the Enterprise Certificate Authority.

Procedure

1. To install Certificate Authority administrative tool, do the following:
   a. Open the Server Manager.
   b. Navigate to **Manage** > **Add roles and features**.
   c. In the left pane, click **Server Roles**.
   d. Select **Active Directory Certificate Services**.

      The application displays Add Roles and Features Wizard window.
   e. Click **Add Features** and click **Next**.
   f. Select the required **Features** and click **Next**.

g. On the Active Directory Certificate Services (AD CS), click **Next**.
h. Select the **Role Services** and click **Next**.
i. Click **Install**.

2. Log on to Avaya Control Manager.
3. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
4. On the Avaya Oceana Server List page, do one of the following:
   - Double-click the **UCAServer** instance.
   - Select the check box for the **UCAServer** instance and click **Edit**.
5. Click the **System Properties** tab.
6. Expand **Omni Channel**.
7. In the **Omni Channel Database Server** field, enter the FQDN of the Omnichannel Windows server.
8. For a secure communication between Avaya Control Manager and your Omnichannel Windows server or host name of the VIP if using Omni Channel Cache mirroring HA, do the following:
   a. In the **Omni Channel Database Server Port Number** field, enter the port number `443`.
   b. Select the **Https** check box.
   c. Click **Save System Properties** icon.
9. Log on to the Omnichannel Database server.
10. Generate a certificate `pfx` file.
    a. Create a Certificate Signing Request (CSR) file.

       See Creating a Certificate Signing Request on page 208.

    b. Click **Start** > **Windows Administrative Tools** > **Certificate Authority**.
    c. Right-click the Certificate Authority and navigate to **All Tasks** > **Submit new request**.
    d. Open the CSR file.
    e. Expand Certificate Authority and navigate to **Pending Requests**.
    f. Right-click the certificate you submitted and select **All Tasks** > **Issue**.
    g. Navigate to **Issued Certificates**.
    h. Double-click the certificate you issued.
    i. In the **Details** tab, select Copy to file.
    j. Select **Base 64 encoded format** and export cer file with name *mmdev1.cer*.
    k. Move the `mmdev1.key` and `mmdev1.cer` file to the same location.

l. Open windows command line from the location.

m. Run the command **`openssl pkcs12 -export -out mmdev1.pfx -inkey mmdev1.key -in mmdev1.cer`**

11. Click **Start** > **Windows Administrative Tools** > **Internet Information Services (IIS) Manager**.
12. In the navigation pane, click the node for Omnichannel Database server.
13. In the content pane, in the IIS area, double-click **Server Certificates**.
14. In the **Actions** pane, click **Import**.

    The **Import Certificate** window opens.
15. In the **Certificate file (.pfx)** field, select the `pfx` file generated for the certificate file.
16. In the **Password** field, provide the password used for the private key.
17. Click **OK**.
18. To export the Certificate Authority file, do the following:
    a. In the **Windows Search** field, enter `mmc` and search.
    b. Open the `mmc.exe` application.
    c. Navigate to **File** > **Add/Remove Snap-in**.
    d. From the **Available snap-ins:** list, select `Certificates` and click **Add>** to move it to the **Selected snap-ins:** list.
    e. On the Certificates snap-in page, select `My user account`.
    f. Click **Finish**.
    g. Expand **Certificates - Current User** and then **Trusted Root Certificate Authority**, then double-click **Certificates**.
    h. Locate the Enterprise Certificate Authority and right-click on it.
    i. Go to **All Tasks** > **Export**.

       The **Certificate Export Wizard** opens.
    j. Click **Next**.
    k. Choose the required option on the **Certificate Export Wizard** and click **Next**.
    l. For Export File Format, select `Base-64 encoded X.509 (.CER)` and click **Next**.
    m. For **File to Export**, in the **File name** field, browse and select the location for file export.
    n. Click **Finish**.
19. Log on to Avaya Control Manager server.
20. Navigate to Windows hosts file located at `C:\Windows\System32\drivers\etc`.

21. Add the FQDN of the Cache server into the Windows hosts file.
22. To import the Certificate Authority as a **Trusted Root Certificate Authority** through the `mmc` application, do the following:
    a. Run the `mmc.exe` application.
    b. Navigate to **File** > **Add/Remove Snap-in**.
    c. From the **Available snap-ins:** list, select `Certificates` and click **Add>** to move the snap-ins to the **Selected snap-ins:** list.
    d. On the Certificates snap-in page, select `My user account`.
    e. Click **Finish**.
    f. Click **OK**.
    g. Expand **Certificates** and right-click **Trusted Root Certificate Authority**.
    h. Navigate to **All Tasks** > **Import**.

       The **Certificate Import Wizard** opens.
    i. Click **Next**.
    j. Choose the required option on the **Certificate Import Wizard** and click **Next**.
    k. For **File to Import**, in the **File name** field, browse and select the location for file import.
    l. Click **Finish**.
23. Log on to Avaya Control Manager .
24. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
25. On the Avaya Oceana Server List page, do one of the following:
    - Double-click the UCAServer instance.
    - Select the check box for the UCAServer instance and click **Edit**.
26. Click the **System Properties** tab.
27. Expand **Omni Channel**.
28. In the **Omni Channel Database Server** field, enter the FQDN of the Omnichannel Windows server.
29. For a non-secure communication between Avaya Control Manager and your Omnichannel Windows server, do the following:
    a. In the **Omni Channel Database Server Port Number** field, enter the port number `80`.
    b. Clear the **Https** check box.
30. Click **Save**.

Starting Omnichannel Administration Utility

About this task

Use this procedure to start Omnichannel Administration Utility from the Avaya Control Manager web interface.

Note:

If you are using Chrome or Firefox, then a ClickOnce plugin must be installed on the browser before the user launches the Oceana administration client or the OCMT.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Omnichannel Administration**.
2. Click **Launch OC Database Administration Client**.

   Avaya Control Manager starts Omnichannel Administration Utility.

Starting Oceana Customer Management Tool

About this task

Use this procedure to start Oceana Customer Management Tool from the Avaya Control Manager web interface. Oceana Customer Management Tool (OCMT) is a ClickOnce application. You must open the Oceana Customer Management Tool using the browser with which you downloaded the ClickOnce application.

Before you begin

Ensure that you have downloaded and installed the following:

- OmniDB server certificate in the trust store of the client's machine.
- Root CA certificate used to create the OmniDB certificate in the trust store of the client's machine.
- .Net framework that matches the .Net framework version of the OCMT client on the client's machine.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Omnichannel Administration**.
2. Click **Launch Customer Management Client**.

   The system starts Oceana Customer Management Tool.

Chapter 14: Configure Communication Manager and Call Center Elite for Avaya Oceana

Configure Communication Manager and Call Center Elite overview

This section provides information about how to configure Communication Manager and Call Center Elite contact center to integrate with Avaya Oceana®. The procedures described in this section must be performed in addition to the standard configuration procedures of Communication Manager and Call Center Elite.

To perform these configuration procedures, you must log in to Communication Manager using a SSH client application, such as PuTTy.

Note:

- Avaya Oceana® supports the agents in a single Hunt Group on a single Communication Manager. Avaya Oceana® maintains all resources across the enterprise in a single pool and assigns work using a single universal matching engine and attributes-driven routing. The hunt group extension is the Group Extension of the hunt group on Communication Manager that the Avaya Oceana® agents are assigned to.
- The person completing the Communication Manager configuration must be an experienced administrator. The configuration steps outlined in this section are the requirements for the Avaya Oceana® only. There are many other basic administration requirements on Communication Manager that are outside the scope of Avaya Oceana®.
- The starting digit of the calling station must be in both public and private numbering.

Configure Communication Manager resources for Avaya Oceana®

This section uses a worked example to describe a basic configuration of Communication Manager and Call Center Elite resources for Avaya Oceana® integration. You can configure these resources as required for your Avaya Oceana® solution.

Auto answer

Using Communication Manager, you can configure the auto answer setting on the agent or on the station. If enabled for the agent, this overrides the station setting. To use auto answer, the station must be in a service state of *in-service/off-hook*. When you log in to a station using a deskphone, Avaya one-X® Agent, Avaya Agent for Desktop, or Avaya Workplace Client, the station is in this

state. In an Avaya Oceana® solution, the following auto answer considerations apply when agents start work using Avaya Workspaces for Avaya Oceana®:

- Deskphone
  - If auto answer is enabled on the agent station, the agent cannot Start Work using Avaya Workspaces for Avaya Oceana®. The agent must first press the headset button or remove the deskphone from the cradle. This places the station in the *in-service/off-hook* state that is required for auto answer. Pressing the headset button again or placing the deskphone in the cradle logs the agent out of the station. If the agents wants to end the call using the deskphone without logging out of the station, a release button must be configured on the station.
  - If auto answer is enabled for the agent only, with the station setting disabled, agents can Start Work using Avaya Workspaces for Avaya Oceana®. However, the station is in the *in-service/on-hook* state after agents start work and auto answer is not active. Agents can receive calls which are not automatically answered, and when the call ends the agent is logged out of the station. To enable auto answer, agents must press the headset button or remove the deskphone from the cradle.
  - If auto answer is enabled for both the agent and the station, the agent setting overrides the station setting. However, in this scenario the agent cannot Start Work using Avaya Workspaces for Avaya Oceana®. The agent must first press the headset button or remove the deskphone from the cradle to place the station in the *in-service/off-hook* state that is required for auto answer.
- Avaya one-X® Agent
  - To use auto answer, the **CM Auto Answer Support Required** check box must be selected in Avaya one-X® Agent System Settings.
  - If auto answer is enabled on the agent station, the agent cannot Start Work using Avaya Workspaces for Avaya Oceana®. The agent must first open and expand the dialpad, and click on one of the configured lines. This places a call to the station; when the agent ends this call the station is in the *in-service/off-hook* state that is required for auto answer.
  - If auto answer is enabled for the agent only, with the station setting disabled, agents can Start Work using Avaya Workspaces for Avaya Oceana®. However, the station is in the *in-service/on-hook* state after agents start work and auto answer is not active. Agents can receive a call which is not automatically answered, and when the call ends the station is in the *in-service/off-hook* state that is required for auto answer. All subsequent calls are auto-answered.
  - If auto answer is enabled for both the agent and the station, the agent setting overrides the station setting. However, in this scenario the agent cannot Start Work using Avaya Workspaces for Avaya Oceana®. The agent must first open and expand the dialpad, and click on one of the configured lines. This places a call to the station; when the agent ends this call the station is in the *in-service/off-hook* state that is required for auto answer.
- Avaya Agent for Desktop (H.323)
  - To use auto answer, the **CM Auto Answer Support Required** check box must be selected on the **Preferences** tab in Avaya Agent Configuration.
  - If auto answer is enabled on the agent station, the agent cannot Start Work using Avaya Workspaces for Avaya Oceana®. The agent must first dial ‘0’. When the agent ends this call the station is in the *in-service/off-hook* state that is required for auto answer.

- If auto answer is enabled for the agent only, with the station setting disabled, agents can Start Work using Avaya Workspaces for Avaya Oceana®. However, the station is in the *in-service/on-hook* state after agents start work and auto answer is not active. Agents can receive a call which is not automatically answered, and when the call ends the station is in the *in-service/off-hook* state that is required for auto answer. All subsequent calls are auto-answered.
- If auto answer is enabled for both the agent and the station, the agent setting overrides the station setting. However, in this scenario the agent cannot Start Work using Avaya Workspaces for Avaya Oceana®. The agent must first dial '0'. When the agent ends this call the station is in the *in-service/off-hook* state that is required for auto answer.

• SIP clients (Avaya Workplace Client / Avaya Agent for Desktop)

  To use auto answer, the CM Auto Answer Support Required check box must be selected.

  There are no further considerations or workarounds required for auto answer when using Avaya Agent for Desktop or Avaya Workplace Client as a SIP endpoint with the Avaya Oceana® solution.

Logging on to Communication Manager

About this task

Log on to Avaya Aura® Communication Manager to configure parameters and resources for integration with Avaya Oceana®.

Procedure

1. Using an SSH client such as PuTTY, begin an SSH session using the Communication Manager IP address.
2. Click **Open**.
3. When prompted enter the user name and password for the Communication Manager.
4. Press return to ignore terminal selection and when prompted for high priority session, enter `n`.
5. To access the System Access Terminal (SAT), type `sat` and enter the same password used above.
6. When prompted, enter a preferred terminal type. For example, select the w2ktt Terminal Emulator.

Configuring System Features and Customer Options

About this task

On the Communication Manager System Parameters Features form, verify that Universal Call Identifier (UCID) is enabled. UCID is an Avaya proprietary call identifier used to help correlate call records between different systems. UCID must also be configured on the Trunk Group to Avaya Aura® Session Manager.

Procedure

1. Using an SSH client: connect to the Communication Manager System Access Terminal (SAT) interface.
2. On page 5 of the FEATURE-RELATED SYSTEM PARAMETERS screen, in the **UNIVERSAL CALL ID** field, perform the following steps:
   a. Set the **Create Universal Call ID (UCID)** field to `y`.
   b. Set the **UCID Network Node ID** field to *any unique node id number*.
3. On page 11 of the system-parameters feature screen, set the **Expert Agent Selection (EAS) Enabled?** field to `y`.
4. On page 13 of the system-parameters feature screen, set the **Send UCID to ASAI** field to `y`.
5. Save the settings.
6. Log in to Avaya Aura® Communication Manager using your credentials.

   Note:

   Ensure that this feature is licensed through Avaya WebLM licensing server.
7. Navigate to **Communication Manager Web Interface** > **Administration** > **Licensing** > **Feature Administration.**

   The Feature Administration page allows you to view and modify the settings of the optional features entitled by the license file. You can view and modify the current settings, or any of the previous settings if available, or the default settings by choosing a feature settings template.
8. In the **Select the feature settings template to display:** area, select the settings you want to view or modify.
9. Click **Display**.
10. On the Feature Administration page, verify that the **Proprietary?** field is set to `On`.

    Important:

    You must use material code 232301 to activate the Proprietary features, for example Agent States.
11. Click **Submit**.

Configuring Signaling and Trunk Groups

About this task

Using Communication Manager, you create Signaling and Trunk Groups for the trunk between Session Manager and Communication Manager. To support Work Assignment, you must configure Universal Call Identifier (UCID) on the Signaling and Trunk Groups.

Procedure

1. Run **`change signaling-group n`**.

   n is the number of the Signaling Group that you need to specify.
2. On page 1 of the SIGNALING GROUP screen, perform the following steps:
   a. Set the **Initial IP-IP Direct Media?** field to `y`.
   b. Set the **Session Establishment Timer (min)** field to `65`.
3. Save the settings.
4. Ensure that UUI is enabled on any trunks configured so that incoming calls to the Work Assignment VDN contain the Agent ID as UUI for routing the Work Assignment call to the selected agent.
5. Run **`change trunk-group n`**.

   n is the number of the Trunk Group that you need to specify.
6. On page 3 of the TRUNK FEATURES screen, perform the following steps:
   a. Set the **UUI Treatment** field to `shared`.

   Note:

   All trunks connected to Avaya Oceana® must use the shared mode and not the service provider mode.
   b. Set the **Send UCID?** field to `y`.
7. On page 4 of the SHARED UUI FEATURE PRIORITIES screen, ensure that the **ASAI**, **UCID**, and **Collected Digits** fields are not blank.
8. Save the settings.

Configuring a Route Pattern

About this task

After configuring the Signaling and Trunk Groups, you must configure a Route Pattern on Communication Manager.

Before you begin

Ensure that you identify the Route Pattern that you want to configure.

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. On page 1 of the route-pattern screen, perform the following steps:
   a. In the **Pattern Name** field, enter a name for the Route Pattern.
   b. In the **Grp No** field, enter the previously-configured Trunk Group number.

c. In the **FRL** field, enter the appropriate FRL.

3. Save the settings.

Adding a Route Pattern to the Locations table

About this task

After configuring a Route Pattern, you must add the Route Pattern to the Locations table on Communication Manager.

Before you begin

Ensure that you identify the Route Pattern that you want to add to the Locations table.

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. On page 1 of the LOCATIONS screen, in the **Proxy Sel Rte Pat** field, enter the previously-configured Route Pattern number.
3. Save the settings.

Configuring CTI-Link to Application Enablement Services

About this task

On Communication Manager, configure IP Services for the Application Enablement Services (AES) transport link and then add a CTI-Link from Communication Manager to the AES server. The other end of this CTI-Link is configured on the AES server.

Procedure

1. Run **`change node-names ip`**.
2. Make an entry for the AES host name and IP address in the respective fields and save the entry.

   The host name must match the host name on the AES server.
3. Save the settings.
4. Run **`change ip-services`**.
5. On page 1 of the IP SERVICES screen, perform the following steps:
   a. In the **Service Type** field, add `AESVCS`.
   b. In the **Enabled** field, set the value to `y`.
   c. In the **Local Node** field, enter `procr`.
   d. In the **Local Port** field, verify that 8765 is the default port.
6. On page 3 of the AE Services Administration screen, perform the following steps:
   a. In the **AE Services Server** field, enter the AES host name.

The host name must match the host name on the AES server.

b. In the **Password** field, enter a password.

The password must have 12 to 16 characters.

c. In the **Enabled** field, set the value to `y`.

7. Save the settings.
8. Run **`add cti-link next`** or **`add cti-link n`**.

n is the number of cti-link that you must use.

9. On page 1 of the CTI LINK screen, perform the following steps:
   a. In the **Extension** field, enter a valid extension.
   b. In the **Name** field, enter the name of the AES server.
   c. In the **Type** field, set the type to `ADJ-IP`.
10. On page 2 of the CTI LINK screen, in the **IC Adjunct Routing** field, set the value to `y`.
11. Save the settings.

Note:

For Avaya Oceana®, ensure that you configure two different CTI-Links for two AES servers. If your solution implements disaster recovery, you must configure four CTI-Links.

Configuring Direct Agent Calling

About this task

Communication Manager uses the Direct Agent Calling (DAC) for the Class of Restriction (COR).

DAC is required for RONA to work. With this setting enabled, you cannot make a direct call using an AgentID if the agent is in an AUX (NR) Not Ready state. When this setting is disabled, you can make a direct call using an AgentID regardless of agent state but RONA does not work correctly.

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Set the **Direct Agent Calling** field to `y`.
3. Save the settings.

Configuring a Hunt Group

About this task

Use the following procedure to configure a Hunt Group for Avaya Oceana®.

Procedure

1. Run **add hunt-group next** or **add hunt-group n**.

   n is the number of the hunt group that you need to specify. For example, 828.

2. On page 1 of the HUNT GROUP screen, perform the following steps:
   a. In the **Group Number** field, enter the number of the Hunt Group.
   b. In the **Group Name** field, enter the name of the Hunt Group. For example, use `Oceana Agent Pool`.
   c. In the **Group Extension** field, enter a value.

      This value is used for the Hunt Group as the provider value in the System Manager Source Details section of the Work Assignment agent configuration.
   d. Set the **ACD** field to `y`.
   e. Set the **Queue** field to `y`.
   f. Set the **Vector** field to `y`.
3. On page 2 of the HUNT GROUP screen, set the **Skill** field to `y`.
4. On page 3 of the HUNT GROUP screen, perform the following steps:
   a. Set the **Redirect on No Answer (rings)** field to an appropriate value.

      The value must specify the number of unanswered rings before the call is redirected.
   b. Set the **Redirect on No Answer to VDN** field to an appropriate value.

      The value must match the RONA VDN number. For example, 8284001.
5. Save the settings.

Configuring Agent Login ID using Communication Manager

About this task

Use this procedure to configure Agent position IDs.

Note:

Using Communication Manager, you can configure the auto answer setting on the agent or on the station. If enabled for the agent, this overrides the station setting. To use the station setting, ensure that the agent Auto Answer setting is set to station.

To use auto answer, the station must be in a service state of *in-service/off-hook*.

Procedure

1. Using an SSH client: connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **add agent-loginID next** or **add agent-loginID n**.

   n is based on the individual Communication Manager dial plan.

3. On page 1 of the AGENT LOGINID screen, perform the following steps:
   a. In the **Login ID** field, enter the login ID of the agent based on the individual Communication Manager dial plan.
   b. In the **Name** field, enter a representative name for the Agent.
   c. In the Auto Answer field, configure the setting to one of the following values as required for your solution: `all`, `acd`, `none`, or `station`.
4. On page 2 of the AGENT LOGINID screen, perform the following steps:
   a. In the **Direct Agent Skill** field, enter the Hunt Group number that you created.
   b. In Row 1, type the previous Hunt Group number in the **SN** field and type `1` in the **SL** field.
5. Save the settings.

Configuring Agent Phone-sets

About this task

Use this procedure to configure agent phones to support Avaya Oceana® and Call Center Elite.

Procedure

1. Configure the Avaya Oceana® agent phones to support the following Call Center Elite capabilities:
   - Call Appearance

     Avaya Oceana® requires three Call Appearance lines on each agent station.
   - Login
   - Logout
   - Auto-in / Manual-in
   - Aux Work
   - After Call (optional)
2. For each SIP User station, ensure that the **Type of 3PCC Enabled** field is set to `Avaya`.
3. For each SIP User station, ensure the **Trunk Selection** field for the phone extension is `aar`.

Chapter 15: Configure Application Enablement Services

Configure Application Enablement Services overview

This section provides information about how to configure Application Enablement Services to enable off-the-shelf and custom integration with Avaya Oceana®.

Application Enablement Services is a set of enhanced telephony APIs, protocols, and Web services. These applications support access to the call processing, media, and administrative features available in Communication Manager.

Note:

Avaya Oceana® does not support Application Enablement Services (AES) Geo Redundant High Availability (GRHA).

Configuring Communication Manager Link to Application Enablement Services

About this task

Add a switch connection so that Application Enablement Services can communicate with Communication Manager. After you add a switch connection, you must associate the switch connection name with a procr IP address. Use this procedure when you are setting up a switch connection with a Communication Manager media server that uses a procr connection to Application Enablement Services.

Add a CTI (TSAPI) link between Application Enablement Services and Communication Manager. When adding a CTI (TSAPI) link, the switch CTI link number on Application Enablement Services must match that of the IP Services Server ID for Application Enablement Services as configured in Communication Manager.

Restart the TSAPI connection between Application Enablement Services and Communication Manager. You must restart the TSAPI Service for changes to the CTI link between Application Enablement Services and Communication Manager to take effect.

Note:

If two instances of Application Enablement Services are used for HA, ensure that you repeat all steps for the other AES server. Also, ensure that you configure the other AES server with the same AES user, AES user password, and CM-Name as the first AES server.

Procedure

1. Log in to Application Enablement Services.
2. Click **Communication Manager Interface** > **Switch Connections**.
3. In the Switch Connection page, enter the name of Communication Manager in the text box and click **Add Connection**.

   The system adds the Communication Manager in the list.
4. Select the newly added Communication Manager from the list and click **Edit Connection**.
5. In the **Switch Password** and **Confirm Switch Password** fields, enter the AESVCS password.

   The password must be same as the password on the Communication Manager ip-services configuration.
6. Select the **Processor Ethernet** check box if you are using the Communication Manager procr interface.
7. Click **Apply**.
8. In the Switch Connections page, click **Edit PE/CLAN IPs**.
9. In the Edit Processor Ethernet IP page, enter the IP address of procr and click **Add/Edit Name or IP**.
10. Click **AE Services** > **TSAPI** > **TSAPI Links**.
11. Click **Add Link**.
12. In the Add TSAPI Links section, do the following:
    a. In the **Link** field, select a number which is not already configured.
    b. In the **Switch Connection** field, select the newly added switch connection.
    c. In the **Switch CTI Link Number** field, select the CTI Link number that corresponds to the CTI Link already configured on Communication Manager.
    d. In the **ASAI Link Version** field, select the highest version available.
    e. In the **Security** field, select **Both**.

       You must select **Both** because each TSAPI Link must be configured for both Encrypted and Unencrypted security types.
    f. Click **Apply Changes**.
13. Click **Security** > **Security Database** > **Tlinks**.
14. On the **Tlinks** page, verify that the CSTA and CSTA-S links are added to the system.
15. To restart TSAPI services, perform the following steps:
    a. Click **Maintenance**.
    b. Click **Service Controller**.

c. Select **TSAPI Service**.

d. Click **Restart Service**.

16. Click the **Status** > **Status and Control** > **TSAPI Service Summary**.
17. On the TSAPI Link Details page, verify that the status of the TSAPI link is `Talking`.
18. Log in to Communication Manager and run the **`status aesvcs cti-link`** command to check if the CTI links are operational and Service State is `established`.

Configuring AES certificates

AES certificate management provides support for setting up secure connections from AES to the relevant Avaya Oceana® component (CSC) using standard identify certificates and trusted CA signed certificates. Certificate installation activity is a maintenance activity and must be performed during maintenance window when there is no call traffic in the system.

In the following procedures described, a TLS based communication links is setup between AES and CSC after creating new AES CA signed certificate and importing both AES CA signed certificate and the CA root certificate into the AES trusted certificates store.

The following procedures in this section uses System Manager as the CA. However, you can also use third party Enterprise CA in the overall solution. In this way, you can perform secure certificate operations in Avaya Oceana® and AES deployment using System Manager. The same method also applies to who do not use Avaya CA's or Enterprise CA.

Creating an end entity

Procedure

1. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
2. In the navigation pane, in the RA Functions section, click **Add End Entity**.
3. In the **End Entity Profile** field, select `INBOUND_OUTBOUND_TLS`.
4. In the **Username** field, enter a user name.
5. In the **Password (or Enrollment Code)** field, enter a password.

   For each end entity, the password is mandatory for authentication of the certificate generation request.
6. In the **Confirm Password** field, re-enter the password.
7. Complete any other fields that you want in your certificate.
8. In the **CN, Common name** field, enter the FQDN of the AES server.

   The Common Name is case-sensitive.
9. In the **Certificate Profile** field, select `ID_CLIENT_SERVER`.

10. In the **CA** field, select `tmdefaultca`.
11. In the **Token** field, select `P12 file`.
12. Click **Add**.

    The system displays the `End Entity <username> added successfully` message.

Creating the server certificate

Procedure

1. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
2. In the navigation pane, click **Public Web**.

   This system displays a new browser tab.
3. In the navigation pane, in the Enroll section, click **Create Keystore**.
4. In the **Username** field, enter the user name that you specified while adding an End Entity.
5. In the **Password** field, enter the password that you specified while adding an End Entity.
6. Click **OK**.
7. On the Keystore Enrollment page, perform the following steps:
8. On the EJBCA Token Certificate Enrollment page, select the key length as 2048 and click **Enroll**.
9. Save the server certificate to a known location.

   This is the signed server certificate that you import to Application Enablement Services.

Downloading the CA certificate

Procedure

1. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
2. In the navigation pane, click **Public Web**.

   This system displays a new browser tab.
3. In the navigation pane, in the Retrieve section, click **Fetch CA certificates**.
4. Click **Download PEM chain**.
5. Save the CA certificate.

Importing the CA certificate to Application Enablement Services

Procedure

1. On the Application Enablement Services web console, click **Security** > **Certificate Management** > **CA Trusted Certificates**.

2. Click **Import** and upload the CA certificate you downloaded (PEM file).
3. Specify an alias name. For example, `caSMGR`.
4. Click **Apply**.

Importing the server certificate to Application Enablement Services

Procedure

1. On the Application Enablement Services web console, click **Security** > **Certificate Management** > **Server Certificates**.
2. Click **Import** and upload the server certificate you created.
3. Select **aeservices** from the drop-down menu.
4. Click **Apply**.
5. Enter the password specified while creating the End Entity.
6. Click **Apply**.
7. On the Server Certificate Import page, click **Apply**.

   The server certificate displays in the list on the Server Certificates page.

Creating Application Enablement Services user for Call Server Connector communication

The Call Server Connector (CSC) snap-in is a Voice-only Service Provider interface to the underlying switching infrastructure. CSC provides call control and agent control functions.

In the Avaya Oceana®, CSC communicates with Communication Manager through the Device, Media and Call Control (DMCC) interface in the Application Enablement Services. The CSC is implemented as a TSAPI application to receive Communication Manager events through Application Enablement Services. CSC uses Application Enablement Services to control and monitor Communication Manager Voice calls and resources.

Before you begin

- Create an Application Enablement Services CT user that has read-write access to User Management features in the Application Enablement Services Management console.
- Create a CT User and CTI User for the CSC snap-in.

Procedure

1. On the Application Enablement Services web console, navigate to **User Management** > **User Admin**.
2. Click **Add User**.

3. Specify a value for each of the following mandatory fields:
   - **User Id**
   - **Common Name**
   - **Surname**
   - **User Password**
   - **Confirm Password**
   - **CT User**: Select `Yes` from the drop-down menu.
4. Click **Apply**.
5. On the Application Enablement Services web console, navigate to **Security** > **Security Database**.
6. Select **CTI Users**.
7. Select **List All Users**.
8. Select the newly added user and click **Edit**.
9. Check the **Unrestricted Access** check box.
10. Click **Apply Changes**.

Verifying Application Enablement Services connection with Call Server Connector service

About this task

Use this procedure to verify that Application Enablement Services is connected to the Call Server Connector (CSC) service.

Procedure

1. On the Application Enablement Services web console, navigate to **Status** > **Status and Control**.
2. Click **DMCC Service Summary**.
3. On the Session Summary page, you see a CSC Primary and a CSC Backup entry for each configured Application Enablement Services/Communication Manager link in CSC. Each entry must have the Far-end identifier same as the IP addresses of the node it is connected to.

   If these sessions are listed, the Application Enablement Services connection to the CSC deployment is successful.

Note:

For two standalone instances of Application Enablement Services, CSC connects only to a single AES at any given time.

Chapter 16: Configure wait treatments for Voice contacts

Configure wait treatments for Voice contacts overview

This chapter uses a worked example to describe how to configure Communication Manager and Call Center Elite to provide wait treatments for calls that route to Avaya Oceana®. Some of this configuration is optional, for example the option the leave a voice mail message or to use estimated wait time (EWT) data.

The following is a list of the configuration items used in this worked example, replace these items with the values for your solution:

Configuration item	Example value	Your value
Hunt Group for Oceana agents	Hunt Group 828, ‘Oceana Agent Pool’	
Fallback announcement extension	8289981	
EWT announcement extension	8289983	
Voice mail announcement extension	8289984	
Communication Manager variables	Any letter not in use	
Ingress VDN	8284100	
Treatment VDN	8284104	
Fallback VDN	8284103	
Routing VDN	8284000	
RONA VDN	8284001	
Coverage VDN	8284105	
Transfer VDN	8284101	
Ingress Vector	1	
Treatment Vector	10	
Fallback Vector	12	
Routing Vector	2	

Table continues…

Configuration item	Example value	Your value
RONA Vector	3	
Coverage Vector	7	
Transfer Vector	5	

Before you customize your vectors, ensure that you read *Avaya Aura® Call Center Elite Feature Reference*.

Note:

You can use Avaya Control Manager Conversation Sphere to import the Avaya Oceana® vectors. The vectors are available as .acs files. Download the .acs files from the Avaya DevConnect portal at http://www.avaya.com/devconnect. You must create the Communication Manager variables before importing the vectors. For information about how to import the .acs files, refer to the Avaya Oceana® Release Notes.

Logging on to Communication Manager

About this task

Log on to Avaya Aura® Communication Manager to configure parameters and resources for integration with Avaya Oceana®.

Procedure

1. Using an SSH client such as PuTTY, begin an SSH session using the Communication Manager IP address.
2. Click **Open**.
3. When prompted enter the user name and password for the Communication Manager.
4. Press return to ignore terminal selection and when prompted for high priority session, enter `n`.
5. To access the System Access Terminal (SAT), type `sat` and enter the same password used above.
6. When prompted, enter a preferred terminal type. For example, select the w2ktt Terminal Emulator.

Configuring the prompting timeout

About this task

You can choose to configure the number of seconds that a collect digit prompt waits for a response before timing out. This value must be a number between 4 and 10. The default setting is 10 seconds.

For example, configure the number of seconds a coverage prompt waits before timing out and routing the call to the Coverage VDN.

Procedure

Use the System Access Terminal (SAT) interface to set the prompting timeout. Use the **change system-parameters features** command.

```
change system-parameters features                              Page  11 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
  EAS
         Expert Agent Selection (EAS) Enabled? y
        Minimum Agent-LoginID Password Length:
          Direct Agent Announcement Extension:                  Delay:
    Message Waiting Lamp Indicates Status For: station
                          Work Mode On Login: aux
  VECTORING
                    Converse First Data Delay: 0      Second Data Delay: 2
               Converse Signaling Tone (msec): 100          Pause (msec): 70
                    Prompting Timeout (secs): 4
                 Interflow-qpos EWT Threshold: 2
    Reverse Star/Pound Digit For Collect Step? n
          Available Agent Adjustments for BSR? n
                              BSR Tie Strategy: 1st-found
   Store VDN Name in Station's Local Call Log? n
  SERVICE OBSERVING
              Service Observing: Warning Tone? y     or Conference Tone? n
    Allowed with Exclusion: Service Observing? n                   SSC? n
            Allow Two Observers in Same Call? n
```

Creating variables using Communication Manager

About this task

Communication Manager vectors use variables to improve efficiency. Different types of variables are available to meet different types of call processing needs. Vector variables can be added to consider location, messaging, and adjunct routing vector steps. Based on the variable type, variables can use call-specific data or fixed values that are identical for all calls. In either case, an administered variable can be reused in many vectors.

Avaya Oceana® has a number of initial vectors. These vectors require the following variables:

- Routing Vector requires a variable used to collect Agent ID.
- Avaya Oceana® vectors require a Persistent variable.

  This variable is used to differentiate between the types of call ingress: (1) Elite-anchored / Adjunct Route path or (2) Web Voice and Video / Breeze-anchored path.
- Avaya Oceana® uses a variable to check if the voice channel is in service. Add this variable to ensure that if there is a routing failure at any point during a call, the call routes to the fallback VDN.

This example procedure also shows a number of further variables that you can add. These additional variables allow you to provide treatments for callers while they wait to speak to an

agent, or to fall back to Call Center Elite when Avaya Oceana® is not in service or a call routing failure occurs.

If the variables used in this example are already in use on Communication Manager, use different variables. Ensure that you use these different variables in your Avaya Oceana® vectors.

Important:

Use variables E - I if your solution uses Call Center Elite to provide Voice Self Service. Otherwise, do not configure these variables.

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Use the **`change variables`** command.
3. On page 1 of the Variables for Vectors screen, perform the following steps for variable A:
   a. In the **Description** field, enter the description of the variable A as `Adjunct Route Digits`.

      This standard description makes maintenance and troubleshooting easier.
   b. In the **Type** field, enter the value `collect`.
   c. In the **Scope** field, enter the value `L`.

      The value L specifies the Local variable.
   d. In the **Length** field, enter the value `16`.
   e. In the **Start** field, enter the value `1`.

      This value specifies the digit start position.
   f. Save the variable A.
4. On page 1 of the Variables for Vectors screen, perform the following steps for variable B:
   a. In the **Description** field, enter the description of the variable B as `Adjunct Route Flag`.

      This standard description makes maintenance and troubleshooting easier.
   b. In the **Type** field, enter the value `collect`.
   c. In the **Scope** field, enter the value `P`.

      The value P specifies the Persistent variable.
   d. In the **Length** field, enter the value `1`.
   e. In the **Start** field, enter the value `1`.

      This value specifies the digit start position.
   f. Save the variable B.

5. On page 1 of the Variables for Vectors screen, perform the following steps for variable Q:
   a. In the **Description** field, enter the description of the variable Q as `Oceana In Service`.

      This standard description makes maintenance and troubleshooting easier.
   b. In the **Type** field, enter the value `value`.
   c. In the **Scope** field, enter the value `G`.

      The value G specifies a global variable.
   d. In the **Length** field, enter the value `1`.
   e. In the **Assignment** field, enter the value `1`.
   f. In the **VAC** field, enter the value of the vector variable for the in service check. For example, enter `VV1`.

      This value enables you to use a Feature Access Code (FAC) to change the variable assignment. For example, you can use a FAC to take Avaya Oceana® out of service for voice. For information about how to take Avaya Oceana® out of service for voice, see *Maintaining and Troubleshooting Avaya Oceana®*.
   g. Save the variable Q.
6. Add any further variables as required for your solution. For example, add the variables as shown below.
7. Save the settings.

Example

```
change variables                                          Page   1 of  39
                              VARIABLES FOR VECTORS

Var Description                Type    Scope Length Start Assignment      VAC
A   Adjunct Route Digits       collect L     16     1
B   Adjunct Route Flag         collect P     1      1
C   ASAI Data                  asaiuui L     2      1
D
E   Collected Digits I         collect L     6      1
F   Collected Digits II        collect L     1      1
G   Collected Digits III       collect L     1      1
H   Collected Digits Concat    collect L     8      1
I   Collected Digits UUI       asaiuui L     8      1
J
K   Expected Wait Time         collect L     5      1
L
M
N
O   Oceana Routing             collect P     1      1
P
Q   Oceana In Service          value   G     1             1              VV1
R
```

Configuring Avaya Aura® Media Server media files for Voice

About this task

Avaya provides a sample workflow for Voice. This workflow uses Avaya Aura® Media Server to play wait treatments to callers. This procedure describes how to manually deploy sample media files for Voice. You must manually create the content namespace and group if they do not already exist. The sample media files available for Voice are:

Announcement	Media file name
Expected Wait Time (EWT)	`ExpectedWaitTime.wav`
Unresponsive	`Unresponsive.wav`
VoiceMail	`VoiceMail.wav`

Note:

These media files are available to download from the Avaya DevConnect portal at http://www.avaya.com/devconnect. For information about downloading Avaya Oceana® resources from Avaya DevConnect, refer to the Avaya Oceana® Release Notes.

Before you begin

Ensure that you have the Engagement Designer workflow for Voice and the accompanying Avaya Aura® Media Server media files.

Procedure

1. In your web browser, enter the following URL:

   `https://<Avaya Aura Media Server FQDN>:8443/em`

2. In the **User ID** field, enter the User ID for logging in to Avaya Aura® Media Server.
3. In the **Password** field, enter the password for logging in to Avaya Aura® Media Server.
4. Click **Log in**.
5. In the navigation pane, click **Tools** > **Media Management**.
6. On the Media Management page, select the **Communication Manager** check box.
7. Click **Browse**.
8. On the Provision Media page, expand the **Communication Manager** content namespace.
9. Select the content group to which you want to add a media file.
10. Click **Add Media**.
11. In the Add Media dialog box, click **Browse** and navigate to the sample media files.
12. Select a file and click **Upload**.
13. Continue uploading all the media files to the **Communication Manager** content namespace.

Adding announcements

About this task

You can use announcements to play wait treatments to callers, and allow callers to provide input. Based on that input, Avaya Oceana® can decide to provide additional treatments or route the call elsewhere. Ensure that the media files exist on Avaya Aura® Media Server or on your Media Gateway.

Note:

These media files are available to download from the Avaya DevConnect portal at http://www.avaya.com/devconnect. For information about downloading Avaya Oceana® resources from Avaya DevConnect, refer to the Avaya Oceana® Release Notes.

Before you begin

In Avaya Aura® Media Server, create a content namespace for Communication Manager and then add the media files (*.wav) for your announcements to the namespace.

Note:

If you use a Media Gateway, you can use the standard procedure to upload the media files.

Procedure

1. Use the System Access Terminal (SAT) interface to add announcements. Use the **`add announcement`** command.
2. In the **Annc Name** field, type the name of the announcement file that you loaded on Avaya Aura® Media Server.
3. In the **Annc Type** field, type `integrated`.
4. In the **Source** field, type the appropriate value for the Avaya Aura® Media Server where you loaded the Welcome announcement file. For example, type `M1`.
5. In the **COR** and **TN** fields, type the required values for your solution.
6. Save the settings.

Example

The examples below show announcements for handling cases where fallback to Elite skills-based routing occurs, for advising the customer of expected wait time (EWT) while waiting for an Avaya Oceana® agent, and for offering the option to leave a voice mail.

```
change announcement 8289981                                    Page   1 of   1

                        ANNOUNCEMENTS/AUDIO SOURCES

  Extension: 828-9981                          COR: 1
  Annc Name: Unresponsive                       TN: 1
  Annc Type: integrated                     Queue? y
     Source: M1
  Protected? n
```

```
change announcement 8289983                                    Page   1 of   1

                        ANNOUNCEMENTS/AUDIO SOURCES

  Extension: 828-9983                          COR: 1
  Annc Name: ExpectedWaitTime                   TN: 1
  Annc Type: integrated                     Queue? y
     Source: M1
  Protected? n
```

```
change announcement 8289984                                    Page   1 of   1

                        ANNOUNCEMENTS/AUDIO SOURCES

  Extension: 828-9984                          COR: 1
  Annc Name: VoiceMail                          TN: 1
  Annc Type: integrated                     Queue? y
     Source: M1
  Protected? n
```

Creating the Fallback Vector Directory Number

About this task

Use this procedure to create the Fallback Vector Directory Number (VDN).

Procedure

1. Run **`add vdn next`** or **`add vdn n`**.

   n is the extension that you want to use for the VDN. This example uses 8284103.

2. On page 1 of the VECTOR DIRECTORY NUMBER screen, perform the following steps:

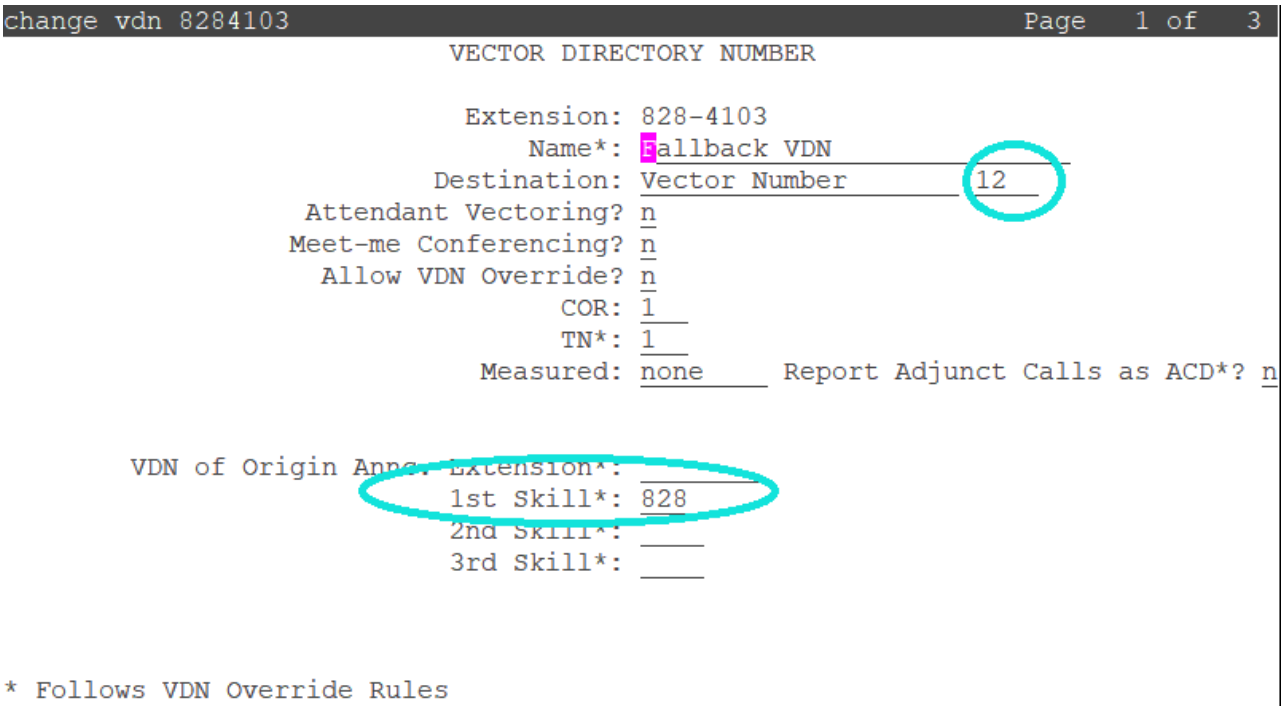
   a. In the **Name** field, enter the name of the VDN.

   b. In the **Destination** field, set the destination to a vector number which is not in use. This example uses 12.

   c. In the **1st Skill*** field, enter the Hunt Group that you created for Oceana agents. This example uses the Oceana Agent Pool Hunt Group, 828.

3. Save the settings.

Example



Configuring a vector for the Fallback VDN

About this task

Use this procedure to configure a vector for the Fallback VDN to automatically route calls to Call Center Elite when Avaya Oceana® is down or call routing fails.

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Fallback VDN. In this example, the vector number is 12.
3. On page 1 of the CALL VECTOR screen, perform the following steps:
   a. In the **Name** field, enter the name of the vector as `Fallback Vector`.

      This standard name makes maintenance and troubleshooting easier.

b. Enter the details required from line 01 to line 06 as shown below:

```
change vector 12                                          Page   1 of   6
                                  CALL VECTOR

    Number: 12              Name: Fallback Vector
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n          Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 #   Oceana encountered error
02 set          0      = none   CATR  0
03 announcement 8289981
04 queue-to     skill 1st  pri h
05 wait-time    60  secs hearing ringback
06 goto step    5            if unconditionally
07
08
09
10
11
12

                        Press 'Esc f 6' for Vector Editing
```

Note:

- The example vector plays an out of service announcement and queues the call to the Elite skill assigned to all Oceana agents. The call can route to any agent logged into this Elite skill. Replace these lines as required for your solution. For example, queue the call to an attendant, queue the call directly to a voice mail number, or queue to any Elite skill.

4. Save the settings.

Creating the Ingress Vector Directory Number

About this task

Use this procedure to create the Ingress Vector Directory Number (VDN) for Adjunct Route.

Procedure

1. Run **`add vdn next`** or **`add vdn n`**.

   n is the extension that you want to use for the VDN. This example uses 8284100.

2. On page 1 of the VECTOR DIRECTORY NUMBER screen, perform the following steps:

   a. In the **Name** field, enter the name of the VDN.

   b. In the **Destination** field, set the destination to a vector number which is not in use. This example uses 1.

   c. In the **1st Skill*** field, enter the Hunt Group that you created for Oceana agents. This example uses the Oceana Agent Pool Hunt Group, 828.

3. Save the settings.

Example

```
change vdn 8284100                                          Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                              Extension: 828-4100
                                  Name*: Oceana Ingress VDN
                            Destination: Vector Number          1
                     Attendant Vectoring? n
                   Meet-me Conferencing? n
                     Allow VDN Override? n
                                    COR: 1
                                    TN*: 1
                               Measured: none       Report Adjunct Calls as ACD*? n

        VDN of Origin Annc. Extension*:
                            1st Skill*: 828
                            2nd Skill*:
                            3rd Skill*:

SIP URI:

* Follows VDN Override Rules
```

Configuring a vector for the Ingress VDN

About this task

Use this procedure to configure a vector for the Ingress VDN to initiate the Adjunct Route to Avaya Oceana®.

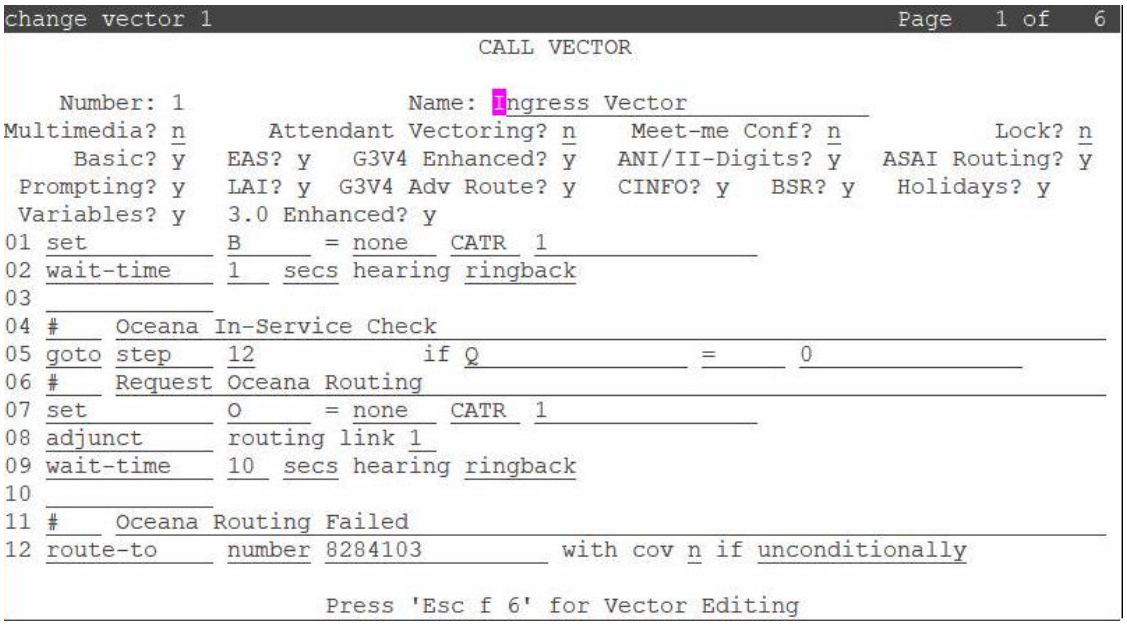
Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Ingress VDN. In this example, the vector number is 1.
3. On page 1 of the CALL VECTOR screen, perform the following steps:
   a. In the **Name** field, enter the name of the vector as `Ingress Vector`.

      This standard name makes maintenance and troubleshooting easier.

b. Enter the details required from line 01 to line 12 as shown below:



```
change vector 1                                          Page   1 of   6
                                CALL VECTOR

    Number: 1                Name: Ingress Vector
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n          Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 set          B      = none   CATR  1
02 wait-time    1   secs hearing ringback
03
04 #    Oceana In-Service Check
05 goto step    12            if Q              =      0
06 #    Request Oceana Routing
07 set          O      = none   CATR  1
08 adjunct      routing link 1
09 wait-time    10  secs hearing ringback
10
11 #    Oceana Routing Failed
12 route-to     number 8284103          with cov n if unconditionally

                        Press 'Esc f 6' for Vector Editing
```

Important:

In line 08, you must specify the number of the first CTI-Link that you created while configuring the CTI-Link to Application Enablement Services. It is recommended that you use two Application Enablement Services and two CTI-Links for robustness. Add the second CTI-Link to the vector after line 08 if required. If your solution implements disaster recovery, configure up to four CTI-Links. You must ensure that you change the other lines in the vector as appropriate if you add multiple CTI-Links.

Note:

- If there is a routing failure at any point during the call, the call routes to the fallback VDN and the configured fallback Elite skill.

4. Save the settings.

Creating the Treatment Vector Directory Number

About this task

Use this procedure to create the Treatment Vector Directory Number (VDN).

Procedure

1. Run **`add vdn next`** or **`add vdn n`**.

   n is the extension that you want to use for the VDN. This example uses 8284104.

2. On page 1 of the VECTOR DIRECTORY NUMBER screen, perform the following steps:

   a. In the **Name** field, enter the name of the VDN.

b. In the **Destination** field, set the destination to a vector number which is not in use. This example uses 10.

c. In the **1st Skill*** field, enter the Hunt Group that you created for Oceana agents. This example uses the Oceana Agent Pool Hunt Group, 828.

3. Save the settings.

Example

```
change vdn 8284104                                          Page   1 of   3
                          VECTOR DIRECTORY NUMBER

                            Extension: 828-4104
                                 Name*: Treatment VDN
                          Destination: Vector Number        10
                Attendant Vectoring? n
               Meet-me Conferencing? n
                 Allow VDN Override? n
                               COR: 1
                               TN*: 1
                          Measured: none        Report Adjunct Calls as ACD*? n


      VDN of Origin Annc.: Extension*:
                           1st Skill*: 828
                           2nd Skill*:
                           3rd Skill*:

SIP URI:

* Follows VDN Override Rules
```

Configuring a vector for the Treatment VDN

About this task

Use this procedure to configure a vector for the Treatment VDN to provide treatments for calls that route to Avaya Oceana®.

Note:

This example vector includes coverage to mailbox and estimated wait time (EWT) options. These sections are optional, remove or edit these sections as required for your solution. For example, remove the option to leave a message if your solution does not include voice mail, or route the caller to different mailboxes based on caller input. The EWT section is line 07 to line 10, and the voice mail section is line 13 to line 15.

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Treatment VDN. In this example, the vector number is 10.

3. On page 1 of the CALL VECTOR screen, perform the following steps:
   a. In the **Name** field, enter the name of the vector as `Treatment Vector`.

      This standard name makes maintenance and troubleshooting easier.

   b. Enter the details required from line 01 to line 23 as shown below:

```
change vector 10                                          Page   1 of   6
                                  CALL VECTOR

    Number: 10               Name: Treatment Vector
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n          Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 #   Check Expected Wait Time
02 collect      5   digits after announcement none     for K
03
04 #   Locate Oceana agent
05 adjunct      routing link 1
06 wait-time    2   secs hearing ringback
07 goto step    11             if K                =      #
08 goto step    11             if K                <=     180
09 #   Optional announcement
10 announcement 8289983
11 wait-time    15  secs hearing ringback
12

                        Press 'Esc f 6' for Vector Editing
```

```
change vector 10                                          Page   2 of   6
                                  CALL VECTOR
13 #   Offer Voicemail option
14 collect      1   digits after announcement 8289984  for none
15 goto step    23             if digits           =      9
16
17 goto step    11             if unconditionally
18
19 #   Oceana encountered error
20 route-to     number 8284103          with cov n if unconditionally
21
22 #   Leave a message
23 route-to     number 8284105          with cov n if unconditionally
24
25
26
27
28
29
30
31
32
```

Important:

In line 05, you must specify the number of the first CTI-Link that you created while configuring the CTI-Link to Application Enablement Services. It is recommended that you use two Application Enablement Services and two CTI-Links for robustness. Add the second CTI-Link to the vector after line 05 if required. If your solution implements disaster recovery, configure up to four CTI-Links. You must ensure that you change the other lines in the vector as appropriate if you add multiple CTI-Links.

Note:

- The example vector collects EWT data, and based on that data can provide a treatment to a caller waiting for an agent. In this example, if EWT is higher than 3 minutes then the EWT announcement plays, followed after a wait by the voice mail announcement and the option to immediately leave a voice mail.
- If there is a routing failure at any point during the call, the call routes to the fallback VDN and the configured fallback Elite skill.

4. Save the settings.

Creating the Routing Vector Directory Number

About this task

Use this procedure to create the Routing Vector Directory Number (VDN).

Procedure

1. Run **`add vdn next or add vdn n`**.

   n is the extension that you want to use for the VDN. This example uses 8284000.

2. On page 1 of the VECTOR DIRECTORY NUMBER screen, perform the following steps:
   a. In the **Name** field, enter the name of the VDN.
   b. In the **Destination** field, set the destination to a vector number which is not in use. This example uses 2.
   c. In the **Allow VDN Override** field, type `y`.
   d. In the **1st Skill*** field, enter the Hunt Group that you created for Oceana agents. This example uses the Oceana Agent Pool Hunt Group, 828.
3. Save the settings.

Example

```
change vdn 8284000                                          Page   1 of   3
                          VECTOR DIRECTORY NUMBER

                            Extension: 828-4000
                                 Name*: Oceana Routing VDN
                          Destination: Vector Number        2
                Attendant Vectoring? n
               Meet-me Conferencing? n
                 Allow VDN Override? y
                               COR: 1
                               TN*: 1
                          Measured: none       Report Adjunct Calls as ACD*? n


      VDN of Origin Annc. Extension*:
                          1st Skill*: 828
                          2nd Skill*:
                          3rd Skill*:



* Follows VDN Override Rules
```

Configuring a vector for the Routing VDN

About this task

Use this procedure to configure a vector for the Routing VDN to collect the digits (containing the Agent ID) set by the Adjunct Route application.

Important:

This example vector assumes the agent ID's are 7 digits in length. You must replace line 05 and 06 as required for your solution.

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Routing VDN. In this example, the vector number is 2.
3. On page 1 of the CALL VECTOR screen, perform the following steps:
   a. In the **Name** field, enter the name of the vector as `Routing Vector`.

      This standard name makes maintenance and troubleshooting easier.

b. Enter the details required from line 01 to line 18 as shown in the following screen:

```
change vector 2                                          Page   1 of   6
                                CALL VECTOR

    Number: 2                Name: Routing Vector
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n          Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y    Holidays? y
 Variables? y   3.0 Enhanced? y
01 goto step    17            if B              <>     1
02
03 #    Connect Oceana agent
04 collect      16   digits after announcement none      for A
05 goto step    7             if A              <=     9999999
06 set          A      = A      SEL   7
07 route-to     number A                with cov n if unconditionally
08
09 #    Handle Presentation Failure
10 adjunct      routing link 1
11 wait-time    3    secs hearing ringback
12

                        Press 'Esc f 6' for Vector Editing
```

```
change vector 2                                          Page   2 of   6
                                CALL VECTOR
13 #    Oceana encountered error
14 route-to     number 8284103          with cov n if unconditionally
15
16 #    Handle Video & Web Voice
17 route-to     digits with coverage n
18 stop
19
20
21
22
23
24
25
26
27
28
29
30
31
32
```

Important:

- This example vector assumes the agent ID's are 7 digits in length. You must replace line 05 and 06 as required for your solution. For example, for a 4 digit dial plan change line 05 06 to: `goto step 7 if A <= 9999 set A = A SEL 4`
- In line 10, you must specify the number of the first CTI-Link that you created while configuring the CTI-Link to Application Enablement Services. It is recommended that you use two Application Enablement Services and two

CTI-Links for robustness. Add the second CTI-Link to the vector after line 10 if required. If your solution implements disaster recovery, configure up to four CTI-Links. You must ensure that you change the other lines in the vector as appropriate if you add multiple CTI-Links.

Note:

- If there is a routing failure at any point during the call, the call routes to the fallback VDN and the configured fallback Elite skill.

4. Save the settings.

Creating the RONA Vector Directory Number

About this task

Use this procedure to create the RONA Vector Directory Number (VDN).

Procedure

1. Run **`add vdn next`** or **`add vdn n`**.

   n is the extension that you want to use for the VDN. This example uses 8284001.

2. On page 1 of the VECTOR DIRECTORY NUMBER screen, perform the following steps:
   a. In the **Name** field, enter the name of the VDN.
   b. In the **Destination** field, set the destination to a vector number which is not in use. This example uses 3.
   c. In the **1st Skill*** field, enter the Hunt Group that you created for Oceana agents. This example uses the Oceana Agent Pool Hunt Group, 828.
3. Save the settings.

Example

```
change vdn 8284001                                          Page   1 of   3
                          VECTOR DIRECTORY NUMBER

                            Extension: 828-4001
                                 Name*: Oceana RONA VDN
                          Destination: Vector Number        3
                Attendant Vectoring? n
               Meet-me Conferencing? n
                 Allow VDN Override? n
                               COR: 1
                               TN*: 1
                          Measured: none       Report Adjunct Calls as ACD*? n


        VDN of Origin Annc. Extension*:
                               1st Skill*: 828
                               2nd Skill*:
                               3rd Skill*:



* Follows VDN Override Rules
```

Configuring a vector for the RONA VDN

About this task

Use this procedure to configure a vector for the RONA VDN to handle Voice Redirect On No Answer (RONA) scenarios. Calls are redirected to the RONA VDN if the number of unanswered rings exceeds the value set for the Hunt Group.

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the RONA VDN. In this example, the vector number is 3.
3. On page 1 of the CALL VECTOR screen, perform the following steps:
   a. In the **Name** field, enter the name of the vector as `RONA Vector`.

      This standard name makes maintenance and troubleshooting easier.

b. Enter the details required from line 01 to line 13 as shown in the following screen:

```
change vector 3                                          Page   1 of   6
                                  CALL VECTOR

    Number: 3                 Name: RONA Vector
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n          Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 goto step   12            if B              <>     1
02 goto step   9             if O              <>     1
03
04 #   Locate Oceana agent
05 adjunct     routing link 1
06 wait-time   10  secs hearing ringback
07
08 #   Oceana encountered error
09 route-to    number 8284103          with cov n if unconditionally
10
11 #   Handle Video & Web Voice
12 disconnect  after announcement none

                    Press 'Esc f 6' for Vector Editing
```

```
change vector 3                                          Page   2 of   6
                                  CALL VECTOR
13 stop
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
```

Important:

In line 05, you must specify the number of the first CTI-Link that you created while configuring the CTI-Link to Application Enablement Services. It is recommended that you use two Application Enablement Services and two CTI-Links for robustness. Add the second CTI-Link to the vector after line 05 if required. If your solution implements disaster recovery, configure up to four CTI-Links. You must ensure that you change the other lines in the vector as appropriate if you add multiple CTI-Links.

Note:

The call routes to the fallback VDN if there is no agent available to answer the call.

4. Save the settings.

Creating the Coverage Vector Directory Number

About this task

Use this procedure to create the Coverage Vector Directory Number (VDN).

Note:

- Perform this procedure only if your solution includes voice mail.
- Avaya Oceana® supports Coverage for the Required Resource scenario where the customer requests a specific agent, but the agent does not answer the call for some reason. If Coverage is configured, the call is routed to the voice mailbox of the agent so that the customer can leave a message for the agent. Avaya Oceana® also supports Coverage as a wait treatment option for callers. For example, callers can choose to leave a voice mail if the estimated wait time (EWT) for their call is high.

Procedure

1. Run **`add vdn next`** or **`add vdn n`**.

   n is the extension that you want to use for the VDN. This example uses 8284105.

2. On page 1 of the VECTOR DIRECTORY NUMBER screen, perform the following steps:

   a. In the **Name** field, enter the name of the VDN.

   b. In the **Destination** field, set the destination to a vector number which is not in use. This example uses 7.

3. Save the settings.

Example

```
change vdn 8284105                                          Page   1 of   3
                          VECTOR DIRECTORY NUMBER

                            Extension: 828-4105
                                 Name*: Coverage VDN
                          Destination: Vector Number        7
                Attendant Vectoring? n
               Meet-me Conferencing? n
                 Allow VDN Override? n
                               COR: 1
                               TN*: 1
                          Measured: none       Report Adjunct Calls as ACD*? n

                                                                .
      VDN of Origin Annc. Extension*:
                          1st Skill*:
                          2nd Skill*:
                          3rd Skill*:


* Follows VDN Override Rules
```

Configuring a vector for the Coverage VDN

About this task

Use this procedure to configure a vector for the Coverage VDN. For example, callers can choose to leave a voice mail if the estimated wait time (EWT) for their call is high.

Note:

- Perform this procedure only if your solution includes voice mail.

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Coverage VDN. In this example, the vector number is 7.
3. On page 1 of the CALL VECTOR screen, perform the following steps:
   a. In the **Name** field, enter the name of the vector as `Coverage Vector`.

      This standard name makes maintenance and troubleshooting easier.
   b. Enter the details required from line 01 to line 13 as shown in the following figure:

Important:

In line 12, you must replace the number in this example (2990000) with the Internal Messaging access number that you configured in Avaya Aura® Messaging. This number must include “~pA” at the end. Change this as required for your solution. Based on caller input you can choose to route the call to any mailbox number. For example, configure a mailbox for every agent or every skill. For more information about configuring calls to route to different mailboxes, see Configuring a vector for the Treatment VDN on page 279.

```
change vector 7                                          Page   1 of   6
                                CALL VECTOR

    Number: 7                Name: Coverage Vector
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n          Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 goto step   8            if B               <>     1
02
03 #   Retrieve Oceana agent
04 collect     16   digits after announcement none    for A
05 goto step   11           if unconditionally
06
07 #   Handle Video & Web Voice
08 set         A      = none   CATR  digits
09
10 #   Connect Voicemail
11 wait-time   1    secs hearing ringback
12 route-to    number 2990000~pA        with cov n if unconditionally

                      Press 'Esc f 6' for Vector Editing
```

```
change vector 7                                          Page   2 of   6
                                CALL VECTOR

13 stop
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
```

4. Save the settings.

Creating a Transfer Vector Directory Number

About this task

Use this procedure to create the Transfer Vector Directory Number (VDN) for Adjunct Route. The types of transfer VDNs created include:

- Transfer to Service VDN
- Transfer to User VDN

Procedure

1. Run **`add vdn next`** or **`add vdn n`**.

   n is the extension that you want to use for the VDN.

   For Transfer to Service VDN, the extension is 8284101.

   For Transfer to User VDN, the extension is 8284114.

2. On page 1 of the VECTOR DIRECTORY NUMBER screen, perform the following steps:

   a. In the **Name** field, enter the name of the VDN.

   b. In the **Destination** field, set the destination to a vector number which is not in use. This example uses 5.

      For Transfer to Service VDN, the vector number is 5.

      For Transfer to User VDN, the vector number is 11.

   c. In the **1st Skill*** field, enter the Hunt Group that you created for Oceana agents. This example uses the Oceana Agent Pool Hunt Group, 828.

3. Save the settings.

Example

Transfer to Service VDN

```
display vdn 8284101                                          Page   1 of   3
                             VECTOR DIRECTORY NUMBER

                               Extension: 828-4101
                                   Name*: Transfer2Srvc VDN
                             Destination: Vector Number        5
                      Attendant Vectoring? n
                     Meet-me Conferencing? n
                       Allow VDN Override? y
                                     COR: 1
                                     TN*: 1
                                Measured: none     Report Adjunct Calls as ACD*? n


          VDN of Origin Annc. Extension*:
                               1st Skill*: 828
                               2nd Skill*:
                               3rd Skill*:

SIP URI:

* Follows VDN Override Rules
```

Transfer to User VDN

```
display vdn 8284114                                          Page   1 of   3
                             VECTOR DIRECTORY NUMBER

                               Extension: 828-4114
                                   Name*: Transfer2Usr VDN
                             Destination: Vector Number        11
                      Attendant Vectoring? n
                     Meet-me Conferencing? n
                       Allow VDN Override? y
                                     COR: 1
                                     TN*: 1
                                Measured: none     Report Adjunct Calls as ACD*? n


          VDN of Origin Annc. Extension*:
                               1st Skill*: 828
                               2nd Skill*:
                               3rd Skill*:

SIP URI:

* Follows VDN Override Rules
```

Configuring a vector for the Transfer to Service VDN

About this task

Use this procedure to configure a vector for the Transfer to Service VDN to initiate the Adjunct Route to Avaya Oceana®.

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Transfer to Service VDN.
3. On page 1 of the CALL VECTOR screen, perform the following steps:
   a. In the **Name** field, enter the name of the vector as `Transfer2Srvc Vector`.

      This standard name makes maintenance and troubleshooting easier.

   b. Enter the details required from line 01 to line 10 as shown in the following screen:

```
display vector 5                                          Page   1 of   6
                                  CALL VECTOR

    Number: 5                Name: Transfer2Srvc Vector
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 set           B      = none   CATR  1
02 wait-time     1   secs hearing ringback
03
04 #    Locate Oceana agent
05 set           O      = none   CATR  1
06 adjunct       routing link 1
07 wait-time     10  secs hearing ringback
08
09 #    Oceana encountered error
10 route-to      number 8284103          with cov n if unconditionally
11
12

                        Press 'Esc f 6' for Vector Editing
```

Important:

In line 06, you must specify the number of the first CTI-Link that you created while configuring the CTI-Link to Application Enablement Services. It is recommended that you use two Application Enablement Services and two CTI-Links for robustness. Add the second CTI-Link to the vector after line 06 if required. If your solution implements disaster recovery, configure up to four CTI-Links. You

must ensure that you change the other lines in the vector as appropriate if you add multiple CTI-Links.

4. Save the settings.

Configuring a vector for the Transfer to User VDN

About this task

Use this procedure to configure a vector for the Transfer to User VDN to initiate the Adjunct Route to Avaya Oceana®.

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Transfer to User VDN.
3. On page 1 of the CALL VECTOR screen, perform the following steps:
   a. In the **Name** field, enter the name of the vector as `Transfer2Usr Vector`.

      This standard name makes maintenance and troubleshooting easier.

   b. Enter the details required from line 01 to line 10 as shown in the following screen:

```
display vector 11                                          Page   1 of   6
                                  CALL VECTOR

    Number: 11               Name: Transfer2Usr Vector
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 set           B      = none   CATR  1
02 wait-time     1   secs hearing ringback
03
04 #    Locate Oceana agent
05 set           O      = none   CATR  1
06 adjunct       routing link 1
07 wait-time     10  secs hearing ringback
08
09 #    Oceana encountered error
10 route-to      number 8284103          with cov n if unconditionally
11
12

                       Press 'Esc f 6' for Vector Editing
```

Important:

In line 06, you must specify the number of the first CTI-Link that you created while configuring the CTI-Link to Application Enablement Services. It is recommended that you use two Application Enablement Services and two CTI-Links for robustness. Add the second CTI-Link to the vector after line 06 if required. If your solution implements disaster recovery, configure up to four CTI-Links. You must ensure that you change the other lines in the vector as appropriate if you add multiple CTI-Links.

4. Save the settings.

Chapter 17: Deploy the sample workflows for Voice

Deploying the sample Voice workflow

About this task

Avaya provides a sample workflow for the Voice channel. With this procedure, you can deploy the sample Voice workflow and configure the workflow attributes.

You can use the same procedure to deploy the other sample workflows of Avaya Oceana®.

Before you begin

- Download the latest version of the sample workflow from the Avaya DevConnect portal at http://www.avaya.com/devconnect. For information about downloading Avaya Oceana® resources from Avaya DevConnect, see *Avaya Oceana® Release Notes*.

Procedure

1. In your web browser, enter the following URL to open the Designer Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. In the Import Workflow dialog box, click **Choose File**.
4. Browse to the folder containing the sample workflow, select the workflow, and click **Import**.
5. Click **Save Workflow**.
6. In the Save Workflow dialog box, do the following:
   a. In the **Workflow Name** field, type `OceanaVoiceAssistedService`.

      You can provide any name for the workflow.

   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy**.
8. In the Deployment Details dialog box, click **Deploy**.

9. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

10. On the Workflows tab, verify that the OceanaVoiceAssistedService workflow is available in the list of deployed workflows.
11. On the Workflows tab, select the Voice workflow and click **Attributes**.
12. On the Workflow Attributes tab, do the following:
    a. In the **CoverageDestination** field, enter a value in the following format:

       <Number>@*<Domain.com>*

       The *<Number>* is the Coverage VDN that you created previously. For example, 8284105@domain.com.

       Enter a value in this field only if you use Coverage.

    b. In the **ExpectedWaitTime** field, set the time in seconds that EWT must exceed before the workflow sends a request to expand the agent pool to reduce the caller wait time.
    c. If you want to enable last agent routing for the voice channel, in the **LastAgentEnabled** field, enter the value `True`. Last agent routing is disabled by default.
    d. In the **PoolExpansionWaitTime** field, set the amount of time in seconds the caller hears wait treatment before the workflow sends a MatchUpdate to Work Assignment.
    e. In the **PriorityExpansionWaitTime** field, set the amount of time in seconds a priority caller hears wait treatment for before the workflow sends a MatchUpdate to Work Assignment to immediately connect the caller to an agent.
    f. In the **TreatmentDestination** field, enter a value in the following format:

       <Number>@*<Domain.com>*

       The *<Number>* is the Treatment VDN that you created previously. For example, 8284104@domain.com.

    g. In the **UseCoverage** field, enter one of the following values:
       - If you do not use Coverage, enter the value `False`.
       - If you use Coverage, enter the value `True`.

    h. Click **Close**.

Modifying the sample Voice workflow

About this task

Engagement Designer provides the IF This Then That (IFTTT) task in a workflow to modify the behavior of the workflow based on the variables defined in rule sets.

When you deploy the OceanaVoiceAssistedService workflow, Engagement Designer creates the empty Oceana Treatment rule set. This rule set is available on the Rules tab in the Admin Console of Engagement Designer.

If you have a single Treatment VDN, you set the **TreatmentDestination** field on the Workflow Attributes tab to the Treatment VDN, and the workflow routes the call to the Treatment VDN.

If you have multiple Treatment VDNs, you must add rules to administer which Treatment is applied for a caller, without having to redeploy the workflow. You can route calls to specific Treatment VDN's based on call attributes.

Use this example procedure to modify the OceanaVoiceAssistedService workflow, and add a rule that routes customer calls based on attributes.

Before you begin

Deploy the sample Voice workflow.

Procedure

1. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

2. Select the **Rules** tab.
3. On the Rules tab, select the check box for the Oceana Treatment rule set and click **Edit**.

   Engagement Designer displays the Edit Rules Editor dialog box.

4. Click **Add Rule**.
5. In the **Set Rule Name** field, type a name for the rule and click the save icon.
6. Click the **Advance** check box.
7. Click **Condition**.
8. In the **Expression** field, type the attribute based condition for this rule and click **Save**. You can also use the Expression builder to configure your condition.

   For example, type `WAInput["ServiceMap"].jsonPath("$.1.attributes.Language[0]") == "English"`. This rule routes calls to a specific VDN based on the language attribute.

9. Under **Then**, click **Add More**.
10. In the **Select Variable** field, select the variable for the Treatment VDN. For example, the Treatment variable in the sample Voice workflow is **FlowData.TreatmentDestination**.

11. In the **Enter value** field, enter the Treatment VDN number in the format `<number>@<domain.com>`. The <*number*> is the Treatment VDN that you created previously. For example, type `8284104@domain.com`.
12. Click **Save**.
13. Repeat Step 4 to Step 12 to add further rules for all of your Treatment VDNs. You can add multiple rules for each VDN.
14. Click **Done**.

Adding a rule to the sample Voice workflow for priority, rank, and service

About this task

When you deploy the OceanaVoiceAssistedService workflow, Engagement Designer creates an empty Oceana Voice Routing Service rule set. This rule set is available on the Rules tab in the Admin Console of Engagement Designer.

You can use this procedure to add rule to sample Voice workflow for priority, rank, and service attributes.

Before you begin

Deploy the sample Voice workflow.

Procedure

1. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`
2. Select the **Rules** tab.
3. On the Rules tab, select the check box for the Oceana Voice Routing Service rule set and click **Edit**.

   Engagement Designer displays the Edit Rules Editor dialog box.
4. Click **Add Rule**.
5. In the **Set Rule Name** field, type a name for the rule and click the save icon.
6. Click the **Advance** check box.
7. Click **Condition**.
8. In the **Expression** field, type the attribute based condition for this rule and click **Save**. You can also use the Expression builder to configure your condition.
9. Under **Then**, click **Add More**.

10. In the **Select Variable** field, select the variable for priority, rank, and service.
11. Click **Save**.
12. Click **Done**.

Sample Voice workflow

The following diagram describes the process flow for the sample Voice workflow:

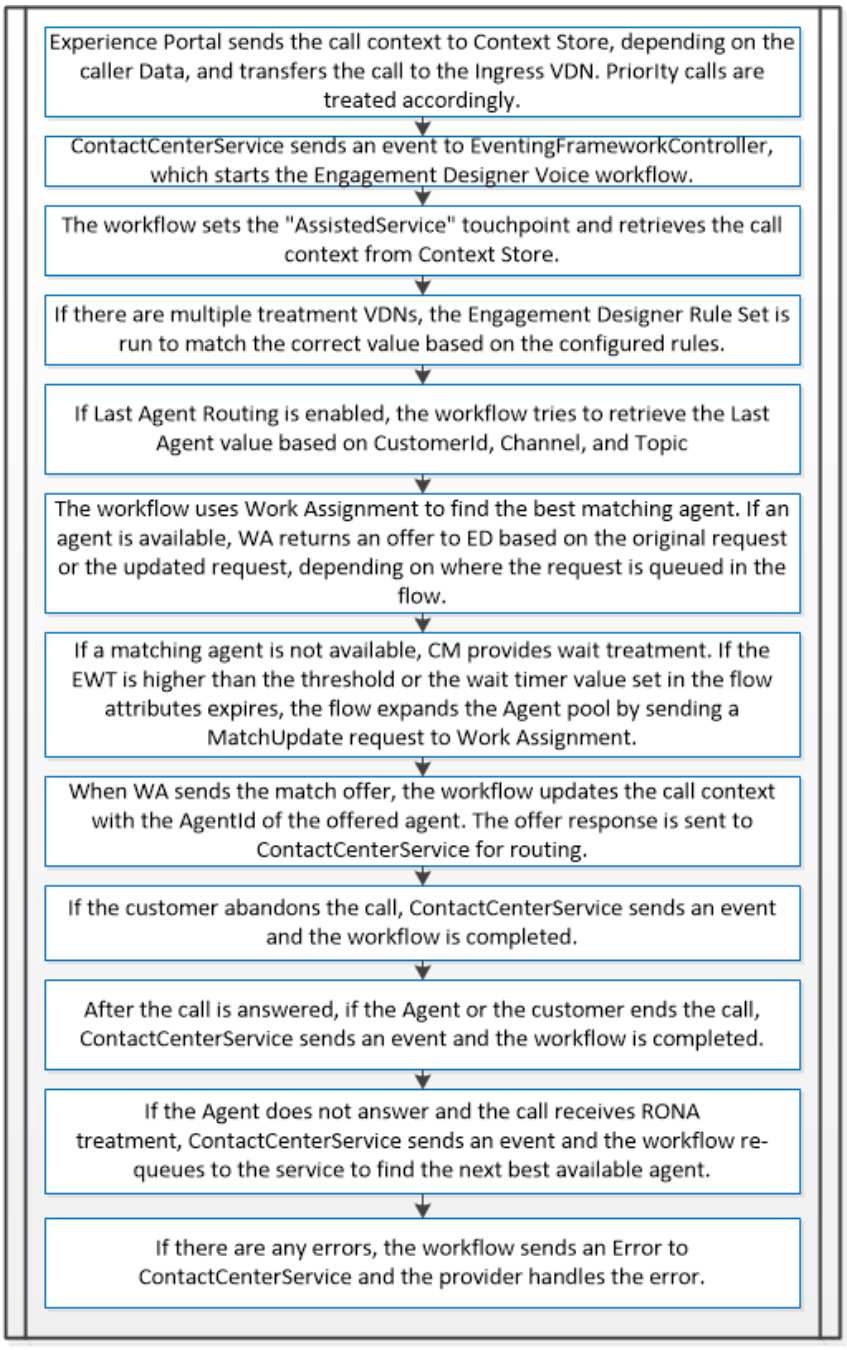


Figure 3: Sample Voice workflow

Deploying the sample Transfer to Service workflow for Voice

About this task

Avaya provides a sample Transfer to Service workflow for the Voice channel. With this procedure, you can deploy the sample Transfer to Service workflow and configure the workflow attributes.

Before you begin

- Download the latest version of the sample workflow from the Avaya DevConnect portal at http://www.avaya.com/devconnect. For information about downloading Avaya Oceana® resources from Avaya DevConnect, refer to the Avaya Oceana® Release Notes.
- In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Designer Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. In the Import Workflow dialog box, click **Choose File**.
4. Browse to the folder containing the sample workflow, select the workflow, and click **Import**.
5. Click **Save Workflow**.
6. In the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaVoiceTransfer`.

      You can provide any name for the workflow.

   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.
8. In the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

10. On the Workflows tab, verify that the OceanaVoiceTransfer workflow is available in the list of deployed workflows.
11. On the Workflows tab, select the Transfer workflow and click **Attributes**.

12. On the Workflow Attributes tab, do the following:
    a. In the **TreatmentDestination** field, enter a value in the following format:

       `<Number>@<Domain.com>`

       The <*Number*> is the Treatment VDN that you created previously. For example, 8284104@domain.com.
    b. Click **Close**.
13. Click the **Routing** tab.
14. Click **Create**.
15. In the **Select event** field, click **ROUTE_CONTACT_TRANSFER**.
16. In the **Select workflows** field, select the OceanaVoiceTransfer workflow.

    Note:

    Ensure that you click the workflow ending with the term `Latest`. For example, OceanaVoiceTransfer:Latest.
17. In the **Enter rule name** field, type `VoiceTransfer`.
18. Click **Add Rule**.
19. In the **Select schema attribute** field, click **RouteContactTransfer.ChannelType:string**.
20. In the **Select function** field, click **is equal to**.
21. In the **Enter value** field, type `Voice`.
22. Click **Save**.

    Engagement Designer displays the newly created rule in the list of rules.

Chapter 18: Configure Voice Self Service

Configure Voice Self Service for Avaya Oceana® overview

In Avaya Oceana®, you can use any of the following options for Voice Self Service:

- Avaya Experience Portal
- Avaya Aura® Call Center Elite

Important:

You must configure certain attributes in Avaya Control Manager before using the sample self-service applications and workflows. Ensure that you create the Language, Service and Location categories and associated attributes to validate the sample Self-Service Application or sample workflows. For more information about adding categories and attributes, see Adding Attribute Categories to Avaya Control Manager on page 238 and Adding Attributes to Avaya Control Manager on page 239.

Capturing custom data from Avaya Oceana® voice calls

Avaya Context Store Snap-in provides a centralized solution to store contextual information about PSTN voice callers and their contacts. Avaya Context Store Snap-in can store context entries which consist of several data elements. The following are the key data elements:

- ContextID: A text field that contains a unique identification for the context. You can specify the contextID while adding the context entry in Context Store. If you do not specify a contextID while creating a context, Context Store generates a unique id.
- Data: The data field in a context entry is an abstract map with multiple key-value pairs. Keys in the data field must be unique. Multiple identical keys in the same request results in the values being overwritten with the last key.

For more information about other Avaya Context Store Snap-in data elements, see *Avaya Context Store Snap-in Reference*

Avaya Context Store Snap-in maps the front-end customer's data model into the Context Store data model. You must consider the type of data and the size of data that you want to store in Context Store. There are several methods to add or update data in Context Store.

If your solution includes Avaya Experience Portal (AAEP), Avaya Oceana® provides a Pluggable Data Connector (PDC) to integrate with AAEP. AAEP uses call flows created in Orchestration Designer (OD) to handle incoming PSTN calls and capture customer data. When you install the Avaya Oceana® PDC in OD, a Context Store Connector node is available in OD. You can use the Context Store Connector node to integrate Avaya Context Store Snap-in into your call flows. You can also configure the Context Store Connector node to perform actions such as creating, getting, updating, or deleting context information using the contextID.

Context Store data expires after the predefined Lease Time parameter expires. The Lease Time parameter is configurable, and Context Store preserves a context entry until the lease time expires. Any Avaya Context Store Snap-in client can renew this lease time, or time-to-live at any time. The default value for lease time is 7200 seconds, you can configure the lease time to be any value between 1 second and 86400 seconds. Clients can also define the lease time while creating a context and specify different lease time values for different scenarios.

Context entries are also persisted to the External Data Mart. After a context has expired from Context Store, it can still be retrieved from the EDM. This is an automatic process. If you attempt to get a context which has expired in the Context Store space, it gets retrieved from the EDM.

The following rules apply to adding, updating, and deleting Avaya Context Store Snap-in data in an Avaya Oceana® deployment:

- Context Store stores the default standard schema detail (caller attributes and Work Assignment related data) against a unique contextID.
- You can pass custom data into Context Store using the Data element. For example, a customer's ticket number, location, or interest. Using a customized version of the default Avaya Oceana® AAEP application, you can capture callers custom data and insert it to an existing Work Request ID (in Avaya Oceana®, the Context ID and the Work Request ID are set to the same value) using the Data field of that existing Work Request. This is on the assumption that there is an existing Work Request ID and it is available to the AAEP application if deployed. The Work Request ID can be generated by Context Store in an Avaya Oceana® and AAEP deployment. If you use Elite IVR, the UCID value is used. AAEP is not required if you use Elite IVR.
- Avaya Oceana® supports data privacy. To adhere to data privacy laws, custom data is not stored in the EDM database by default. If there is a requirement to store custom data, an administrator can change the default setting.
- Avaya recommends a maximum value of 600 Bytes for the custom data field size. If you want to use a larger data field size, please contact Avaya Support.

For other Avaya Context Store Snap-in deployments where there is a requirement to add custom data, see *Avaya Context Store Snap-in Developer Guide* and *Avaya Context Store Snap-in Reference*, available on the Avaya Support website at https://support.avaya.com.

Configure Avaya Experience Portal

Avaya Experience Portal provides an Interactive Voice Response (IVR) front-end for voice calls in Avaya Oceana®.

To install and commission Experience Portal, see:

- *Implementing Avaya Experience Portal on a single server*
- *Implementing Avaya Experience Portal on multiple servers*
- *Deploying Avaya Experience Portal in an Avaya Customer Experience Virtualized Environment*
- *Administering Avaya Experience Portal*

Sample Self-Service Application (SSA)

Avaya provides a sample Voice Self-Service Application (SSA) as part of Avaya Oceana®. The sample SSA collects customer requirements before transferring the call to an Avaya Engagement

Designer workflow to match the customer to a suitable agent. After you deploy this application, this application provides a basic IVR front-end to Avaya Oceana®.

You can also create custom voice applications in Orchestration Designer by importing the sample application source code and using it as a starting point. Orchestration Designer is an Eclipse plug-in used to create applications for Experience Portal. The sample application and source code are available on the Avaya DevConnect portal at http://www.avaya.com/devconnect. For information about Avaya DevConnect, see *Avaya DevConnect Program Guide* available on https://support.avaya.com.

SSA requires a Nuance Text-to-Speech server to play English language voice prompts to the calling customer. To match the customer to a suitably-skilled agent, SSA prompts the customer to specify the Service Type and Language. SSA interacts with Context Store to keep vital call-related data for the lifetime of the call.

Avaya Engagement Designer also uses this data to make the request to Work Assignment Snap-in for a suitable agent. You must deploy SSA on an Application Server, which can be installed on Experience Portal, or on a stand-alone server running the Linux operating system.

Sample Self-Service Application deployment

Installing a new application server

About this task

This section lists the procedure you must perform if the application server is not deployed. You must install the Experience Portal application server on the local Experience Portal system or on a dedicated Linux server.

Procedure

1. Copy the `AAEP.iso` file to the server.
2. Login as sroot.
3. Run the following command to create the `/mnt/disk` directory:

   `mkdir /mnt/disk`
4. Run the following command to mount the `ISO` file in the `/mnt/disk` directory:

   `mount –o loop <ISO location and filename> /mnt/disk`
5. Run the following command to change to the application server directory:

   `cd /mnt/disk/Support/Appserver`
6. Run the following command to install the application server:

   `./InstallAppServer.sh <install directory/opt/AppServer>`

   The application server is displayed under **System Management** in the Experience Portal Management web interface.

   The application server uses the port 7080 as default and is set to auto deploy applications when added to the `tomcat/webapps` directory.

Adding the Avaya Oceana® Cluster 1 certificate to Orchestration Designer on Avaya Experience Portal

About this task

Use this procedure to add the Avaya Oceana® Cluster 1 certificate to Orchestration Designer on Avaya Experience Portal. This certificate allows secure connections from Avaya Experience Portal to Avaya Oceana®.

Before you begin

Have the root CA certificate that you use to sign the identity certificates of the Avaya Breeze® platform nodes in Avaya Oceana® Cluster 1.

Procedure

1. In your web browser, enter the following URL:

   `http://<IP address of the Experience Portal server>:7080/runtimeconfig/`

2. In the **Username** field, type `ddadmin`.

   `ddadmin` is the default user name for the first time.

3. In the **Password** field, type `ddadmin`.

   `ddadmin` is the default password for the first time.

4. Click **Login**.
5. In the navigation pane, click **Certificates**.
6. Click **Add**.
7. In the **Name** field, type an appropriate name for the certificate.
8. In the **Enter Certificate Path** field, click **Choose File**, navigate to the root CA certificate, and click **Continue**.

   The browser displays the new certificate on the screen.

9. Click **Save**.

Deploying run-time support files

About this task

Use this procedure to deploy the run-time support files for each application server where you want to install the Orchestration Designer applications.

Before you begin

Add or modify certificates in the default keystore on the application server at `<TOMCAT_HOME>/lib/trusted_weblm_cert.jks` and then save a copy of the existing `trusted_weblm_certs.jks` file.

Procedure

1. Download the appropriate `runtimeSupportTomcat.zip` file from the Orchestration Designer environment that you used to compile the Avaya Oceana® Self Service application.

   See the *Avaya Orchestration Designer Developer's Guide* for instructions on how to extract this zip file.

2. On the application server, go to the `<TOMCAT_HOME>` folder and unzip the `runtimeSupportTomcat.zip` file.

   The system extracts the run-time support jars to the `<TOMCAT_HOME>/runtimeSupportTomcat/lib` folder.

3. From the `<TOMCAT_HOME>/runtimeSupportTomcat/lib` folder, copy the run-time support jars to the `<TOMCAT_HOME>/lib` folder.

4. If you have copied the default keystore, copy that to `<TOMCAT_HOME>/lib/trusted_weblm_certs.jks`.

Deploying the self-service application

About this task

Use this procedure to deploy the self-service application by copying two `.war` files and a lib directory to the application server. These files are required to be updated for certificate authentication for https support.

Procedure

1. Log in to the server as sroot.
2. Copy the following files to the `/opt/AppServer/tomcat/webapps` location:
   - `WorkAssignmentSelfService-x.x.*.war`
   - `runtimeconfig.war`

     You can export the `runtimeconfig.war` file from Avaya Orchestration Designer/ Eclipse.
3. Restart the application server by using one of the following methods:
   - Command line
   - Web interface
4. **(Optional)** If you use the command line method, do the following:
   a. On the command line, type `cd /opt/AppServer/tomcat/bin` and press **Enter**.
   b. Type `./shutdown.sh` and press **Enter**.
   c. After waiting for a few seconds, type `./startup.sh` and press **Enter**.

5. **(Optional)** If you use the web interface method, do the following:
    a. On the Experience Portal Management web console, click **System Management** > **Application Server**.
    b. Select the check box for the application server that you want to restart and click **Stop**.
    c. After waiting for a few seconds, click **Start**.

Upgrading the self-service application

Procedure

1. Log in to the server as sroot.
2. Go to the `/opt/AppServer/tomcat/webapps/WorkAssignmentSelfService-x.x/config` location.
3. Take a backup of the `attributes.xml` file.
4. Go to the `/opt/AppServer/tomcat/webapps` location.
5. Delete the older version of the `WorkAssignmentSelfService-x.x.*.war` file.
6. Copy the new version of the `WorkAssignmentSelfService-x.x.*.war` file to the `/opt/AppServer/tomcat/webapps` location.
7. Go to the `/opt/AppServer/tomcat/webapps/WorkAssignmentSelfService-x.x/config` location.
8. Restore the `attributes.xml` file.
9. **(Optional)** Update the content of the `config.properties` file based on the previously made changes.

Configuring the config.properties file of Self-Service Application

About this task

Use this procedure to configure the `config.properties` file of Self-Service Application (SSA) after deploying SSA on the Experience Portal application server.

Procedure

1. Log in to the server as sroot.
2. Edit the `config.properties` file by typing `vi /opt/AppServer/tomcat/webapps/WorkAssignmentSelfService/config/config.properties`.
3. In the `config.properties` file, do the following:
    a. **(Optional)** In the SpecifiedResource section, add the details of resources in the following format:

    `SpecifiedResource=<NativeResourceId>@<SourceName>`

    For example, SpecifiedResource=8551007@CM41155, 8551008@CM41156, 8551009@CM41157.

<NativeResourceId> specifies the Native Resource ID of the agent and *<SourceName>* specifies the Voice provider name to which the agent is associated. To get the Voice provider name, you must log on to Avaya Control Manager and access the Providers tab on the Avaya Oceana Server Edit page.

Note:

Add the details of resources in this file only if you use the Specified (Required or Preferred) Resource or Coverage feature.

b. Define appropriate values for the following attributes to test queueing to multiple services:

- **Language**
- **Location**
- **Channel**
- **Priority**

c. Define appropriate values for the following parameters:

- **PriorityCustomer** — you can change this to a different number as required for your solution. If a caller enters this number while receiving front-end self-service treatment, the call is treated as a priority call. The agent hears an audible priority tone when the call routes to them.
- **Topic** — use this parameter to tag a contact with a descriptive topic.
- **AccountType** — use this parameter to denote the type of account. For example, “SUBSCRIPTION_ID” or “ACCOUNT_ID”.
- **CRMIdentifier** — use this parameter to supply a reference to an external CRM system.

d. For the **CustomerAPI** parameter, do the following:

- For a Voice and Multimedia deployment of Avaya Oceana®, keep the default value `true`.

  When you keep the default value true, Self-Service Application fetches the CustomerId from the Cache database using OCPDataServices. Self-Service Application then updates the CustomerId in Context Store, so that Customer Journey displays the current interaction and all previous interactions across all channels.

- For a Voice-only deployment of Avaya Oceana®, set the value to `false`.

  When you set the value to false, Customer Journey only displays the current interaction and does not display previous interactions.

Note:

Ensure that you review the `config.properties` file and customize it for your environment. However, for basic sanity checks, you can use the file in its default state.

4. Save the file.

Configuring Work Assignment attributes for Self-Service Application

About this task

Self-Service Application (SSA) has some pre-defined attributes that can be modified, added, or removed. The configured attributes are presented to the customer for attribute selection.

Before you begin

Ensure that you add the Work Assignment attributes in Avaya Control Manager.

Note:

The `config.properties` file of the Self-Service Application lists the attributes for Experience Portal.

Procedure

1. Log in to the server as sroot.
2. Edit the `attributes.xml` file by typing `vi /opt/AppServer/tomcat/webapps/WorkAssignmentSelfService/config/attributes.xml`.
3. To add a new attribute, type the following in the `attributes.xml` file:

```
<value>
<alias>Attribute Alias</alias>
<key>Attribute Value</key>
</value>
```

Note:

Do not add any spaces in Attribute Value and ensure that this value exactly matches the Work Assignment attribute that you configure in Avaya Control Manager. The order of the attributes determines how they are presented to the customer.

`Attribute Alias` specifies the name that TTS server uses to display the prompt to the customer, and `Attribute Value` specifies the value which is forwarded to Work Assignment as a match request for a suitable agent.

Adding Self-Service Application in Experience Portal

Procedure

1. On the Experience Portal Management web console, click **System Configuration** > **Applications**.
2. On the Applications page, click **Add**.
3. In the **Name** field, specify a name for the application.

4. In the **VoiceXML URL** field, enter the following URI:

   `http://<AppServer IP address>:7080/WorkAssignmentSelfService/Start`

   <AppServer IP address> is the IP address of the application server hosting the Self-Service Application.
5. Click **Verify** to ensure it is deployed correctly.
6. In the Speech Servers area, do the following:
   a. In the **TTS** field, select the speech server that you configured on the Speech Servers page.
   b. Move the required value from **Voices** list to **Selected Voices** list.
7. In the Application Launch area, do the following:
   a. In the **Called Number** field, enter a number that must be dialed to start the application.
   b. Click **Add**.
8. Click **Advanced Parameters** and do the following:
   a. Set **Generate UCID** to `Yes`.
   b. Set **Operation Mode** to `Shared UUI`.
   c. Set **Transport UCID in Shared Mode** to `Yes`.
9. Click **Save**.
10. On the Experience Portal Management web console, click **System Configuration** > **Applications**.
11. Click the **Edit** icon next to the application that you created.
12. Specify the following values for DataCenter1:
    a. In the **Data Center 1: Name** field, enter the name of the data center.
    b. In the **Data Center 1: Assisted Service Destination** field, enter the Ingress VDN in the following format:

       `sip:8284100@domain.com`
    c. In the **Data Center 1: Fallback Destination** field, enter the Fallback VDN in the following format:

       `sip:8284103@domain.com`
    d. In the **Data Center 1: Work Assignment Cluster IP** field, enter the FQDN or IP address of Avaya Oceana® Cluster 1.
    e. In the **Data Center 1: Context Store Cluster IP** field, enter the FQDN of Avaya Oceana® Cluster 1 or the FQDN of your standalone Context Store cluster if your solution includes standalone Context Store.
    f. In the **Data Center 1: Customer Management Cluster IP** field, enter the FQDN of Avaya Oceana® Cluster 1.

g. In the **Data Center 1: Unified Collaboration Model Cluster IP** field, enter the FQDN or IP address of Avaya Oceana® Cluster 1.

h. Select the **Use Secure Connection** check box if the connection between Experience Portal and Avaya Oceana® is secure.

13. Click **Save**.
14. Restart the application server using **System Management** > **Application Server**.

Importing the sample application project in Orchestration Designer

Before you begin

- Install the Avaya Oceana® Pluggable Data Connector (PDC) plug-in and the Context Store Pluggable Data Connector (PDC) plug-in on the Orchestration Designer system where the sample application is being imported. For information about installing the Avaya Oceana® Pluggable Data Connector (PDC) plug-in, see Installing or Upgrading Avaya Oceana Pluggable Data Connector plug-in on page 313. For information about installing the Context Store PDC plug-in, see *Avaya Context Store Snap-in Developer Guide*.
- Download the zip file containing the source code for the WorkAssignmentSelfService sample application from the Avaya DevConnect portal at http://www.avaya.com/devconnect.

  For information about Avaya DevConnect, see *Avaya DevConnect Program Guide* available on https://support.avaya.com.
- Unzip the file to extract the sample application.

Procedure

1. On the Orchestration Designer system, start the Eclipse application.
2. Click **File** > **Import**.
3. Click **General** > **Existing Project into Workspace** and click **Next**.
4. Enable the **Select root directory** option.
5. Browse to the directory where you have extracted the sample applications.
6. Select the `WorkAssignmentSelfService` folder and click **Finish**.
7. On the Runtime Version Mismatch window, click **OK**.
8. Ensure that the Avaya Oceana® PDC plug-in and the Context Store PDC plug-in are enabled for application.
9. In the Properties for WorkAssignmentSelfService dialog box, select **Orchestration Designer**.
10. On the Orchestration Designer pane, click the **Pluggable Connectors** tab.
11. In the **Available Connectors** list, enable the **Context Store Connector** and the **Oceana Services Connector** by clicking the Enabled check box.
12. Click **OK**.

    The Context Store PDC plug-in can be used with the default settings. For information about the advanced settings of the plug-in, see *Avaya Context Store Snap-in Reference*.

Note:

Ensure that the machine where you want to install the Avaya Oceana® PDC plug-in and the Context Store PDC plug-in can resolve Avaya Oceana® Cluster 1 IP address. If DNS is not set up on the machine, you must add Avaya Oceana® Cluster 1 IP address in the hosts file.

For information about the Avaya Oceana® PDC plug-in, see section “Oceana Pluggable Data Connector (PDC)” and the “Oceana PDC Help jar” available on http://www.devconnectprogram.com

For information about the Context Store PDC plug-in, see *Avaya Context Store Snap-in Developer’s Guide*.

Next steps

Customize the Avaya Oceana® sample Self-Service Application to your requirements using the Orchestration Designer flows.

Avaya Oceana® PDC provides the APIs required for integration with Context Store from the Avaya Oceana® sample Self-Service Application. Additional Context Store functionality is provided by the Context Store PDC plug-in.

For more information, see:

- *Getting Started with Avaya Orchestration Designer*
- *Avaya Orchestration Designer Developer’s Guide*
- *Administering Avaya Experience Portal*
- *Avaya Context Store Snap-in Developer’s Guide*
- Avaya Oceana® PDC Help jar

Installing or Upgrading Avaya Oceana® Pluggable Data Connector plug-in

Procedure

1. Open Orchestration Designer.

   The speech perspective must be open to configure the Context Store PDC.

2. Select **Window** > **Perspective** > **Open Perspective** > **Speech in Orchestration Designer**.
3. Right-click **Project** > **Properties**, in the Avaya Orchestration Designer Navigator window and open the properties for each project open in Orchestration Designer.
4. On the **Pluggable Connector** tab, locate **Oceana Services**.If there is no Oceana Services Pluggable Connector in the list, close Orchestration Designer and proceed to step 10.
5. If the **Oceana Services Pluggable Connector** is enabled, un-deploy the existing plug-in by un-checking the enabled check box.
6. Select **Apply and Close**.

   Complete this step for each project that is open in Orchestration Designer and then close Orchestration Designer.

7. From the plug-in folder located at `C:\ AAOD\eclipse\plugins`, check if there is an existing Oceana PDC plug-in jar in the eclipse plug-in folder and delete it.

   Note:

   If there was an Oceana PDC in the list of Pluggable Connectors, but not enabled on any open project, the existing plug-in must be deleted from the plug-ins folder.

8. Start Orchestration Designer without any Oceana PDC plug-in jar in `C:\ AAOD\eclipse\plugins`.
9. Close Orchestration Designer.

   Note:

   If steps 8-9 are not present you may encounter an issue where the 'Oceana Services' connector is absent from the Pluggable Connectors tab mentioned in step 4. In that case Eclipse cache invalidation is required. E.g. AOD has to be run with "-clean" parameter using the following steps:

   a. Press the **Windows Start** button
   b. Type the **Command** prompt.
   c. Click **Command** prompt.
   d. Navigate to Eclipse install folder for example: `C:\AOD-8.1\eclipse`.
   e. Enter **eclipse.exe -clean** and click **return**.

   For example: `C:\AOD-8.1\eclipse>eclipse.exe -clean`.

10. Copy the new Oceana PDC plug-in jar into the plug-in folder located at `C:\ AAOD\eclipse\plugins`.
11. Start Orchestration Designer.
12. To deploy the Oceana PDC plug-in, do the following:

    a. Right-click on the relevant project in the Avaya Orchestration Designer Navigator window.
    b. Navigate to **Orchestration Designer** > **Pluggable Connectors** tab.
    c. Select the **Oceana Services Pluggable Connector** enabled check box.
    d. Click **Apply and Close**.

Exporting the sample application project

Before you begin

Stop the Tomcat server on the Avaya Orchestration Designer system.

Procedure

1. On the File menu, click **Export**.

2. In the Export wizard window, double-click **Avaya OD Development**.
3. Click **Export Orchestration Designer Speech** project.
4. Click **Next**.
5. In the Export orchestration Designer Project wizard, on the Specify Export Parameters page, select `WorkAssignmentSelfService` project and specify the directory where you want to export the project.
6. Click **Next**.
7. On the Specify Deployment Parameters page, select the **Include extra files and folder** option.
8. In the Select Resource window, select **config**.

   The sample application comes with external configuration files that have pre-defined editable attributes.
9. Click **OK**.
10. Click **Next**.
11. Click **Finish**.

Configure Avaya Aura® Call Center Elite

In an Avaya Oceana®, you can configure Avaya Aura® Call Center Elite to provide front-end IVR for voice calls.

This section uses a worked example to describe how Elite IVR can use a number of sample prompts and the default vector to collect data from callers. You can use the sample Elite IVR Self Service workflow to test voice calls using Avaya Aura® Call Center Elite to provide front-end IVR.

Elite IVR supports multiple Self Service menus. You must define these menus in the Extract Attributes task of the Engagement Designer Elite IVR workflow. For example in the US, you want your prompt to say “Press 1 for English, 2 for Spanish”, whereas in Brazil you want your prompt to say “Press 1 for Portuguese, 2 for Spanish, 3 for English”. Your schema name defines which menu structure within the XML to use. You must also define the schema names for each menu in the Work Assignment Attributes property of Engagement Designer. The name of the default MenuSchema in the sample Elite IVR workflow is “SelfService1”.

For more information about configuring Avaya Oceana® tasks in Engagement Designer, see *Avaya Engagement Designer Developer’s Guide*, available from the Avaya Support website at http://support.avaya.com.

Adding Communication Manager as a trusted node on Avaya Aura® Media Server

About this task

Avaya Aura® Media Server processes SIP traffic from trusted nodes. Therefore, you must add Communication Manager as a trusted node on Avaya Aura® Media Server.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **System Configuration**.
3. Click **Signaling Protocols** > **SIP** > **Nodes and Routes**.
4. On the SIP Nodes and Routes page, in the Trusted Nodes section, click **Add**.
5. On the Add SIP Trusted Node page, enter the host name or server IP address of Communication Manager that you want to add as a trusted node.
6. Click **Save**.

Adding a node name for Avaya Aura® Media Server on Communication Manager

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change node-names ip`**.
3. On the IP NODE NAMES screen, specify the node name and IP address of Avaya Aura® Media Server.
4. Save the settings.

Creating a signaling group for Avaya Aura® Media Server

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`add signaling-group n`**.

   n is the number of the signaling group that you need to specify.
3. On page 1 of the SIGNALING GROUP screen, perform the following steps:
   a. In the **Group Type** field, type `sip`.
   b. In the **Transport Method** field, set the method of transport as `tcp` or `tls`.
   c. In the **Peer Detection Enabled** field, type `n`.
   d. In the **Peer Server** field, type `AMS`.
   e. In the **Near-end Listen Port** field, type `5060` or `5061` based on the method of transport that you set.
   f. In the **Far-end Node Name** field, enter the node name of Avaya Aura® Media Server that you created.
   g. In the **Far-end Listen Port** field, type `5060` or `5061` based on the method of transport that you set.

4. On page 2 of the SIGNALING GROUP screen, perform the following steps:
   a. In the **Enable on the main Processor (s)** field, type `y`.
   b. In the **Enable on Survivable Processors (ESS and LSP)** field, type `all`.
5. Save the settings.

Creating a media server on Communication Manager

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`add media-server n`**.
3. On the MEDIA SERVER screen, perform the following steps:
   a. In the **Signaling Group** field, type the number of the signaling group that you created for Avaya Aura® Media Server.
   b. In the **VoIP Channel License Limit** field, specify a value to limit the number of channels that can be established on the specified media server.
4. Save the settings.

Configuring Avaya Aura® Media Server media files for Elite IVR

About this task

Avaya provides a sample Engagement Designer workflow for Voice Self Service provided by Avaya Aura® Call Center Elite. This workflow uses Avaya Aura® Media Server to play media files and provide front-end IVR. This procedure describes how to deploy sample media files for Voice Self Service. The sample media files available for Voice Self Service are:

Announcement	Media file name
Welcome	`WelcomeCustomer.wav`
Service	`Service.wav`
Language	`Language.wav`
Directing	`Directing.wav`
Wait music	`Wait.wav`

Note:

These media files are available to download from the Avaya DevConnect portal at http://www.avaya.com/devconnect. For information about downloading Avaya Oceana® resources from Avaya DevConnect, refer to the Avaya Oceana® Release Notes.

Before you begin

Ensure that you have the Engagement Designer workflow for Voice Self Service and the accompanying Avaya Aura® Media Server media files.

Procedure

1. In your web browser, enter the following URL:

   `https://<Avaya Aura Media Server_FQDN>:8443/em`
2. In the **User ID** field, enter the User ID for logging in to Avaya Aura® Media Server.
3. In the **Password** field, enter the password for logging in to Avaya Aura® Media Server.
4. Click **Log in**.
5. In the navigation pane, click **Tools** > **Media Management**.
6. On the Media Management page, select the **Communication Manager** check box.
7. Click **Browse**.
8. On the Provision Media page, expand the Communication Manager content namespace.
9. Select the content group to which you want to add a media file.
10. Click **Add Media**.
11. In the Add Media dialog box, click **Browse** and navigate to the sample media files.
12. Select a file and click **Upload**.
13. Continue uploading all the media files to the Communication Manager content namespace.

Creating announcements on Communication Manager

Before you begin

In Avaya Aura® Media Server, create a content namespace for Communication Manager and then add the sample media files available for Voice Self Service to the namespace:

Announcement	Media file name
Welcome	`WelcomeCustomer.wav`
Service	`Service.wav`
Language	`Language.wav`
Directing	`Directing.wav`
Wait music	`Wait.wav`

These media files are available to download from the Avaya DevConnect portal at http://www.avaya.com/devconnect. For information about downloading Avaya Oceana® resources from Avaya DevConnect, refer to the Avaya Oceana® Release Notes.

Note:

If you use a Media Gateway, you can use the standard procedure to upload the media files.

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.

2. Perform the following steps to create the Welcome announcement:
    a. Run **add announcement <Welcome_Annc_Extn_Number>**.
    b. In the **Annc Name** field, enter the name of the Welcome announcement file that you loaded on Avaya Aura® Media Server.
    c. In the **Annc Type** field, type `integrated`.
    d. Press **Enter**.
    e. In the **Source** field, enter the appropriate value for the Avaya Aura® Media Server where you loaded the Welcome announcement file.

       For example, `M1`.
    f. In the **COR** and **TN** fields, enter appropriate values based on your environment.
    g. Save the settings.
3. Perform the following steps to create the Service announcement:
    a. Run **add announcement <Service_Annc_Extn_Number>**.
    b. In the **Annc Name** field, enter the name of the Service announcement file that you loaded on Avaya Aura® Media Server.
    c. In the **Annc Type** field, type `integrated`.
    d. Press **Enter**.
    e. In the **Source** field, enter the appropriate value for the Avaya Aura® Media Server where you loaded the Service announcement file.

       For example, `M1`.
    f. In the **COR** and **TN** fields, enter appropriate values based on your environment.
    g. Save the settings.
4. Perform the following steps to create the Language announcement:
    a. Run **add announcement <Language_Annc_Extn_Number>**.
    b. In the **Annc Name** field, enter the name of the Language announcement file that you loaded on Avaya Aura® Media Server.
    c. In the **Annc Type** field, type `integrated`.
    d. Press **Enter**.
    e. In the **Source** field, enter the appropriate value for the Avaya Aura® Media Server where you loaded the Language announcement file.

       For example, `M1`.
    f. In the **COR** and **TN** fields, enter appropriate values based on your environment.
    g. Save the settings.

5. Perform the following steps to create the Directing announcement:
   a. Run **add announcement <Directing_Annc_Extn_Number>**.
   b. In the **Annc Name** field, enter the name of the Directing announcement file that you loaded on Avaya Aura® Media Server.
   c. In the **Annc Type** field, type `integrated`.
   d. Press **Enter**.
   e. In the **Source** field, enter the appropriate value for the Avaya Aura® Media Server where you loaded the Directing announcement file.

      For example, `M1`.
   f. In the **COR** and **TN** fields, enter appropriate values based on your environment.
   g. Save the settings.
6. Perform the following steps to create the Music announcement:
   a. Run **add announcement <Music_Annc_Extn_Number>**.
   b. In the **Annc Name** field, enter the name of the Music announcement file that you loaded on Avaya Aura® Media Server.
   c. In the **Annc Type** field, type `integ-mus`.
   d. Press **Enter**.
   e. In the **Source** field, enter the appropriate value for the Avaya Aura® Media Server where you loaded the Music announcement file.

      For example, `M1`.
   f. In the **COR** and **TN** fields, enter appropriate values based on your environment.
   g. Save the settings.

Creating variables on Communication Manager

About this task

Communication Manager vectors use variables to improve efficiency. Different types of variables are available to meet different types of call processing needs. Vector variables can be added to consider location, messaging, and adjunct routing vector steps. Based on the variable type, variables can use call-specific data or fixed values that are identical for all calls. In either case, an administered variable can be reused in many vectors.

If the variables used in this example are already in use on Communication Manager, use different variables. Ensure that you use these different variables in your Avaya Oceana® vectors.

Important:

Use variables E - I to provide Call Center Elite Voice Self Service.

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.

2. Use the **change variables** command.
3. Create variables E to I as shown below:

```
change variables                                          Page   1 of  39
                              VARIABLES FOR VECTORS

Var Description                 Type    Scope Length Start Assignment      VAC
A   Adjunct Route Digits        collect L     16     1
B   Adjunct Route Flag          collect P     1      1
C   ASAI Data                   asaiuui L     2      1
D
E   Collected Digits I          collect L     6      1
F   Collected Digits II         collect L     1      1
G   Collected Digits III        collect L     1      1
H   Collected Digits Concat     collect L     8      1
I   Collected Digits UUI        asaiuui L     8      1
J
K   Expected Wait Time          collect L     5      1
L
M
N
O   Oceana Routing              collect P     1      1
P
Q   Oceana In Service           value   G     1            1              VV1
R
```

4. Save the settings.

Creating the SelfService Vector Directory Number

About this task

Use this procedure to create the SelfService Vector Directory Number (VDN).

Procedure

1. Run **add vdn next** or **add vdn n**.

   n is the extension that you want to use for the VDN.
2. On page 1 of the VECTOR DIRECTORY NUMBER screen, perform the following steps:
   a. In the **Name** field, enter the name of the VDN.
   b. In the **Destination** field, set the destination to a vector number which is not in use.
   c. In the **1st Skill*** field, enter the Hunt Group that you created for Oceana agents. This example uses the Oceana Agent Pool Hunt Group, 828.
3. Save the settings.

Configuring a vector for the SelfService VDN

About this task

Use this procedure to configure a vector for the SelfService VDN.

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the SelfService VDN.
3. On page 1 of the CALL VECTOR screen, perform the following steps:
   a. In the **Name** field, enter the name of the vector as `SelfService Vector`.

      This standard name makes maintenance and troubleshooting easier.
   b. Enter the details required from line 01 to line 41 as shown below:

```
display vector 8                                          Page   1 of   6
                                CALL VECTOR

    Number: 8                Name: SelfService Vector
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 set           B      = none   CATR  1
02 wait-time     1   secs hearing ringback
03
04 #    Interview Caller
05 collect       6    digits after announcement 8289988  for E
06 goto step     5              if E                =      none
07
08 #    Optional steps to zero-pack account number
09 goto step     24             if E                >      99999
10 goto step     22             if E                >      9999
11 goto step     21             if E                >      999
12 goto step     20             if E                >      99

                      Press 'Esc f 6' for Vector Editing
```

```
display vector 8                                                Page   2 of   6
                                  CALL VECTOR
13 goto step     19            if E                 >      9
14 goto step     17            if E                 =      none
15 goto step     17            if E                 =      #
16 goto step     18            if E                 <=     9
17 set           E      = E      CATL  0
18 set           E      = E      CATL  0
19 set           E      = E      CATL  0
20 set           E      = E      CATL  0
21 set           E      = E      CATL  0
22 set           E      = E      CATL  0
23
24 collect       1    digits after announcement 8289986  for F
25 goto step     24            if F                 =      none
26 collect       1    digits after announcement 8289985  for G
27 goto step     26            if G                 =      none
28 set           H      = none   CATR  E
29 set           H      = H      CATR  F
30 set           H      = H      CATR  G
31 set           I      = none   CATR  H
32
```

```
display vector 8                                                Page   3 of   6
                                  CALL VECTOR
33 announcement 8289980
34
35 #    Capture Oceana context
36 adjunct       routing link 1
37 wait-time     10  secs hearing 8289987  then silence
38 goto step     37            if unconditionally
39
40 #    Oceana encountered error
41 route-to      number 8284103          with cov n if unconditionally
42
43
44
45
46
47
48
49
50
51
52
```

The sample workflow and default vector supports three prompts. The first prompt collects a 6-digit customer ID and the other two prompts collect a single-digit routing attribute. Replace these lines as required for your solution. If there is a routing failure at any point during the call, the call routes to the fallback VDN and the configured fallback Elite skill.

4. Save the settings.

Adding the SelfService VDN to Avaya Control Manager

About this task

Use this procedure to add the Self Service VDN for Call Center Elite IVR.

Before you begin

- Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.
- Run ACM Synchronizer to push the SelfService VDN to Avaya Control Manager.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Server Details**.
2. On the Avaya Oceana Server List page, double-click the UCAServer server.
3. Select the **VDN** tab.
4. In the **Avaya Oceana VDN Type** field, select **Self Service**.
5. Move the single required SelfService VDN from the **CM VDNs** list to the **Selected** list.
6. Click **Save**.

Deploying the sample Elite IVR SelfService workflow

About this task

This procedure describes how to deploy the sample workflow that provides callers with front-end IVR using Call Center Elite. The sample Elite IVR Self Service workflow uses the data Call Center Elite and the SelfService vector collects from the caller, before using this data to route the call. The sample workflow uses the sample media files previously uploaded to Avaya Aura® Media Server.

If call routing fails, the sample configuration ensures that the call defaults to the Fallback VDN.

Before you begin

- Download the latest version of the sample workflow from the Avaya DevConnect portal at http://www.avaya.com/devconnect. For information about downloading Avaya Oceana® resources from Avaya DevConnect, refer to the Avaya Oceana® Release Notes.
- Deploy and configure the OceanaVoiceAssistedService workflow.
- In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Designer Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.

3. In the Import Workflow dialog box, click **Choose File**.
4. Browse to the folder containing the sample workflow, select the workflow, and click **Import**.
5. Click **Save Workflow**.
6. In the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaVoiceSelfService`.

      You can provide any name for the workflow.

   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.
8. In the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`
10. On the Workflows tab, verify that the OceanaVoiceSelfService and OceanaVoiceAssistedService workflows are available in the list of deployed workflows.
11. On the Workflows tab, select the SelfService workflow and click **Attributes**.
12. In the Workflow Attributes dialog box, in the **AssistedServiceDestination** field, enter the value in the following format:

    <Number>@*<Domain.com>*

    The *<Number>* is the Ingress VDN that you created previously. For example, 8284100@domain.com.
13. In the **Locale** field, replace the default value `en_us` with the required value.
14. In the **DataCenter** field, replace the default value `DataCenter1` with the value that is applicable for your data center.
15. In the **MenuSchema** field, replace the default value `SelfService1` with the required value. This name must match the name of the Menu Schema defined in Engagement Designer.
16. In the **Priority** field, replace the default value `5` with the required value.
17. In the **PriorityCustomer** field, replace the default value `456789` with the required value. The sample application uses this number to allow callers to generate a priority 1 contact.

    You can use a comma-separated list of values to add multiple priority customers.
18. In the **Strategy** field, replace the default value `Most Idle` with the required value.

19. In the **UseCustomerManagement** field, do the following:
    - For a Voice and Multimedia deployment of Avaya Oceana®, keep the default value `True`.
    - For a Voice-only deployment of Avaya Oceana®, replace the default value `True` with the value `False`.

      When you set the value to `False`, Customer Journey only displays the current interaction and does not display previous interactions.
20. To create a routing rule for the OceanaVoiceSelfService workflow, click the **Routing** tab.
21. Click **Create**.
22. In the **Select event** field, select **ROUTE_CONTACT_VOICE**.
23. In the **Select workflows** field, select the OceanaVoiceSelfService workflow.

    Note:

    Ensure that you click the workflow ending with the term `Latest`. For example, `OceanaVoiceSelfService:Latest`.
24. In the **Enter Rule Name** field, type a name for the rule.

    For example, type `Elite SelfService`.
25. Click **Add Rule**.
26. In the **Select schema attribute** field, select **RouteContact.WorkflowType:string**.
27. In the **Select function** field, click **is equal to**.
28. In the **Enter value** field, type `SelfService`.
29. Click **Save**.

    Engagement Designer displays the newly created rule in the list of rules.

    When you create a routing rule for the OceanaVoiceSelfService workflow, Engagement Designer automatically creates the `default` rule to ensure that the new OceanaVoiceSelfService workflow does not affect the normal OceanaVoiceAssistedService workflow. Avaya recommends that you rename the `default` rule as `AssistedService`.

    Note:

    Engagement Designer creates the `default` rule only at the first instance of adding a rule for an event. Ensure that you set the default rule to **not equal to**.

Customizing Engagement Designer attributes for Elite IVR Self Service

About this task

This procedure describes how to customize the sample Elite IVR workflow and vectors to meet the requirements of your solution. This example describes how to collect 4 digits from the caller during front-end IVR, instead of the default value of 6 digits, using a second Self Service menu.

Elite IVR supports multiple Self Service menus. You must define these menus in the Extract Attributes task of the Engagement Designer Elite IVR workflow. For example in the US, you want your prompt to say “Press 1 for English, 2 for Spanish”, whereas in Brazil you want your prompt to say “Press 1 for Portuguese, 2 for Spanish, 3 for English”. Your schema name defines which menu structure within the XML to use. You must also define the schema names for each menu in the Work Assignment Attributes property of Engagement Designer. In this example procedure the ‘SelfService2’ menu collects 4 digits.

For more information about configuring Avaya Oceana® tasks in Engagement Designer, see *Avaya Engagement Designer Developer’s Guide*, available from the Avaya Support website at http://support.avaya.com.

Procedure

1. Log on to the System Manager web console.
2. Click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
3. On the Service Clusters tab, from the **Cluster** list select Avaya Oceana® Cluster 1.
4. From the **Service** list, select **EngagementDesigner**.
5. From the list of DEFAULT_GROUP attributes, navigate to **Work Assignment Attributes**.
6. Edit the **Work Assignment Attributes** property as required for your solution. For example, define a second menu to collect 4 digits. You can then configure the workflow to use this menu.

```
<?xml version="1.0" encoding="UTF-8"?>
<recipe>
    <schema name="SelfService1" startposition="1">
        <segment type="customerid" digits="6"/>
        <segment type="category" digits="1">
Service
</segment>
        <segment type="category" digits="1">
Language
</segment>
        <category name="Service">
            <value name="SalesSupport" value="1"/>
            <value name="CorporateAccounts" value="2"/>
            <value name="TechnicalSupport" value="3"/>
        </category>
        <category name="Language">
            <value name="English" value="1"/>
            <value name="Spanish" value="2"/>
            <value name="French" value="3"/>
            <value name="Italian" value="4"/>
            <value name="German" value="5"/>
            <value name="Gaeilge" value="6"/>
            <value name="Irish" value="7"/>
        </category>
    </schema>
    <schema name="SelfService2" startposition="1">
        <segment type="customerid" digits="4"/>
        <segment type="category" digits="1">
Department
</segment>
        <segment type="category" digits="1">
Location
</segment>
        <category name="Department">
```

```
            <value name="Sales" value="1"/>
            <value name="Finance" value="2"/>
            <value name="Design" value="3"/>
        </category>
        <category name="Location">
            <value name="Inhouse" value="1"/>
            <value name="South" value="2"/>
            <value name="East" value="3"/>
            <value name="West" value="4"/>
        </category>
    </schema>
</recipe>
```

7. Click **Commit**.

Next steps

To support using a second menu for 4 digit collection, you must add a second Self Service VDN, vector, and then add the new VDN to Avaya Control Manager. Ensure that the second vector collects 4 digits in the “Interview” section. You must also add another set of corresponding variables to collect digits for the second menu, and ensure that these variables hold the correct number of digits. To create these configuration items, repeat the following procedures and edit the values as required to collect 4 digits:

- Creating variables on Communication Manager on page 320
- Creating the SelfService Vector Directory Number on page 321
- Configuring a vector for the SelfService VDN on page 321
- Adding the SelfService VDN to Avaya Control Manager on page 324

Chapter 19: Configure Callback Assist

Callback Assist overview

Callback Assist integrates with Avaya Oceana® at the callback state. Instead of having Callback Assist and Experience Portal bridged into the call throughout, Callback Assist integration occurs from within the Treatment vector.

Calls are initially front-ended and then transferred to Call Center Elite for assisted service. If no agent is available, calls are given advanced wait treatment using Communication Manager vectoring. Callers are periodically presented with the option to leave a voice mail or request a callback. After a caller selects the callback option, the call is routed to Callback Assist where Immediate or Scheduled callback options are selected and the call is dropped.

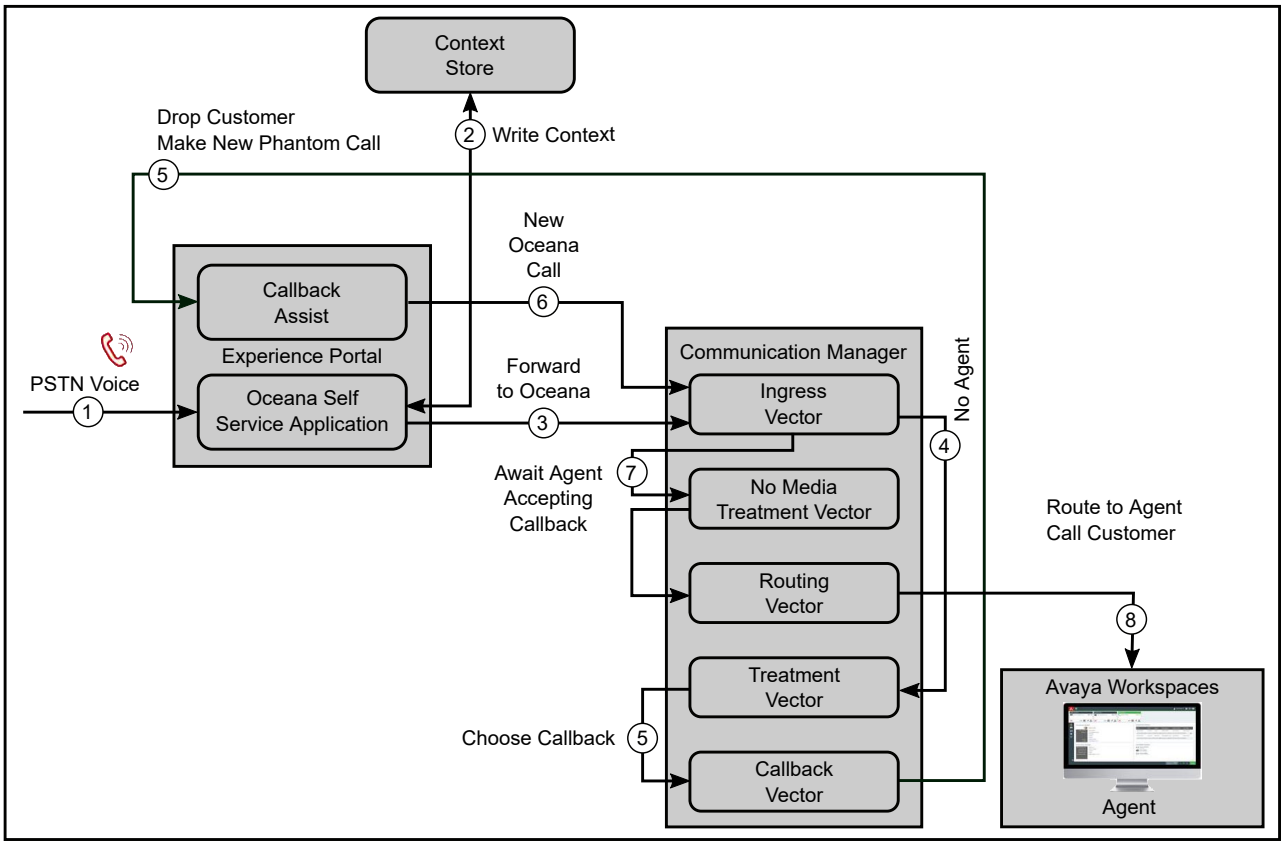
For the Immediate callback option, Callback Assist makes a new media-less call to Avaya Oceana® for routing to a suitable agent. After the agent answers the call, the customer is out-dialed and connected to the agent.

The callback call from Callback Assist must not receive any media treatment while awaiting an agent. If media is accidentally provided, it establishes the dialog from a SIP perspective, and Callback Assist treats this as an agent answer. Therefore, you must configure a No Media treatment vector. The No Media treatment VDN is used when the incoming call is a callback, as opposed to a regular customer call.

From the agent and customer, the first party whom Callback Assist must call depends on an install-time option that cannot be changed through configuration. You can change this option only through an upgrade.

Callback Assist currently supports PSTN Voice, but does not support Web Voice and Web Video.

The following diagram depicts the Callback Assist flow:



Prerequisites for configuring Callback Assist

To configure Callback Assist, you must install the Callback Assist application server. For installation instructions, see *Installing and Configuring Avaya Callback Assist*.

Creating a Web Service user in Experience Portal

About this task

Use this procedure to create a Web Service user in Experience Portal for creating a site definition in Avaya Callback Assist Administration.

Procedure

1. Log on to the Experience Portal Manager (EPM) interface.
2. In the navigation pane, click **User Management** > **Users**.
3. On the Users page, click **Add**.

The interface displays the Add User page.

4. In the **Name** field, type a name for the user.
5. In the **Roles** field, select the **Web Services** check box.
6. In the **Password** field, type a password.
7. In the **Verify Password** field, retype the same password.
8. Click **Save**.

Logging on to the Avaya Callback Assist Administration interface

About this task

Use this procedure to log on to the Avaya Callback Assist Administration interface.

Procedure

1. Enter the following URL in your web browser:

   `http://<IP address of the Callback Assist server>/admin`
2. In the **Username** field, enter the user name of the Callback Assist server.
3. Click **Submit**.
4. In the **Password** field, enter the password of the Callback Assist server.
5. Click **Logon**.

Creating a site definition

About this task

Use this procedure to create a site definition in Avaya Callback Assist Administration to link Callback Assist to Experience Portal.

Before you begin

Create a Web Service user in Experience Portal Manager (EPM).

Procedure

1. Log on to the Avaya Callback Assist Administration interface.
2. In the navigation pane, click **Site Definitions**.
3. On the Site Definitions page, click **Add New**.

The interface displays the Add Site dialog box.

4. In the **Site name** field, type a name for the site.
5. Click **Add New**.

   The interface displays the Add Primary EPM dialog box.
6. In the **Outbound Web Service IP Address/Hostname** field, enter the IP address or host name of the EPM server.
7. In the **Outbound Web Service User** field, enter the user name of the Web Service user that you created in EPM.
8. In the **Outbound Web Service Password** field, enter the password of the Web Service user that you created in EPM.
9. **(Optional)** In the **Outbound Web Service Timeout(milliseconds)** field, change the default value based on your requirement.
10. Click **Ok**.
11. In the Add Site dialog box, click **Ok**.
12. On the Site Definitions page, verify the row for the new site.

Taking a note of the Outbound Callback application name

About this task

Use this procedure to note down the name of the Outbound Callback application because this name must match the Experience Portal configuration.

Procedure

1. Log on to the Avaya Callback Assist Administration interface.
2. In the navigation pane, click **Global Settings**.
3. On the Global Settings Management page, select the **IVR** tab.
4. In the **EPM Callback Outbound application name** row, note down the value.

Setting the System ANI parameter

About this task

Use this procedure to set the System ANI parameter. This value specifies the number that the customers see when they receive callbacks. This value must match the number assigned to the Oceana Callback in Experience Portal applications.

Procedure

1. Log on to the Avaya Callback Assist Administration interface.
2. In the navigation pane, click **Global Settings**.
3. On the Global Settings Management page, select the **General** tab.
4. In the **System ANI** row, in the **Actions** column, click the **Edit** icon.

   The interface displays the Configuration Entry dialog box.
5. In the **Value** field, set the value of the System ANI parameter.
6. Click **Ok**.

Setting the Storage URL parameter

About this task

Use this procedure to set the Storage URL parameter. This value specifies the path for storing audio files.

Procedure

1. Log on to the Avaya Callback Assist Administration interface.
2. In the navigation pane, click **Global Settings**.
3. On the Global Settings Management page, select the **Audio** tab.
4. In the **Storage URL** row, in the **Actions** column, click the **Edit** icon.

   The interface displays the Configuration Entry dialog box.
5. In the **Value** field, set the value of the Storage URL parameter in the following format:

   `http://<IP address of the Callback Assist server>:8098/riak`
6. Click **Ok**.

Setting Avaya Oceana®-specific parameters

About this task

Use this procedure to set the parameters that are specific to Avaya Oceana®.

Procedure

1. Log on to the Avaya Callback Assist Administration interface.
2. In the navigation pane, click **Oceana Configuration**.

The interface displays the Oceana Configuration page.

3. For each of the following parameters, click the corresponding **Edit** icon, set the appropriate value, and click **Ok**:

Parameter	Example value
Default Oceana Ingress VDN	The Ingress VDN that you configured while configuring wait treatments for Voice contacts.
Extended Context Lease Time (in minutes)	5
Oceana Context Store Touch Point Label	Voice__CallbackAttempted
Oceana Core Data Service REST API Connection Timeout (in milliseconds)	4000
Oceana Core Data Service REST API IP Address/Hostname	The IP address or FQDN of the cluster that hosts the OceanaCoreDataService snap-in.
Oceana Core Data Service REST API Port Number	443
Work Assignment REST API Connection Timeout (in milliseconds)	4000
Work Assignment REST API IP Address/ Hostname	The IP address or FQDN of the cluster that hosts the Work Assignment snap-in.
Work Assignment REST API Port Number	443

Creating a callback configuration

About this task

Use this procedure to create a callback configuration for Avaya Oceana®.

Procedure

1. Log on to the Avaya Callback Assist Administration interface.
2. In the navigation pane, click **Callback Configurations**.
3. On the Callback Configuration Management page, click **Add New**.

   The interface displays the Create Callback Configuration dialog box.
4. Keep the default **Voice** option selected and click **Next**.

   The interface displays the Add Voice Callback Configuration dialog box.
5. In the **Name** field, type a name for the callback configuration.
6. Select the **Oceana** check box.
7. In the **DNIS** field, enter the initial Vector Directory Number (VDN), service number, or externally-determined route that receives customer calls.

8. In the **Oceana Ingress VDN** field, enter the Ingress VDN of Avaya Oceana® to queue calls.
9. In the following fields, enter the appropriate value:

Field	Example value
Minimum EWT Threshold(minutes)	0
Maximum EWT Threshold(minutes)	600
Maximum Call Error Attempts	1
Maximum Call Busy Attempts	1
Maximum Call No Answer Attempts	1
Maximum Total Attempts	1

10. Select the **Validate ANI** check box.
11. Select the **Prompt for ANI confirmation** check box.
12. Clear the **Announce EWT** check box.
13. Clear the **Always Announce EWT** check box.
14. To configure holidays, do the following:
    a. Select the **Availability** tab.
    b. In the Configure Callback Availability area, click the **Configure** column for Sunday.

       The interface displays the Configure Day: Sunday dialog box.
    c. Clear the **Not Used** check box.
    d. In the **Slot Interval** field, keep the default value `30`.
    e. In the **Call Center Start Time** field, select `12:00 AM`.
    f. In the **Call Center End Time** field, select `12:00 AM`.
    g. Select the **Enable Immediate Callbacks** check box.
    h. Select the **Enable Scheduled Callback Offer** check box.
    i. Select the **Enable Scheduled Callback Delivery** check box.
    j. In the **Number of Available Scheduled Callbacks to accept per slot** field, type `100`.
    k. Click **Ok**.

       The name of the **Configure** column changes to **Configure 30m Slot**.
    l. Click **Ok**.
    m. Repeat Step b to Step k for the other days of the week.
    n. In the Time Zone Message area, in the **Type** field, select `Audio`.
    o. Click **Choose File**.

p. Browse and select the `eastern_time.wav` file available on the Callback Assist server at `/opt/Avaya/callbackassist/apache-tomcat-ddapps/webapps/CBAPhrases/samples/englishUS/en-us/default`.

q. Click **OK**.

Note:

For scheduled callbacks, each callback configuration can have its own time zone to define time slots. Therefore, you can configure the callback-specific time zones through the fields in the Time one Settings area.

15. To configure announcements, do the following:

a. Select the **Customer** tab.

To configure announcements, you must use the default `Welcome.wav`, `Goodbye.wav`, and `holdmusic.wav` files from the Callback Assist server at `/opt/Avaya/callbackassist/apache-tomcat-ddapps/webapps/CBAPhrases/samples/englishUS/en-us/default`.

b. In the Welcome Message area, in the **Type** field, select `Audio`.

c. Click **Choose File**.

d. Browse and select the `Welcome.wav` file.

e. Click **OK**.

f. In the Goodbye Message area, in the **Type** field, select `Audio`.

g. Click **Choose File**.

h. Browse and select the `Goodbye.wav` file.

i. Click **OK**.

j. In the Customer WTA area, in the **Type** field, select `Audio`.

k. Click **Choose File**.

l. Browse and select the `holdmusic.wav` file.

m. Click **OK**.

n. Select the **Disallow Multiple Pending Requests** check box.

16. To configure agents, do the following:

a. Select the **Agent** tab.

To configure agents, you must use the default `moh.wav` file from the Callback Assist server at `/opt/Avaya/callbackassist/apache-tomcat-ddapps/webapps/CBAPhrases/samples/englishUS/en-us/default`.

b. In the Agent Prompt Language and Format area, select the **24hs format** option.

c. Select the **Enable Call Auto Launch** check box.

d. In the Agent WTA Message area, in the **Type** field, select `Audio`.

e. Click **Choose File**.

f. Browse and select the `moh.wav` file.

g. Click **OK**.

17. Click **Ok**.
18. On the Callback Configuration Management page, verify the row for the new callback configuration.

Configuring the default Line of Business configuration

About this task

Use this procedure to configure the default Line of Business (LOB) configuration to assign all available ports to the default LOB.

This configuration is required for Callback Assist 4.7 and later versions.

Procedure

1. Log on to the Avaya Callback Assist Administration interface.
2. In the navigation pane, click **LOB Configurations**.

   The interface displays the Line of Business Configurations page.
3. In the **DefaultLOB** row, in the **Actions** column, click the **Edit** icon.

   The interface displays the Edit LOB dialog box.
4. In the **Associate Callback Configurations** field, type the name of the callback configuration that you created for Avaya Oceana®.
5. Click **Ok**.

Exporting the Avaya Oceana® Cluster 1 certificate

About this task

Use this procedure to export the Avaya Oceana® Cluster 1 certificate to your local machine.

Note:

All three nodes of Avaya Oceana® Cluster 1 generally have the same identity certificate. Therefore, you can export the certificate from node 1 of the cluster. However, if all three nodes have different identity certificate, then you must export the certificate from each node and import it to Callback Assist Administration.

Procedure

1. Log on to the System Manager web console.
2. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
3. On the Manage Elements page, select the check box for an Avaya Oceana® Cluster 1 node, and click **More Actions** > **Manage Identity Certificates**.
4. On the Manage Identity Certificates page, select **securitymodule_http** and click **Export**.
5. Save the `.pem` file on your local machine.

Importing certificates to Callback Assist

About this task

Use this procedure to import the following certificates to Callback Assist:

- Avaya Oceana® Cluster 1 certificate
- System Manager or third-party root certificate

Before you begin

Export the Avaya Oceana® Cluster 1 certificate.

Procedure

1. In your web browser, enter the following URL:

   `http://<IP address of the Callback Assist server>:8080/runtimeconfig/`

2. In the **Username** field, type `ddadmin`.

   `ddadmin` is the default user name for the first time.

3. In the **Password** field, type `ddadmin`.

   `ddadmin` is the default password for the first time.

4. Click **Login**.
5. In the navigation pane, click **Certificates**.
6. On the Certificates page, import the Avaya Oceana® Cluster 1 and System Manager or third-party root certificates.

Deploying the OceanaCallback application

About this task

You can deploy the OceanaCallback sample application by copying its `.war` file to the application server.

Procedure

1. Log in to the server as sroot.
2. Copy the `OceanaCallback.war` file to the `/opt/AppServer/tomcat/webapps` location.
3. Restart the application server using one of the following methods:
   - Command line
   - Web interface
4. If you use the command line method, do the following:
   a. On the command line, type `cd /opt/AppServer/tomcat/bin` and press **Enter**.
   b. Type `./shutdown.sh` and press **Enter**.
   c. After waiting for a few seconds, type `./startup.sh` and press **Enter**.
5. If you use the web interface method, do the following:
   a. On the Experience Portal Management web console, click **System Management** > **Application Server**.
   b. Select the check box next to the application server you want to restart and click **Stop**.
   c. After waiting for a few seconds, click **Start**.

Adding Callback applications in Experience Portal

About this task

You can add the following applications to Experience Portal and ensure that the shared UUI option is set for these applications:

- OceanaCallback
- Outbound Callback

Procedure

1. On the Experience Portal Manager (EPM) web console, click **System Configuration** > **Applications**.
2. In the Applications page, click **Add**.
3. In the **Name** field, specify a name for the application.

4. In the **VoiceXML URL** field, enter the following URI:

   `http://<AppServer> IP address>:7080/OceanaCallback/Start`

   `<AppServer IP address>` is the IP address of the application server hosting the OceanaCallback application.
5. Click **Verify** to ensure the OceanaCallback application is deployed correctly.
6. Under the Speech Servers area, do the following:
   a. In the **TTS** field, select the speech server configured on the Speech Servers page.
   b. Move the required value from the **Voices** list to the **Selected Voices** list.
7. In the **Application Launch** field, do the following:
   a. In the **Called Number** field, enter a number that you dial to start the application.
   b. Click **Add**.
8. Click **Advanced Parameters** and do the following:
   a. In the **Generate UCID** field, select `Yes`.
   b. In the **Operation Mode** field, select `Shared UUI`.
   c. In the **Transport UCID in Shared Mode** field, select `Yes`.
9. Click **Save**.
10. In the Applications page, click **Add**.
11. In the **Name** field, specify the name of the Outbound Callback application that you noted down from the Avaya Callback Assist Administration interface.
12. In the **Type** field, select `CCXML`.
13. In the **CCXML URL** field, enter the following value:

    `http://<IP address of the Callback Assist server>:8080/CBAScripts/cbaCallControl`
14. Under the Speech Servers area, in the **TTS** field, select `No TTS`.
15. In the **Application Launch** field, select `Outbound`.
16. Click **Advanced Parameters** and do the following:
    a. In the **Generate UCID** field, select `Yes`.
    b. In the **Operation Mode** field, select `Shared UUI`.
    c. In the **Transport UCID in Shared Mode** field, select `Yes`.
17. Click **Save**.

Verifying the dial plan for Avaya Oceana®

About this task

Use this procedure to verify that the dial plan for Avaya Oceana® is correctly configured to allow Experience Portal to dial back the customer.

Procedure

1. Log on to the Experience Portal Manager (EPM) interface.
2. In the navigation pane, click **System Configuration** > **VoIP Connections**.
3. On the SIP tab, verify the entry for Session Manager.
4. Log on to the System Manager web console.
5. On the System Manager web console, click **Elements** > **Routing** > **Dial Patterns** > **Dial Patterns**.
6. On the Dial Patterns page, verify the dial pattern that Session Manager can use to route calls to Communication Manager.

Creating the Callback Vector Directory Number

About this task

Use this procedure to create the Callback Vector Directory Number (VDN).

Procedure

1. Run **`add vdn next`** or **`add vdn n`**.

   n is the extension that you want to use for the VDN. This example uses 8284102.
2. On page 1 of the VECTOR DIRECTORY NUMBER screen, perform the following steps:
   a. In the **Name** field, enter the name of the VDN.
   b. In the **Destination** field, set the destination to a vector number which is not in use. This example uses 9.
3. Save the settings.

Example

```
change vdn 8284102                                          Page   1 of   3
                          VECTOR DIRECTORY NUMBER

                            Extension: 828-4102
                                 Name*: Callback VDN
                          Destination: Vector Number        9
              Attendant Vectoring? n
            Meet-me Conferencing? n
              Allow VDN Override? n
                             COR: 1
                             TN*: 1
                        Measured: none      Report Adjunct Calls as ACD*? n


      VDN of Origin Annc. Extension*:
                          1st Skill*:
                          2nd Skill*:
                          3rd Skill*:



* Follows VDN Override Rules
```

Configuring a vector for the Callback VDN

About this task

Use this procedure to configure a vector for the Callback VDN.

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Callback VDN. In this example, the vector number is 9.
3. On page 1 of the CALL VECTOR screen, perform the following steps:
   a. In the **Name** field, enter the name of the vector as `Callback Vector`.

      This standard name makes maintenance and troubleshooting easier.

b. Enter the details required from line 01 to line 04 as shown below:

```
change vector 9                                          Page   1 of   6
                                CALL VECTOR

    Number: 9                Name: Callback Vector
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n          Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 #   Connect Callback
02 wait-time    1   secs hearing ringback
03 route-to     number 2801001          with cov n if unconditionally
04 stop
05
06
07
08
09
10
11
12

                        Press 'Esc f 6' for Vector Editing
```

In this example, 2801001 is the number that you previously configured for OceanaCallback in Experience Portal applications.

4. Save the settings.

Editing the existing Treatment vector

About this task

Use this procedure to edit the existing Treatment vector to add the lines for callback.

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Treatment VDN. In this example, the vector number is 10.

3. On page 1 of the CALL VECTOR screen, update the details in line 16 to line 26 as shown below:

```
change vector 10                                          Page   2 of   6
                                  CALL VECTOR
13 #   Offer Voicemail option
14 collect      1    digits after announcement 8289984  for none
15 goto step    23             if digits          =      9
16 goto step    25             if digits          =      8
17 goto step    11             if unconditionally
18
19 #   Oceana encountered error
20 route-to     number 8284103          with cov n if unconditionally
21
22 #   Leave a message
23 route-to     number 8284105          with cov n if unconditionally
24
25 #   Request a callback
26 route-to     number 8284102          with cov n if unconditionally
27
28
29
30
31
32
```

   The new lines that are added for callback are 16, 24, 25, and 26.

   In this example, 8284102 is the Callback VDN.

4. Save the settings.

Adding the Callback VDN to Avaya Control Manager

About this task

Use this procedure to add the Callback VDN to Avaya Control Manager.

Before you begin

- Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.
- Run ACM Synchronizer to push the Callback VDN to Avaya Control Manager.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Server Details**.
2. On the Avaya Oceana Server List page, double-click the UCAServer server.
3. Select the **VDN** tab.
4. In the **Avaya Oceana VDN Type** field, select **Callback**.

5. Move the single required Callback VDN from the **Available CM VDN** list to the **Selected CM VDN** list.
6. Click **Save**.

Creating the No Media Treatment Vector Directory Number

About this task

Use this procedure to create the No Media Treatment Vector Directory Number (VDN).

Procedure

1. Run **`add vdn next`** or **`add vdn n`**.

   n is the extension that you want to use for the VDN. This example uses 8284113.
2. On page 1 of the VECTOR DIRECTORY NUMBER screen, perform the following steps:
   a. In the **Name** field, enter the name of the VDN.
   b. In the **Destination** field, set the destination to a vector number which is not in use. This example uses 14.
   c. In the **1st Skill*** field, enter the Hunt Group that you created.
3. Save the settings.

Example

```
change vdn 8284113                                          Page   1 of   3
                          VECTOR DIRECTORY NUMBER

                            Extension: 828-4113
                                Name*: NoMedia Vector
                          Destination: Vector Number        14
                 Attendant Vectoring? n
               Meet-me Conferencing? n
                 Allow VDN Override? n
                               COR: 1
                               TN*: 1
                          Measured: none       Report Adjunct Calls as ACD*? n


       VDN of Origin Annc. Extension*:
                           1st Skill*: 828
                           2nd Skill*:
                           3rd Skill*:



* Follows VDN Override Rules
```

Configuring a vector for the No Media Treatment VDN

About this task

Use this procedure to configure a vector for the No Media Treatment VDN.

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the No Media Treatment VDN. In this example, the vector number is 14.
3. On page 1 of the CALL VECTOR screen, perform the following steps:
   a. In the **Name** field, enter the name of the vector as `NoMedia Vector`.

      This standard name makes maintenance and troubleshooting easier.

   b. Enter the details required from line 01 to line 10 as shown below:

```
change vector 14                                          Page   1 of   6
                                CALL VECTOR

    Number: 14               Name: NoMedia Vector
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n          Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 #   Collect Expected Wait Time
02 collect      5   digits after announcement none     for K
03
04 #   Locate Oceana agent
05 adjunct      routing link 1
06 wait-time    60  secs hearing ringback
07 goto step    6            if unconditionally
08
09 #   Oceana encountered error
10 route-to     number 8284103          with cov n if unconditionally
11
12

                        Press 'Esc f 6' for Vector Editing
```

4. Save the settings.

Adding the No Media Treatment VDN to Avaya Control Manager

About this task

Use this procedure to add the No Media Treatment VDN to Avaya Control Manager.

Before you begin

- Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.
- Run ACM Synchronizer to push the No Media Treatment VDN to Avaya Control Manager.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Server Details**.
2. On the Avaya Oceana Server List page, double-click the UCAServer server.
3. Select the **VDN** tab.
4. In the **Avaya Oceana VDN Type** field, select **Treatment**.
5. Move the single required No Media Treatment VDN from the **Available CM VDN** list to the **Selected CM VDN** list.
6. Click **Save**.

Updating the voicemail announcement

About this task

Use this procedure to update the `VoiceMail.wav` announcement in Avaya Aura® Media Server

Before you begin

Download the `VoiceMail.wav` file from the Avaya DevConnect portal at http://www.avaya.com/devconnect.

Procedure

1. In your web browser, enter the following URL:

   `https://<Avaya Aura Media Server FQDN>:8443/em`
2. In the **User ID** field, enter the User ID for logging in to Avaya Aura® Media Server.
3. In the **Password** field, enter the password for logging in to Avaya Aura® Media Server.
4. Click **Log in**.
5. In the navigation pane, click **Tools** > **Media Management**.
6. On the Media Management page, select the **Communication Manager** check box.

7. Click **Browse**.
8. On the Provision Media page, expand the **Communication Manager** namespace.
9. Select the content group to which you want to add a media file.
10. Click **Add Media**.
11. In the Add Media dialog box, click **Choose File** and navigate to the new `VoiceMail.wav` file.
12. Select a file and click **Upload**.

Configuring the Voice workflow for Callback Assist

About this task

Use this procedure to configure the Voice workflow for Avaya Oceana® to support the Callback Assist feature.

Procedure

1. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

2. On the Workflows tab, verify that the OceanaVoiceAssistedService workflow is available in the list of deployed workflows.
3. On the Workflows tab, select the Voice workflow and click **Attributes**.
4. On the Workflow Attributes tab, do the following:
   a. In the **CallbackDestination** field, enter a value in the following format:

      <Number>@<Domain.com>

      The *<Number>* is the No Media Treatment VDN that you created previously. For example, 8284113@domain.com.

   b. Click **Close**.

Configuring the session timer

About this task

Use this procedure to configure the session timer to control the time for which Callback Assist waits for an agent to answer the callback.

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change signaling-group n`**.

   n is the number of the signaling group.
3. On page 1 of the SIGNALING GROUP screen, in the **Session Establishment Timer (min)** field, update the value of the session timer.

   This value reflects the length of time for which a call remains waiting for an agent in the agent-first mode. Therefore, you must adjust this value carefully. For more information, see the Callback Assist documentation.
4. Save the settings.

Disabling video on the incoming SIP trunk

About this task

Use this procedure to disable video on the incoming SIP trunk. Otherwise, no initial Callback Assist menu is heard when the call leaves Communication Manager for Callback Assist.

You must disable video on the incoming SIP trunk only if the callback is not working.

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change signaling-group n`**.

   n is the number of the signaling group.
3. On page 1 of the SIGNALING GROUP screen, in the **IP Video** field, type `n`.
4. Save the settings.

Chapter 20: Configure Post Call Survey

Post Call Survey overview

Avaya Oceana® provides the Post Call Survey feature. This feature shows how to integrate Avaya Oceana® with an external survey application to solicit feedback from a customer after the customer completes the call with an agent. This feature builds on the VDN Return Destination feature of Communication Manager to first direct the calls to a Survey Vector Directory Number (VDN) and then to an application such as Experience Portal.

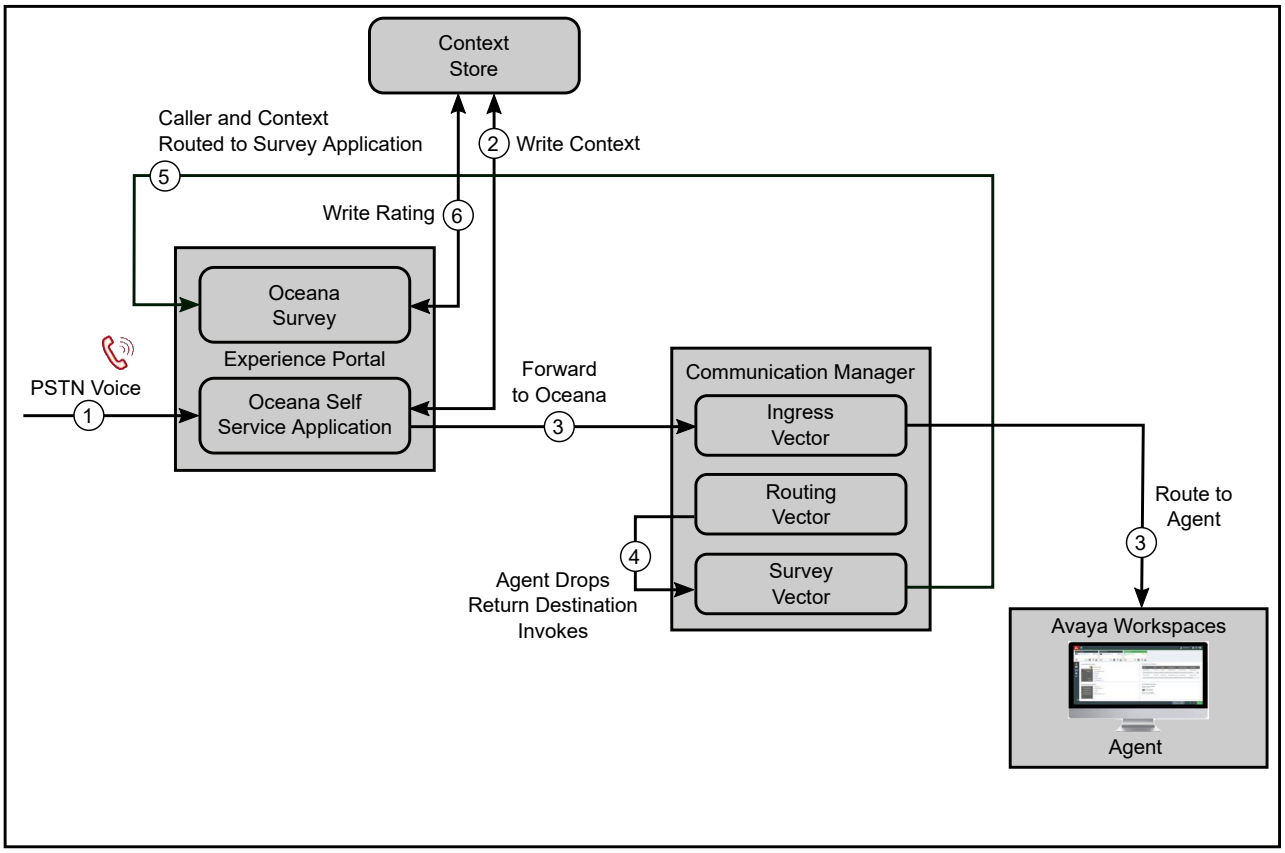
When Communication Manager detects that the agent is dropped from a voice call, the customer is kept connected and is directed the configured survey application. Calls that terminate in coverage or callback must not connect to the survey application. Therefore, you must carefully administer the Vector Return Destination (VRD).

Avaya Oceana® provides a sample Experience Portal application named OceanaSurvey. This application is intended to demonstrate how to retrieve the following details to the customer:

- Account ID
- Agent ID of the agent who interacted with the contact
- Disposition of the contact

The caller is prompted for a rating from 0 to 9. This rating is stored in the customer's journey along with the other context from the call.

The following diagram depicts the Post Call Survey flow:



When you configure this feature, you must correctly configure the Allow VDN Override parameter to ensure that callers get the survey at the right instances. For example, it is not desirable to provide a survey to a customer who has requested a callback without having spoken to an agent.

VDN Override is a Communication Manager Call Center Elite feature that allows information of the subsequent VDN where a call is routed, instead of the information of the previously-active VDN. If a VDN is configured with the Allow VDN Override parameter as no, it maintains ownership of the call throughout the routing process. Therefore, when the agent receives the call, all call data is transferred to this VDN.

The following configuration supplies a post call survey to the caller in the following situations:

Survey Applied	Vector	Comment
Yes	Ingress > Routing	Agent surplus
Yes	Ingress > Treatment > Routing	Call surplus
No	Ingress > Treatment > Callback	Caller requests callback
No	Ingress > Treatment > Coverage	Caller chooses to leave a voicemail
No	Ingress > Fallback	Routing error occurred or Avaya Oceana® out-of-service
Yes	Ingress > Routing > Transfer > Routing	Call transfer, Agent surplus

Table continues…

Survey Applied	Vector	Comment
Yes	Ingress > Routing > Transfer > Treatment > Routing	Call transfer, Call surplus
No	Ingress > Routing > Transfer > Treatment > Callback	Call transfer and then callback
No	Ingress > Routing > Transfer > Treatment > Coverage	Call transfer and then voicemail
RONA not shown	-	RONA follows the above rules at any point

You must configure the Allow VDN Override and Return Destination parameters for Avaya Oceana® VDNs as follows:

VDN	Allow VDN Override	Return Destination
Ingress	Y	Not Set
Treatment	Y	Not Set
NoMedia	Y	Not Set
Routing	Y	Set to Survey VDN
RONA	Y	Not Set
Transfer	Y	Not Set
Fallback	N	Not Set
Callback	N	Not Set
Coverage	N	Not Set
Survey	N	Not Set

Note:

If survey is not required, it is recommended that you configure the Allow VDN Override parameters according to this table. However, the Return Destination parameter on the Routing vector can be omitted. With this configuration, customers can quickly enable or disable survey from a single setting.

Deploying the OceanaSurvey application

About this task

Use this procedure to deploy the OceanaSurvey sample application by copying its `.war` file to the application server.

Procedure

1. Log in to the server as sroot.

2. Copy the `OceanaSurvey.war` file to the `/opt/AppServer/tomcat/webapps` location.
3. Restart the application server by using one of the following methods:
   - Command line
   - Web interface
4. **(Optional)** If you use the command line method, do the following:
   a. On the command line, type `cd /opt/AppServer/tomcat/bin` and press **Enter**.
   b. Type `./shutdown.sh` and press **Enter**.
   c. After waiting for a few seconds, type `./startup.sh` and press **Enter**.
5. **(Optional)** If you use the web interface method, do the following:
   a. On the Experience Portal Management web console, click **System Management** > **Application Server**.
   b. Select the check box for the application server that you want to restart and click **Stop**.
   c. After waiting for a few seconds, click **Start**.

Adding the OceanaSurvey application in Experience Portal

About this task

Use this procedure to add the OceanaSurvey application in Experience Portal and ensure that the shared UUI option is set for the application.

Procedure

1. Log on to the Experience Portal Manager (EPM) interface.
2. In the navigation pane, click **System Configuration** > **Applications**.
3. On the Applications page, click **Add**.
4. In the **Name** field, type `OceanaSurvey`.
5. In the **Type** field, select `VoiceXML`.
6. In the **VoiceXML URL** field, enter the following value:

   `http://<IP address of the OceanaSurvey server>:7080/OceanaSurvey/Start`
7. In the **Application Launch** field, select `Inbound`, and then select `Number`.
8. In the **Called Number** field, enter the telephone number that you want to associate with the OceanaSurvey application, and then click **Add**.
9. Expand **Advanced Parameters**.
10. In the **Generate UCID** field, select `Yes`.

11. In the **Operation Mode** field, select `Shared UUI`.
12. In the **Transport UCID in Shared Mode** field, select `Yes`.
13. Click **Save**.
14. On the Applications page, in the **OceanaSurvey** row, click the **Edit** icon.
15. In the **Data Center 1: Context Store Cluster IP** field, enter the IP address of Avaya Oceana® Cluster 1.
16. If secured connection is enabled on Context Store, select the **Use Secure Connection** check box.
17. Click **Save**.

Creating the Survey Vector Directory Number

About this task

Use this procedure to create the Survey Vector Directory Number (VDN).

Procedure

1. Run **`add vdn next`** or **`add vdn n`**.

   n is the extension that you want to use for the VDN. This example uses 8284107.
2. On page 1 of the VECTOR DIRECTORY NUMBER screen, perform the following steps:
   a. In the **Name** field, enter the name of the VDN.
   b. In the **Destination** field, set the destination to a vector number which is not in use. This example uses 4.
3. Save the settings.

Example

```
change vdn 8284107                                          Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                              Extension: 828-4107
                                  Name*: Survey VDN
                            Destination: Vector Number          4
                     Attendant Vectoring? n
                   Meet-me Conferencing? n
                     Allow VDN Override? n
                                    COR: 1
                                    TN*: 1
                               Measured: none       Report Adjunct Calls as ACD*? n


          VDN of Origin Annc. Extension*:
                              1st Skill*:
                              2nd Skill*:
                              3rd Skill*:

SIP URI:

* Follows VDN Override Rules
```

Configuring a vector for the Survey VDN

About this task

Use this procedure to configure a vector for the Survey VDN.

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Survey VDN. In this example, the vector number is 4.
3. On page 1 of the CALL VECTOR screen, perform the following steps:
   a. In the **Name** field, enter the name of the vector as `Survey Vector`.

      This standard name makes maintenance and troubleshooting easier.

b. Enter the details required from line 01 to line 10 as shown below:

```
change vector 4                                          Page   1 of   6
                                CALL VECTOR

    Number: 4                Name: Survey Vector
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n          Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 #   Ensure Survey played only once
02 goto step   9             if digits          =      999999999
03 set         digits = none   ADD   999999999
04 wait-time   1   secs hearing ringback
05
06 #   Connect Survey
07 route-to    number 2801002          with cov n if unconditionally
08
09 disconnect  after announcement none
10 stop
11
12

                        Press 'Esc f 6' for Vector Editing
```

In this example, 2801002 is the number that you previously configured in the OceanaSurvey application in Experience Portal.

4. Save the settings.

Configuring the Return Destination parameter on the Routing vector

About this task

Use this procedure to configure the Return Destination parameter on the Routing vector.

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vdn n`**.

   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Routing VDN.
3. On page 2 of the VECTOR DIRECTORY NUMBER screen, do the following:
   a. In the **Call Origin** field, type `both`.
   b. In the **Return Destination** field, enter the Survey VDN. This example uses 8284107.

4. Save the settings.

Example

```
change vdn 8284000                                          Page   2 of   3
                          VECTOR DIRECTORY NUMBER

                             AUDIX Name: _______
                   Return Destination*: 828-4107      Call Origin*: both
               VDN Timed ACW Interval*: ____ After Xfer or Held Call Drops*? n
                      BSR Application*: ___
          BSR Available Agent Strategy*: 1st-found      Used for BSR Polling? n
                    BSR Tie Strategy*: system

                Observe on Agent Answer? n

  Send VDN as Called Ringing Name Over QSIG? n

              Display VDN for Route-To DAC*? n
            VDN Override for ASAI Messages*: no

                         BSR Local Treatment*? n

              Reporting for PC or POM Calls? n
           Pass Prefixed CPN to VDN/Vector*? system
* Follows VDN Override Rules
```

Enabling the Allow VDN Override parameter on specific VDNs

About this task

Use this procedure to enable the Allow VDN Override parameter on the following VDNs:

- Ingress
- Treatment
- Routing
- NoMedia
- Transfer
- RONA

Important:

Do not enable the Allow VDN Override parameter on the Callback and Coverage VDNs.

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Ingress VDN.
3. On page 1 of the VECTOR DIRECTORY NUMBER screen, in the **Allow VDN Override** field, type `y`.
4. Save the settings.
5. Repeat Step 2 to Step 4 for the following VDNs:
   - Treatment
   - Routing
   - NoMedia
   - Transfer
   - RONA

Adding the Survey VDN to Avaya Control Manager

About this task

Use this procedure to add the Survey VDN to Avaya Control Manager.

Before you begin

- Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.
- Run ACM Synchronizer to push the Survey VDN to Avaya Control Manager.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Server Details**.
2. On the Avaya Oceana Server List page, double-click the UCAServer server.
3. Select the **VDN** tab.
4. In the **Avaya Oceana VDN Type** field, select **Survey**.
5. Move the single required Survey VDN from the **Available CM VDN** list to the **Selected CM VDN** list.
6. Click **Save**.

Chapter 21: Configure Authorization Service for Outbound Connector

Configuring authorization service for outbound connector provider cluster

About this task

Use this procedure to configure authorization service for Outbound Connector provider cluster.

Procedure

1. Log in to Avaya Aura® System Manager .
2. Navigate to **Elements** > **Avaya Breeze®** > **Cluster Administration**.
3. Click the **Outbound Connector Provider** check box.
4. Select the **Cluster State** and from the drop-down list, click **Deny New service**.
5. Select **Outbound Connector Provider Cluster** check box.
6. Click **Edit**.
7. Under **Cluster Attributes**, in the **Authorization Service Address** field, enter the FQDN or the cluster's IP address under which authorization service is installed.
8. Click **Commit**.
9. Click **Reboot** and wait for the cluster to run.
10. Select the **Cluster State** and accept the **Services** by selecting **Accept New Service** from the drop-down.

Enabling authentication flag in the OCP service cluster

About this task

Use this procedure to enable authentication flag in the OCP service cluster.

Procedure

1. Log in to System Manager web console.
2. Click **Elements** and select **Configuration** or search **Attributes** using the search toolbox.
3. In **Attributes Configuration**, select **Service Cluster**.
4. Select the **Cluster** in which the OBCService is deployed, and select **Service** (OBCService) from the drop-down.
5. Go to **Advanced** option, and confirm the status of **Enable Authentication**.

   By default, Enable Authentication flag is set to True for OBCService Cluster.

   If the Enable Authentication is set to false, then set it to True, and reboot the cluster to reflect the Enable Authentication flag changes.

Chapter 22: Configure voice resources through Avaya Control Manager

Configure Voice resources through Avaya Control Manager

This section describes how to use Avaya Control Manager to configure Communication Manager and Avaya Oceana® agent and Voice contact resources.

Note:

You can use Avaya Control Manager Conversation Sphere to import the Avaya Oceana® vectors. The vectors are available as .acs files. Download the .acs files from the Avaya DevConnect portal at http://www.avaya.com/devconnect. You must create the Communication Manager variables before importing the vectors. For information about how to import the .acs files, refer to the Avaya Oceana® Release Notes.

Configuring a Communication Manager Hunt Group

About this task

Important:

Skip this procedure if you have configured the Communication Manager Hunt Group using the Communication Manager System Access Terminal (SAT) interface.

Use this procedure to configure a Communication Manager Hunt Group. Since all Work Assignment agents must be in a single pool, they must be in the same Hunt Group or Skill.

Procedure

1. On the Avaya Control Manager webpage, click **Communication Manager Objects** > **Hunt Group**.
2. On the Hunt Group page, click **Add**.
3. In the **Location** field, select the location to which the Hunt Group is assigned.
4. In the **Group Number** field, enter a group number.

This value is used for the Hunt Group as the provider value in the System Manager Source Details section of the Work Assignment agent configuration.

5. In the **Group Name** field, enter the Hunt Group name.
6. In the **Extension** field, enter the Hunt Group extension number.
7. Perform the following steps to add an extension to the Hunt Group:
   a. In the **Add Extension Number** field, enter the extension number.
   b. Click **Add Extension**.

      The system displays the extension in the bottom of the screen.
8. Perform the following steps to add an extension range to the Hunt Group:
   a. In the **Start from extension** field, enter the first extension number of the extension range.
   b. In the **End at extension** field, enter the last number of the extension range.
   c. Click **Add Range**.

      The system displays the extensions in the bottom of the screen.
9. Click **Add Extension From Location List** to get a list of extensions that are assigned to the Hunt Group location.

   You must use this option when working in a location-based environment.
10. To add an extension, select the option next to the extension and click **Add**.
11. Click **Save**.

Creating variables using Avaya Control Manager

About this task

Important:

Skip this procedure if you have configured the Communication Manager variables using the Communication Manager System Access Terminal (SAT) interface.

Communication Manager vectors use variables to improve efficiency. Different types of variables are available to meet different types of call processing needs. Vector variables can be added to consider location, messaging, and adjunct routing vector steps. Based on the variable type, variables can use call-specific data or fixed values that are identical for all calls. In either case, an administered variable can be reused in many vectors.

Avaya Oceana® has a number of initial vectors:

- Fallback Vector - Automatically routes calls to Elite when Avaya Oceana® is down
- Ingress Vector - Initiates the Adjunct Route
- Treatment Vector - Provides treatments for calls that route to Avaya Oceana®
- Routing Vector - Collects the digits set by the Adjunct Route application.

  These digits contain the Agent ID.

- RONA Vector - To handle Voice Redirect On No Answer (RONA) scenarios
- Coverage Vector - To route callers to a voice mail mailbox
- Transfer to Service Vector - To initiate the Adjunct Route

These vectors require the following variables:

- Routing Vector requires a variable used to collect Agent ID.
- Avaya Oceana® vectors require a Persistent variable.

  This variable is used to differentiate between the types of call ingress: (1) Elite-anchored / Adjunct Route path or (2) the Web Voice / Avaya Breeze® platform-anchored path.

Procedure

1. On the Avaya Control Manager webpage, click **Communication Manager Objects** > **Variable**.
2. On the Variable page, click **New**.
3. In the **Location** field, select your Communication Manager.
4. In the **Variable** field, enter a name for the variable. For example, `A`.

   Important:

   Ensure that your Communication Manager does not already have a variable configured with the same name.
5. In the **Description** field, enter a description for the variable as `Adjunct Route Digits`.

   This standard description makes maintenance and troubleshooting easier.
6. In the **Type** field, select `collect`.
7. In the **Scope** field, select `L`.
8. Click **Save**.
9. On the Variable page, click **New**.
10. In the **Location** field, select your Communication Manager.
11. In the **Variable** field, enter a name for the variable. For example, `B`.

    Important:

    Ensure that your Communication Manager does not already have a variable configured with the same name.
12. In the **Description** field, enter a description for the variable as `Adjunct Route Flag`.

    This standard description makes maintenance and troubleshooting easier.
13. In the **Type** field, select `collect`.
14. In the **Scope** field, select `P`.
15. Click **Save**.

16. Add any further variables as required for your solution. For example, add the variables as shown below.

Example

```
change variables                                          Page   1 of  39
                              VARIABLES FOR VECTORS

Var Description                Type    Scope Length Start Assignment       VAC
A   Adjunct Route Digits       collect L     16     1
B   Adjunct Route Flag         collect P     1      1
C   ASAI Data                  asaiuui L     2      1
D
E   Collected Digits I         collect L     6      1
F   Collected Digits II        collect L     1      1
G   Collected Digits III       collect L     1      1
H   Collected Digits Concat    collect L     8      1
I   Collected Digits UUI       asaiuui L     8      1
J
K   Expected Wait Time         collect L     5      1
L
M
N
O   Oceana Routing             collect P     1      1
P
Q   Oceana In Service          value   G     1             1              VV1
R
```

Configuring Vector Directory Numbers

About this task

Important:

Skip this procedure if you have configured the Communication Manager Vector Directory Numbers (VDNs) using the Communication Manager System Access Terminal (SAT) interface.

Use this procedure to configure VDNs for Avaya Oceana®. A VDN is an extension that directs an incoming call to a specific vector. This number is a virtual extension number which is not assigned to an equipment location. VDNs must follow your dial plan.

Create a VDN for each of the following:

- Ingress Vector to Adjunct Route
- Routing Vector
- RONA Vector
- Transfer to Service Vector

Procedure

1. On the Avaya Control Manager webpage, click **Communication Manager Objects** > **VDN**.

2. On the VDN page, click **Add**.
3. In the **Location** field, select the location.
4. In the **VDN Number** field, enter the VDN.
5. In the **VDN Name (English)** field, enter the VDN name that is added to the Communication Manager.
   - The name must be in English.
   - The name must have up to 22 letters
   - The name must not have any special character other than underscore (_).
6. In the **Description** field, enter a description for the VDN.
7. In the **VDN TEMPLATE** field, select a template.

   The VDN default settings are populated based on the selected template.
8. Click **Save**.
9. Repeat step 2 through 8 to add more VDNs.

Adding Provider, Skills, VDN, and Extensions to Avaya Oceana®

About this task

Use the following procedure to configure the required voice resources for Avaya Oceana®.

You can select and use 1 Routing VDN for voice. You can select multiple VDNs for other VDN types. To provide different wait treatments to different callers, Avaya recommends using a single Ingress VDN and multiple Treatment VDNs and vectors. You can configure the voice workflow to differentiate between callers based on data, such as the caller number, routing attributes, or any other available data.

Before you begin

- Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.
- Ensure that you use Dial Plan when using a shared Communication Manager with Avaya Oceana® or Avaya Workspaces for Call Center Elite.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. Do one of the following:
   - Double-click the administered Avaya Oceana® server and click **Edit**.
   - Select the administered Avaya Oceana® server and click **Edit**.
4. Select the **Providers** tab.
5. To add the Voice Communication Manager, do the following:
   a. Click **Add**.

b. From the **Type** drop-down list, select **CM**.

c. In the **Name** field, type the same name as the `providerId` value that you entered when creating the CSC attributes in the Communication Manager list.

d. In the **Address** field, type the address in the following format:

`<Oceana Routing VDN>@<domain name>.com`

For example, type: `8284000@domain.com`

<Oceana Routing VDN> is the VDN that you configured in Communication Manager.

Important:

This VDN extension number must match the Routing VDN you configure in Step 12 and Step 13.

e. **(Optional)** In the **Voice mail Access** field, type the number to access the voice mail system through Avaya Workspaces.

f. **(Optional)** In the **External Access Code** field, type the number to make an external voice call.

Avaya Workspaces prefixes this number when an agent makes an external call.

g. Select or clear the **Video Enabled** check box to enable or disable the provider to support video with voice.

When you select this check box, you can assign both voice and video channels to the agents who have accounts for this provider.

h. Click **Save**.

Important:

To make the new provider available to Avaya Workspaces agents, restart the clusters.

6. Select the **Skill** tab.
7. Move the single required Hunt Group from the **Available Skill** list to the **Selected Skill** list.

Note:

When you use Avaya Control Manager (ACM) for an Avaya Workspaces agent to add or remove a skill, the agent must log out from Avaya Workspaces and log back in for the application to reflect the changes.

8. Click **Save**.
9. Select the **VDN** tab.
10. From the **Avaya Oceana VDN Type** drop-down list, select **Ingress**.
11. Move the required Ingress VDNs from the **CM VDNs** list to the **Selected** list.
12. In the **Avaya Oceana VDN Type** field, select **Routing**.

13. Move the single required Routing VDN from the **CM VDNs** list to the **Selected** list.
14. In the **Avaya Oceana VDN Type** field, select **Treatment**.
15. Move the required Treatment VDNs from the **CM VDNs** list to the **Selected** list.
16. In the **Avaya Oceana VDN Type** field, select **RONA**.
17. Move the required RONA VDNs from the **CM VDNs** list to the **Selected** list.
18. In the **Avaya Oceana VDN Type** field, select **Transfer**.
19. Move the required Transfer to Service VDNs from the **CM VDNs** list to the **Selected** list.
20. In the **Avaya Oceana VDN Type** field, select **Coverage**.
21. Move the required Coverage VDNs from the **CM VDNs** list to the **Selected** list.
22. In the **Avaya Oceana VDN Type** field, select **Fallback**.
23. Move the required Fallback VDNs from the **CM VDNs** list to the **Selected** list.
24. In the **Avaya Oceana VDN Type** field, select **Survey**.
25. Move the required **Survey VDNs** from the **CM VDNs list** to the **Selected** list.
26. Click **Save**.
27. Select the **Extensions** tab.
28. To add DMCC extensions, select the **Recorder Extension**.
29. Move the required extensions from the **Available Extensions** list to the **Selected Extensions** list.
30. Click **Save**.

Creating a user to handle Voice contacts

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.
3. Click **Add**.
4. Enter appropriate value in each of the following fields:
   a. In the **First Name (English)** field, enter the first name of the user in English.
   b. In the **Surname (English)** field, enter the surname of the user in English.
   c. In the Available applications section, select the **Avaya Oceana** check box.
   d. In the **LDAP Username** field, enter the LDAP user name of the user.

      The LDAP user name must be in the username@domain.com format. This user name is used to log on to Avaya Workspaces.

e. In the **Username** field, enter a user name.

In this release, the user name is the internal handle.

f. In the **Password** field, enter a password.

This password is used to log on to Avaya Control Manager.

g. In the **Confirm Password** field, re-enter the password.

h. In the **Extension** field, enter the station associated with this agent.

This is used when logging on to Avaya Workspaces.

Note:

You must enter a value in this field only if the agent has to handle Voice contacts.

i. In the **AVAYA Login** field, enter the Elite agent login ID.

When creating an agent, if the **Profile** field is set to **Agent** and the **AVAYA Login** field is populated, then this agent is added to Elite. However, if the **AVAYA Login** field is not populated, then this agent is not added to Elite. Therefore, the agent cannot handle Avaya Oceana® Voice contacts. This type of agent can handle only Multimedia contacts.

j. Select **Team** as required.

k. Select **Template** as required.

l. Click **Save**.

5. Scroll to the right and select the **Avaya Oceana** tab.
6. Select the **Voice** check box.

Important:

To change the channel of an agent while the agent is live, the agent must be logged out and logged in again.

7. **(Optional)** Select the **Prompt agent for extension number at login** check box to enable Hot Desking.

If you enable Hot Desking, agents can change their extension number.

8. Click **Save**.

Adding attributes to an agent

About this task

Use this procedure to add routing attributes to an agent.

Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.

3. Select a user and click **Edit User**.
4. Scroll to the right and select the **Avaya Oceana** tab.
5. Ensure the user has a Voice account.
6. Select the **Attributes** tab.
7. Move the required attributes from the **Available Attributes** list to the **Agent Attributes** list.
8. Click **Save**.

Creating a Transfer Target service for Voice

About this task

Use this procedure to create a Transfer Target service for Voice through Avaya Control Manager. The service is automatically available to consult, and the user can complete consult calls as transfer or conference. After you create a service, the Transfer Target service is also available to consult on, where the user can complete the consult to service call as a transfer or a conference.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™** > **Work Assignment**.
2. Select the **Services** tab.
3. On the Services tab, click **Add**.
4. To add a Transfer Target service, perform the following steps:
   a. In the **Service Name** field, enter the name of the service.
   b. Select the **Available for Transfer** check box.

      The system automatically selects the **Agent Display** check box.
   c. Move the required attributes from the **Available Attributes** list to the **Included Attributes** list.
   d. In the Transfer Routepoints section, in the **PSTN Voice** field, select the Transfer VDN that you created for Voice.
   e. Click **Save**.

Restarting the CallServerConnector service

About this task

Restart the CallServerConnector service to reacquire or acquire the Hunt Group.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.

2. On the Service Clusters tab, do the following:
    a. In the **Cluster** field, select Avaya Oceana® Cluster 1.
    b. In the **Service** field, select **CallServerConnector**.
3. For **Deploy CSC**, type `false` in the **Effective Value** field and wait to ensure that CSC is undeployed.
4. For **Deploy CSC**, type `true` in the **Effective Value** field and wait to ensure that CSC is deployed.

Chapter 23: Verify Voice contacts

Verify Voice contacts using Avaya Workspaces

This section describes how to use Avaya Workspaces to verify the Avaya Oceana® deployment and configuration for Voice contacts. This section also describes how to use Avaya Workspaces to verify Voice calls.

For information about the guidelines on Avaya Oceana® user's client software and platform requirements, setting and configuring browsers for use within Avaya Oceana® deployment, see User's Client Software and Platform requirements for secure connections on page 41.

Deploying Avaya Workspaces

Procedure

1. Install and commission Avaya Workspaces.

   For information about how to install and commission Avaya Workspaces, see the following documents:

   - *Using Avaya Workspaces for Avaya Oceana®*
   - *Administering Avaya Oceana®*
2. Configure Avaya one-X® Agent or a Communication Manager deskphone for making test calls.

Logging in to Avaya Workspaces

About this task

Use this procedure to log in to Avaya Workspaces to verify access details and agent status.

Procedure

1. Enter one of the following URLs in your web browser:
   - For an Avaya Oceana® deployment that supports up to 100 active agents, enter `https://<AvayaOceanaCluster1_FQDN>/services/UnifiedAgentController/workspaces/#/login`.
   - For an Avaya Oceana® deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, enter `https://<AvayaOceanaCluster2_FQDN>/services/UnifiedAgentController/workspaces/#/login`.

2. On the Agent Login screen, perform the following steps:
   a. In the **Username** field, enter the LDAP username of the agent as configured on the Users page on Avaya Control Manager.

      Note:

      - Ensure that the agent is configured through Avaya Control Manager to process Voice contacts.
      - Ensure that the agent has appropriate attributes for this test contact.
      - To simplify initial verification, ensure that no other agent with Voice capabilities is logged in. It ensures that the initial Voice calls are all routed to this agent.

   b. In the **Password** field, enter the password of the agent.
   c. Click **SIGN IN**.
3. On the Activate Agent screen, click **ACTIVATE**.
4. On the Avaya Workspaces agent interface, in the bottom right corner, verify that the agent state is `CONNECTED`.

Starting work in Avaya Workspaces

About this task

Use this procedure to configure the agent to accept incoming customer calls.

Procedure

1. On the Avaya Workspaces agent interface, from the agent status drop-down list, select **StartWork**.
2. In the bottom right corner, verify that the agent state changes to `READY`.

   Note:

   On the Avaya Workspaces agent interface, when an agent is in the `READY` state, the agent remains available for receiving interactions until the agent is occupied on all channels for which the agent is configured.

   Avaya Oceana® provides the following agent states:

   - `CONNECTED`: The state of agents when they log in and activate themselves in the Avaya Workspaces or when they click the **Finish Work** button. In this state, agents do not remain available for receiving interactions.
   - `Ready`: The state of agents when they click the **Start Work** or **Go Ready** button. In this state, agents remain available for receiving interactions.
   - `Not Ready`: The state of agents when they click the **Additional Work** or **Go Not Ready** button. In this state, agents do not remain available for receiving interactions.

If multiplicity configuration of an agent allows receiving multiple interactions on a channel, the agent remains available for receiving interactions on that channel until the maximum multiplicity is achieved.

Verifying Voice contact routing to agents

About this task

Use this procedure to make a test phone call to verify that Avaya Workspaces and Avaya Oceana® are correctly configured.

Procedure

1. Ensure that the agent is logged in and is ready to handle customer calls.
2. Using Avaya one-X® Communicator or a Communication Manager deskphone, do one of the following:
   - To verify the Experience Portal Interactive Voice Response (IVR), dial the inbound launch number configured in Experience Portal.

     The inbound launch number is configured on the Experience Portal Management web console by clicking **System Configuration** > **Applications** > **Application Launch** > **Called Number**. Calls to this number are treated and then routed to suitable agents based on the attributes.
   - To verify the Call Center Elite IVR, dial the Self Service Vector Directory Number (VDN) configured in Communication Manager.

   Important:

   Engagement Designer workflows reject the calls made from Communication Manager stations that are monitored by Avaya Control Manager or Avaya Oceana®. Therefore, to make a test call, you must use a station that is not monitored by Avaya Control Manager or Avaya Oceana®.

   To make a test call to Experience Portal or Call Center Elite Self Service test number, you can use Avaya one-X® Communicator or a Communication Manager deskphone with an unmonitored station.

   A monitored station specifies the station that you define and configure in Avaya Control Manager. If a station is defined in Avaya Control Manager and assigned as an Avaya Oceana® station, the CallServerConnector service identifies all configured agent stations, and also identifies when the stations are used with Avaya Oceana® even if Communication Manager and Application Enablement Services report the station as unmonitored.

   Do not use any station that is configured in Avaya Control Manager for Avaya Oceana® use to make test calls into the system. If an incoming voice call is originated from an agent station that is configured in Avaya Control Manager as an Avaya Oceana® resource, the call fails at the retrieving context step in the Engagement Designer workflow and does not get routed to an Avaya Oceana® agent.

3. Verify that the test call is presented to the agent in Avaya Workspaces.
4. Using Avaya Workspaces, answer the routed call.
5. Ensure that there is an audio speech path between the test customer and agent.
6. Place the call On Hold and Off Hold to verify call control functionality.
7. Release the test call.
8. Continue to verify Voice contact configuration in your solution.

Note:

When an agent accepts an interaction within in Avaya Workspaces, the Customer Journey widget is populated using the Customer Journey Service APIs. You must ensure that that the CustomerJourneyService attribute is correctly configured to communicate with the External Data Mart for this feature to work. You must deploy customer journey on the same cluster as Context Store Manager. Customer journey displays any interactions that create touchpoints on the EDM.

Chapter 24: Configure Avaya Oceana® with Avaya WebRTC Connect agents

Avaya WebRTC Connect solution configurations and prerequisites

Configurations

Avaya Oceana® provides the following WebRTC Connect configurations. Based on your requirements, you can choose from the following configurations and complete all tasks:

- Avaya Oceana® with WebRTC Connect agents.

  With this configuration, WebRTC Connect agents can answer PSTN voice calls.

- Avaya Oceana® with web and mobile voice calls.

  With this configuration, phone-enabled agents can answer web and mobile voice calls that customers make through web and mobile devices on the public internet.

- Avaya Oceana® with web and mobile voice calls and WebRTC Connect agents.

  With this configuration, WebRTC Connect and phone-enabled agents can answer PSTN, web, and mobile voice calls.

- Avaya Oceana® with web and mobile video calls and WebRTC Connect agents.

  With this configuration, WebRTC Connect agents can answer web and mobile video calls.

Important:

- Before doing any of these configurations, you must deploy the Elite voice solution.
- WebRTC Connect agents do not support the Auto answer feature. Therefore, do not configure WebRTC Connect agents to use this feature.
- Avaya Oceana® supports web and mobile video calls only if you have Avaya Aura® 7.1.3 or later.
- Hot Desking configuration does not apply to WebRTC Connect agents.
- Web calls made using the Microsoft Edge browser do not support STUN, TURN-TCP, or TURN-TLS.
- Web calls made using the Microsoft Edge browser support UDP TURN.

- WebRTC Connect only supports secure deployment options.

Prerequisites

The following are the prerequisites for the WebRTC Connect solution:

- LDAP/Active Directory
- Avaya Aura® Communication Manager, Avaya Aura® Session Manager, Avaya Aura® System Manager, and Avaya Breeze® platform.
- Avaya Aura® Media Server for Avaya Breeze® platform
- Avaya Aura® Device Services
- Avaya Aura® Web Gateway
- Avaya Control Manager
- Avaya Contact Recorder Advanced for recording

Checklist for configuring Avaya Oceana® with Avaya WebRTC Connect agents

Use the following checklist to configure Avaya Oceana® with WebRTC Connect agents so that the agents can answer PSTN voice calls:

No.	Task	Description	✔
1	Configure LDAP	See Configure LDAP on page 377.	
2	Synchronize LDAP users in System Manager	See Synchronizing LDAP users in System Manager on page 379.	
3	Assign SIP Handles to the synchronized LDAP users in System Manager	-	
4	Install and configure Avaya Aura® Device Services, Avaya Aura® Media Server, and Avaya Aura® Web Gateway	See the following: • Avaya Aura Device Services deployment on page 380. • Avaya Aura Media Server deployment on page 386. • Avaya Aura Web Gateway deployment and configuration on page 400.	

Table continues…

No.	Task	Description	✔
5	Publish the COMM_ADDR_HANDLE values of the WebRTC Connect agent on Avaya Aura® Device Services	See Publishing COMM_ADDR_HANDLE values on Avaya Aura Device Services on page 385.	
6	Configure the voice media path	See the following: • Configuring codecs in Avaya Aura Web Gateway on page 407. • Prioritizing codecs in Avaya Aura Media Server on page 408. • Prioritizing codecs in Communication Manager on page 408.	
7	Configure authorization on Avaya Aura® Web Gateway	See Avaya Aura Web Gateway authorization on page 407.	
8	Create WebRTC Connect agents that can use media in browsers	See Creating a user in Avaya Control Manager on page 413.	

Configure LDAP

The configuration of LDAP involves the following:

- Preconfiguration on page 377
- Creating a user in Active Directory on page 378
- Synchronizing LDAP users in System Manager on page 379

Note:

Before you configure LDAP, ensure the following:

- NTP servers are configured and operational
- FQDNs of all servers are created in DNS servers.

Preconfiguration

Ensure that you install and configure Windows Active Directory or any supported LDAP and also configure System Manager with LDAP by using a secure link.

- Get a working LDAP to complete the installation of Avaya Aura® Device Services and Avaya Aura® Web Gateway.
- Assign a user to the selected admin group to administer the system after the installation.

- Create the following in your AD or LDAP system:
  - A domain for the users.

    This domain does not need to match the SIP domain. Multiple Avaya Oceana® deployments can use the same users from the same LDAP or domain.
  - An organizational unit under the domain.
  - A test user that Avaya Aura® Device Services uses for connectivity.
  - Two LDAP security groups for authenticating users and administrators.

    The following table lists the groups:

Group name	Purpose
AADS_User	General users including all WebRTC Connect users and Avaya Aura® Device Services users.
AADS_Admin	Users who can administer Avaya Aura® Device Services and Avaya Aura® Web Gateway after logging on to the AD or LDAP system.

Creating a user in Active Directory

About this task

Use this procedure to create a user in Active Directory who can act as a general user for Avaya Aura® Device Services, and can also administer Avaya Aura® Device Services and Avaya Aura® Web Gateway.

Procedure

1. Log in to the server containing the Active Directory.
2. Click **Start** > **Administrative Tools** > **Active Directory Users and Computers**.
3. In the navigation pane, expand the domain that you created for the users.
4. Right-click the Active Directory organizational unit (OU) and click **New** > **User**.
5. In the **New Object - User** dialog box, do the following:
   a. In the **First name** field, enter the first name of the user.
   b. In the **Last name** field, enter the surname of the user.
   c. In the **User logon name** field, enter the user name.
   d. Click **Next**.
   e. In the **Password** field, enter a password for the user.
   f. In the **Confirm Password** field, re-enter the password.
   g. Clear the **User must change password at next logon** check box.
   h. Select the **Password never expires** check box.
   i. Click **Next**.

j. Click **Finish**.

The server displays the new user in the list in the content pane.

6. In the content pane, right-click the new user and click **Add to a group**.
7. In the Select Groups dialog box, add the user to the standard users group and the appropriate administrator group, and click **OK**.

Synchronizing LDAP users in System Manager

About this task

Use this procedure to synchronize LDAP users in System Manager.

Procedure

1. On the System Manager web console, click **Users** > **Directory Synchronization** > **Sync Users**.
2. On the User Synchronization page, on the Synchronization Datasources tab, click **New**.
3. On the New User Synchronization Datasource page, in the Directory Parameters section, do the following:
   a. In the **Datasource Name** field, enter the name to identify Active Directory.
   b. In the **Host** field, enter the FQDN address of your LDAP server.

      Ensure that LDAP certificates contain a SAN entry.
   c. In the **Principal** field, enter the LDAP login details.

      For example, myDomain\Administrator.
   d. In the **Password** field, enter the password for the LDAP login account that you specify.
   e. In the **Port** field, enter the port number as `636`.
   f. In the **Base Distinguished Name** field, enter the LDAP details.

      For example, CN=user,DC=myDomain,DC=com
   g. In the **Search Filter** field, enter the LDAP search string.

      For example, CN=Alex*.
   h. In the **LDAP User Schema** field, enter the LDAP User Schema details.
   i. Select the **Use SSL** check box.
   j. Click **Test Connection**.
4. On the New User Synchronization Datasource page, in the Attribute Parameters section, do the following:
   a. Click **Add Mapping** to add a row.
   b. From the drop-down list on the left, select **cn**.

c. From the corresponding drop-down list on the right, select **sourceUserKey**.
d. Click **Add Mapping** to add another row.
e. From the drop-down list on the left, select **mail**.
f. From the corresponding drop-down list on the right, select **loginName**.

Note:

Instead of the **mail** field pointing to **loginName**, you can also use **userPrincipalName** depending on the configuration of the LDAP server. For example, if the **mail** field is not set in the LDAP server.

g. Click **Add Mapping** to add another row.
h. From the drop-down list on the left, select **sn**.
i. From the corresponding drop-down list on the right, select **surname**.
j. Click **Add Mapping** to add another row.
k. From the drop-down list on the left, select **givenName**.
l. From the corresponding drop-down list on the right, select **givenName**.
m. Click **Add Mapping** to add another row.
n. From the drop-down list on the left, select **displayName**.
o. From the corresponding drop-down list on the right, select **displayName**.

5. Click **Save**.
6. On the User Synchronization page, click **Active Synchronization Jobs**.
7. Click **Create New Job**.
8. On the New User Synchronization Job page, in the **Datasource Name** field, select the LDAP server and click **Run Job**.

   Wait for the job to complete so that all LDAP users are loaded in System Manager.
9. On the User Synchronization page, click **Synchronization Job History**.
10. In the **Status** column, verify that the status of the job is `RUNNING`.

    The status changes to `COMPLETED` when the job is complete.

Avaya Aura® Device Services deployment

Avaya Oceana® requires Avaya Aura® Device Services to provide login services to Video-enabled SIP agents through a browser endpoint.

Adding a data center

About this task

Use this procedure to add a data center in System Manager.

Procedure

1. On the System Manager web console, click **Elements** > **Session Manager** > **System Status** > **User Data Storage**.
2. On the User Data Storage page, click the **Data Center** tab.
3. Click **New**.

   System Manager displays the Edit Data Center page.
4. In the **Name** field, enter a name for the data center.
5. In the **Description** field, enter the description of the data center.
6. Click **Commit**.

Assigning Session Manager to the data center

About this task

Use this procedure to assign Session Manager to the newly created data center.

Procedure

1. On the System Manager web console, click **Elements** > **Session Manager** > **Session Manager Administration**.
2. On the Session Manager Instances tab, select an instance and click **Edit**.

   System Manager displays the Edit Session Manager page.
3. In the General area, in the **Data Center** field, select the newly created data center.
4. Click **Commit**.

Deploy Avaya Aura® Device Services on a virtualized environment

Adding an Avaya Aura® Device Services instance to System Manager inventory

About this task

Use this procedure to add an instance of Avaya Aura® Device Services to System Manager inventory.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, click **New**.

System Manager displays the New Elements page.

3. In the **Type** field, select `Avaya Aura Device Services`.

   System Manager displays the New Avaya Aura Device Services page.

4. On the General tab, do the following:
   a. In the **Name** field, enter the name of the Avaya Aura® Device Services server.
   b. In the **Node** field, enter the IP address of the Avaya Aura® Device Services server.
   c. In the **Description** field, enter the description of the Avaya Aura® Device Services server.
5. Click the **Attributes** tab.
6. On the Attributes tab, do the following:
   a. In the **Login** field, enter the user name to access the Avaya Aura® Device Services server.

      The user name that you enter in this field is the administrator user name provided during the Avaya Aura® Device Services OVA deployment.

   b. In the **Password** field, enter the password to access the Avaya Aura® Device Services server.

      This is the administrator password provided during the Avaya Aura® Device Services OVA deployment.

   c. In the **Confirm Password** field, re-enter the password to access the Avaya Aura® Device Services server.
   d. In the **Version** field, enter the Avaya Aura® Device Services base version (7).
   e. In the **Location** field, enter the location of the Avaya Aura® Device Services server.

      This is an optional field.
7. Click the **General** tab.
8. Select the TrustManagement access profile and click **Edit**.
9. Leave the **Container type** field blank.
10. In the **Host** field, enter the hostname of the Avaya Aura® Device Services server.
11. Click **Save**.
12. To add an EMURL access profile to enable SSO login, do the following:
    a. On the General tab, in the Access Profile area, click **New**.
    b. In the **Access Profile Type** field, select `EMURL`.
    c. In the **Host** field, enter the FQDN of the Avaya Aura® Device Services server.
    d. In the **Port** field, type `8445`.
    e. In the **Path** field, type `/admin`.

f. Click **Save**.

13. Click **Commit**.

Pairing Session Manager with an Avaya Aura® Device Services server

About this task

Use this procedure to pair Session Manager with an Avaya Aura® Device Services server.

Procedure

1. On the System Manager web console, click **Elements** > **Session Manager** > **Session Manager Administration**.
2. On the Session Manager Instances tab, select an instance and click **Edit**.

   System Manager displays the Edit Session Manager page.
3. **(Optional)** In the General area, in the **Data Center** field, select a data center if Session Manager is not assigned to a data center.
4. In the **Avaya Aura Device Services Server Pairing** field, select an Avaya Aura® Device Services server to pair with Session Manager.
5. Click **Commit**.

Installing Avaya Aura® Device Services

About this task

Use this procedure to install Avaya Aura® Device Services.

Before you begin

On the System Manager web console, click **Elements** > **Session Manager** > **Dashboard** and verify that all Session Manager instances are up and running.

Procedure

1. Go to the Avaya directory by typing the following command:

   ```
   cd /opt/Avaya
   ```
2. Run the following command:

   ```
   app install
   ```

   The Initial Installation Configuration screen appears.
3. Select the **Cluster Configuration** menu and ensure that the **Initial cluster node** option is set to `y`.
4. To return to the previous menu, select **Return to Main Menu** and press **Enter**.
5. Select the **Front-end host, System Manager and Certificate Configuration** menu and configure the settings that are accessible from the menu.

6. In the **Front-end FQDN** field, type the Avaya Aura® Device Services FQDN to extend the system to an Avaya Aura® Device Services cluster.

   You must use the hostname corresponding to the virtual IP address. For a standalone Avaya Aura® Device Services, this field is the same as the local front end host.

7. In the fields specific to System Manager, enter the required values.

   Keystore password must have six or more characters. The password must be the same on all nodes in the cluster.

   After you enter the System Manager FQDN and press **OK**, the installer tries to check the validity of the hostname.

8. Select **Return to Main Menu** and press **Enter**.
9. Select the **Session Manager Cassandra Configuration** menu and type the Session Manager Management and Asset IP addresses.
10. Read the End User License Agreement (EULA) and press **Accept** to accept the EULA.

    The system configures the other settings such as required RPMs, downloads certificates from System Manager, creates database schema, and does the required initial configuration required for the Avaya Aura® Device Services server installation.

11. Select **Continue** to finish the installation.
12. Select **LDAP Configuration**.
13. On the LDAP configuration screen, type values for each parameter manually.

    Important:

    Do not copy-paste these values to avoid invalid characters such as spaces.

14. Navigate to **Advanced LDAP parameters** and click **Select**.
15. On the Advanced LDAP parameter screen, verify the default values for the parameters and update the required values.
16. Select **Return to Main Menu** and press **Enter**.
17. Navigate to **TestUser** and click **Select**.
18. Add an LDAP test user for better validation of the LDAP parameters.

    The test user must be a valid user on LDAP and must be present in the provided Base Context DN. The LDAP user must correspond to **UID Attribute ID**.

19. Click **OK**.
20. Click **Apply**.
21. Click **Yes**.
22. Click **Continue**.
23. Leave the **CORS Configuration** and **Serviceability Agent Configuration** fields unchanged.

24. Click **Continue**.
25. On the prompt to restart Avaya Aura® Device Services, click **Yes**.
26. Click **Continue**.

Publishing COMM_ADDR_HANDLE values on Avaya Aura® Device Services

Procedure

1. On the Avaya Aura® Device Services web administration portal, click **Dynamic Configuration** > **Configuration**.
2. On the Configuration page, click the **Group** tab.
3. In the **COMM_ADDR_HANDLE_TYPE** field, click `Avaya SIP`.
4. In the **COMM_ADDR_HANDLE_LENGTH** field, enter the number of digits in the extension number of the SIP agent.
5. Click **Publish**.

   The portal displays the Publish/Delete Settings dialog box.
6. Select the **Group settings will be applied to group** check box.
7. In the text box, type the first five characters of the LDAP group that contains the agents.
8. In the drop-down list, click the group.
9. Click **Publish**.
10. Click **Yes**.
11. To verify whether the values are published, do the following:
    a. In your web browser, enter the following URL:

       `https://<Avaya Aura Device Services FQDN>:8443/acs/resources/configurations`

    b. On the prompt, enter the login credentials of the LDAP user who is a part of the LDAP user group.
    c. Verify the output.

       The following is an example of the output:

```
## File Generation Notes
## Avaya Dynamic Configuration Service does not recognize User-Agent - Mozilla/5.0 (Windows)

SET SIPSECURE 0
SET SIPENABLED 1
SET SIPDOMAIN oceana.com
SET SIPUSERNAME 8831093
SET SIPHA1 70e9ab3f778a27d0012d725f941783c8
SET ACSPORT 8843
SET ACSSECURE 1
SET ACSENABLED 1
SET ACSSSO 1
SET SIP_CONTROLLER_LIST 10.133.34.202:5061;transport=TLS
SET ACSSRVR 10.133.34.204
SET SIPPROXYSRVR 10.133.34.202
SET SIPPORT 5061
SET LOCKED_PREFERENCES "SIPSECURE,SIPENABLED,SIPDOMAIN,SIPUSERNAME,SIPHA1,ACSPORT,ACSSECURE
SET OBSCURE_PREFERENCES ""
```

Avaya Aura® Media Server deployment

In an Avaya Oceana® deployment, you need to install one to three media servers depending on your feature requirements.

The following table lists the media servers that you can install as a part of your deployment:

Quantity	Purpose
1	Avaya Aura® Communication Manager
1	Avaya Breeze® platform
1	Avaya Aura® Web Gateway

For information about how to install and configure Avaya Aura® Media Server, see *Deploying Avaya Breeze® platform*. In the *Deploying Avaya Breeze® platform* document, see the section about the deployment of Avaya Aura® Media Server that contains installation and configuration procedures required for the deployment of Avaya Aura® Media Server.

Important:

- To support Web Video in Avaya Oceana®, you must install Avaya Aura® Media Server Release 8.0.
- After deploying Avaya Aura® Media Server, you must configure the Engagement Designer attributes so that you can use Avaya Aura® Media Server with Avaya Breeze® platform.

Install and configure Avaya Aura® Media Server for Avaya Breeze® platform

For information about how to install and configure Avaya Aura® Media Server, see *Deploying Avaya Breeze® platform*. In the *Deploying Avaya Breeze® platform* document, see the section

about the deployment of Avaya Aura® Media Server that contains installation and configuration procedures required for the deployment of Avaya Aura® Media Server.

Important:

To support Web Voice in Avaya Oceana®, you must install Avaya Aura® Media Server Release 7.8 with Profile 1.

For this release, Avaya Breeze® platform uses REST instead of SIP to communicate with Avaya Aura® Media Server. Therefore, Avaya Aura® Media Server requires enrollment with System Manager and configuration for REST operations. For more information, see the section about the deployment of Avaya Aura® Media Server in *Deploying Avaya Breeze® platform*.

For more information about how to install, update, implement, and administer Avaya Aura® Media Server, see:

- *Deploying and Updating Avaya Aura® Media Server Appliance*
- *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS*
- *Implementing and Administrating Avaya Aura® Media Server*

After deploying Avaya Aura® Media Server, you must configure the Engagement Designer attributes so that you can use Avaya Aura® Media Server with Avaya Breeze® platform.

Configuring Avaya Aura® Media Server media files for Web Voice

About this task

Avaya provides a sample Engagement Designer workflow for Web Voice that uses Avaya Aura® Media Server to play ringback, announcements, and music files. This procedure describes how to deploy sample media files for Web Voice. You must manually create the content namespace and group if they do not already exist. The available sample media files for Web Voice are:

Announcement	Media file name
Ringback	`RingBack.wav`
Welcome	`WelcomeCustomer.wav`
Wait music	`Wait.wav`
Please wait	`PleaseWait.wav`
Required resource unavailable	`RequiredResourceUnavailable.wav`
Update	`Update.wav`
Sorry	`Sorry.wav`
Maintenance mode	`MaintenanceMode.wav`

Note:

These media files are available to download from the Avaya DevConnect portal at http://www.avaya.com/devconnect. For information about downloading Avaya Oceana® resources from Avaya DevConnect, see *Avaya Oceana® Release Notes*.

Before you begin

Ensure that you have the Engagement Designer workflow for Web Voice and the accompanying Avaya Aura® Media Server media files.

Procedure

1. In your web browser, enter the following URL:

   `https://<Avaya Aura Media Server_FQDN>:8443/em`
2. In the **User ID** field, enter the User ID for logging in to Avaya Aura® Media Server.
3. In the **Password** field, enter the password for logging in to Avaya Aura® Media Server.
4. Click **Log in**.
5. In the navigation pane, click **Tools** > **Media Management**.
6. On the Media Management page, in the Content Namespaces section, click **Add**.
7. In the **Name** field, type `workflow` for the name of the content namespace.
8. Click **Save**.
9. In the navigation pane, click **Tools** > **Media Management**.
10. On the Media Management page, in the Content Namespaces section, select the content namespace.
11. Click **Browse**.
12. On the Provision Media page, in the navigation pane, select the content namespace.
13. Click **Add Content Group**.
14. In the New Content Group dialog box, in the **Name** field, type `media` for the name of the content group.
15. Click **Save**.
16. On the Provision Media page, in the navigation pane, select the **media** content group.
17. Click **Add Content Group**.
18. In the New Content Group dialog box, in the **Name** field, type `en_us` for the name of the content group.
19. Click **Save**.
20. In the navigation pane, click **Tools** > **Media Management**.
21. On the Media Management page, select the check box next to the content namespace.
22. Click **Browse**.
23. On the Provision Media page, expand the content namespace.
24. Select the content group to which you want to add a media file.
25. Click **Add Media**.
26. In the Add Media dialog box, click **Browse** and navigate to the Web Voice sample media files.
27. Select a file and click **Upload**.

28. Continue uploading all the media files to the **workflow** > **media** > **en_us** content namespace and group.

Deploying the sample Web Voice workflow

About this task

Avaya provides a sample workflow for the Web Voice channel. With this procedure, you can deploy the sample Web Voice workflow and configure the workflow attributes.

Before you begin

- Download the latest version of the sample workflow from PLDS.
- In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Designer Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. In the Import Workflow dialog box, click **Choose File**.
4. Browse to the folder containing the sample workflow, select the workflow, and click **Import**.
5. Click **Save Workflow**.
6. In the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaWebVoiceAssistedService`.

      You can provide any name for the workflow.

   b. Select the folder to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.
8. In the Deployment Details dialog box, click **OK**.

   Important:

   Ensure that you do not add unique information in the first five seconds of the initial announcement.

   A setup time associated with the Session Traversal Utilities for NAT (STUN) server specifies that the client cannot hear the first five seconds of the initial announcement. However, in the first five seconds of the initial announcement, you can add ring back or play music.

9. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

`https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

10. On the Workflows tab, verify that the OceanaWebVoiceAssistedService workflow is available in the list of deployed workflows.
11. On the Workflows tab, select the OceanaWebVoiceAssistedService workflow and click **Attributes**.
12. In the Workflow Attributes dialog box, do the following:
    a. In the **DefaultDestination** field, enter the value in the following format:

       <Number>@<Domain.com>

       The *<Number>* is the Fallback VDN that you created previously. For example, 8284103@domain.com.

    b. Click **Close**.

Configuring a Avaya WebRTC Connect service profile

About this task

Use this procedure to create a WebRTC Connect service profile for all WebRTC Connect contacts and all WebRTC Connect Transfer to Service for both Web Voice and Web Video.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Service Profiles**.
2. On the Service Profile Configuration page, click **New**.
3. On the Service Profile Editor page, perform the following steps:
   a. In the **Name** field, enter a name for the service profile.

      For example, WebRTCServiceProfile.

   b. Select the **All Services** tab.
   c. In the **Available Service to Add to this Service Profile** list, click the plus sign (**+**) for each of the following services to add the services to the service profile:
      - AvayaMobileCommunications
      - EngagementDesigner
   d. Click the **Service Invocation Details** tab.

      The **Called Service Invocation Order** list displays the services that you have added to the service profile.

   e. In the **Called Service Invocation Order** list, in the **Order: First to Last** column, click the arrows to move the services up or down in the invocation order of the call intercept services to ensure that the AvayaMobileCommunications service is invoked before EngagementDesigner.

4. Click **Commit**.

Changing the default password in Avaya Aura® Media Server

About this task

Use this procedure to change the default password in Avaya Aura® Media Server after completing the installation.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the login page, do the following:
   a. In the **User ID** field, type `admin` as the default user name.
   b. In the **Password** field, type `Admin123$` as the default password.
   c. Click **Sign In**.
3. Change the default password on the initial login.
4. **(Optional)** On the Avaya Aura® Media Server Element Manager interface, click **Account Management** > **Policies**, and change the required value in the fields in the Password area.
5. Click **Save**.

Installing Avaya Aura® Media Server updates

About this task

The OVA might not be the latest version. Therefore, you must install the applicable patches after installing the OVA.

The following are the two types of updates that must be installed:

- System software updates
- Avaya Aura® Media Server software updates

These updates are released in the ISO format.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the login page, enter the login credentials and click **Sign In**.
3. On the Avaya Aura® Media Server Element Manager interface, click **Tools** > **Manage Software** > **Updates**.

4. In the Upload Updates area, click **Choose File**.
5. Browse and select the system software ISO file and click **Upload**.
6. Accept the license agreement on the completion of the upload process.
7. In the Upload Updates area, click **Choose File**.
8. Browse and select the Avaya Aura® Media Server software ISO file and click **Upload**.
9. Accept the license agreement on the completion of the upload process.
10. Click **Install Updates**.

    The upgrade process takes several minutes to complete.

Setting up the Avaya Aura® Media Server cluster

Procedure

1. On the primary Avaya Aura® Media Server, do the following:
    a. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

       `https://<Avaya Aura Media Server_FQDN>:8443/em`

    b. On the login page, enter the login credentials and click **Sign In**.
    c. On the Avaya Aura® Media Server Element Manager interface, click **Cluster Configuration** > **Server Designation**.
2. Note the UUID.
3. Select the **Enable Replication Account** check box.
4. In the **Username** field, type `repluser`.
5. In the **Password** field, type `replpass`.
6. Click **Save**.
7. Confirm the Avaya Aura® Media Server restart.
8. On the secondary Avaya Aura® Media Server, do the following:
    a. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

       `https://<Avaya Aura Media Server_FQDN>:8443/em`

    b. On the login page, enter the login credentials and click **Sign In**.
    c. On the Avaya Aura® Media Server Element Manager interface, click **Cluster Configuration** > **Server Designation**.
9. In the **Role** field, select `Secondary`.
10. In the **Primary Server UUID** field, enter the UUID you note from the primary server.
11. In the **Primary Server Address** field, enter the IP address of the primary server.

12. Select the **Enable Replication Account** check box.
13. In the **Username** field, type `repluser`.
14. In the **Password** field, type `replpass`.
15. Click **Save**.
16. Confirm the Avaya Aura® Media Server restart.
17. On the standard Avaya Aura® Media Server, do the following:
    a. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

       `https://<Avaya Aura Web Gateway_FQDN>:8443/emlogin`

    b. On the login page, enter the login credentials and click **Sign In**.
    c. On the Avaya Aura® Media Server Element Manager interface, click **Cluster Configuration** > **Server Designation**.
18. In the **Role** field, select `Standard`.
19. On the primary server, click **Cluster Configuration** > **Server Designation**.
20. In the Standard Designation area, verify that all servers are listed.
21. On the primary server, click **System Status** > **Cluster Status** to reverify all servers.

Enrolling Avaya Aura® Media Server with System Manager

About this task

Use this procedure to enroll Avaya Aura® Media Server with System Manager.

Before you begin

On the Avaya Aura® Media Server Element Manager interface, click **System Configuration** > **Network Settings** > **Name Resolution** and add an entry to map System Manager FQDN to its IP address.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the login page, enter the login credentials and click **Sign In**.
3. On the Avaya Aura® Media Server Element Manager interface, click **Security** > **System Manager** > **Enrollment**.
4. On the System Manager Enrollment page, enter names and descriptions for the Avaya Aura® Media Server node and Avaya Aura® Media Server cluster.

   For clustered systems, you must enter the name and description of each node in the cluster.

5. Click **Next**.
6. Enter the FQDN of System Manager.

   Important:

   Do not enter the IP address instead of FQDN.
7. Enter the administrator user name and password for System Manager.
8. Click **Next**.
9. Select the option for creating a new System Manager signed certificates and click **Next**.
10. Enter the details of the certificate.
11. Select the **Include Subject Alternative Name with IP address** check box.
12. Include Subject Alternative Name with FQDN
13. Enter the System Manager enrollment password.

    On the completion of the enrollment, Avaya Aura® Media Server Element Manager automatically logs you out.

    Enrollment switches the Avaya Aura® Media Server to a single sign-on mode. Therefore, you must log in to Avaya Aura® Media Server Element Manager through System Manager.
14. **(Optional)** To enable standard login to Avaya Aura® Media Server Element Manager, click **Account Management** > **Policies** and set the **Authentication and authorization source** to `Avaya Aura® Media Server`.

Configuring security certificates

About this task

Use this procedure to configure security certificates for Avaya Aura® Media Server nodes.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`
2. On the login page, enter the login credentials and click **Sign In**.
3. On the Avaya Aura® Media Server Element Manager interface, click **Security** > **Certificate Management** > **Key Store**.
4. In the Service Profiles area, click **Assign**.
5. For each field, select the System Manager-generated certificate.

   The System Manager-generated certificate ends with `_signed`.
6. Click **Save**.
7. Click **Confirm** to restart.

8. Repeat Steps 1 to 7 for all Avaya Aura® Media Server nodes in the cluster.

Configuring Avaya Aura® Media Server

About this task

For clustered systems, you must do these configurations on the primary Avaya Aura® Media Server node. After you complete these configurations on the primary node, they are automatically propagated to the other Avaya Aura® Media Server nodes in the cluster.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server FQDN>:8443/emlogin`

2. On the login page, enter the login credentials and click **Sign In**.
3. On the Avaya Aura® Media Server Element Manager interface, click **Licensing** > **General Settings**.
4. In the **Server Host Name or IP Address** field, enter the IP address of System Manager.
5. Click **Save**.
6. Restart the Avaya Aura® Media Server node.
7. Log in to Avaya Aura® Media Server Element Manager.
8. On the Avaya Aura® Media Server Element Manager interface, click **Licensing** > **Monitoring**.
9. Verify that the **License Status** field is set to `License Acquired`.
10. Click **System Configuration** > **Network Settings** > **General Settings**.
11. In the SOAP area, in the **Trusted Nodes** field, enter the IP address of System Manager.
12. In the Connection Security area, in the **TLS Version** field, select `TLSv1.2`.
13. In the Connection Security area, clear the **Verify Host Name of TLS Client Connections** check box.
14. Click **Save**.
15. Click **System Configuration** > **Signaling Protocols** > **REST** > **General Settings**.
16. Clear the **Basic Authentication** check box.
17. Click **Save**.
18. Click **System Configuration** > **Server Profile** > **General Settings**.
19. Select the **Video Media Processor** check box.
20. Click **Save**.
21. Click **System Status** > **Element Status**.

22. Click **Restart**.
23. Click **Confirm** to restart.

Assigning a location to media servers

About this task

Use this procedure to assign a location to media servers in System Manager.

Procedure

1. On the System Manager web console, click **Elements** > **Media Server** > **Server Administration**.
2. Verify the entry for each installed media server.
3. Select the entry for a media server and click **Edit**.
4. In the **Location** field, assign the appropriate location to the media server.
5. Repeat Steps 3 and 4 for all media servers.

Configure Avaya Aura® Media Server for Avaya Breeze® platform

The configuration of Avaya Aura® Media Server for Avaya Breeze® platform includes the following:

- Configure Avaya Aura® Media Server for Web Voice.
- Configure sample Engagement Designer workflow for Web Voice.

  The workflow uses canned Avaya Aura® Media Server to play ringback, announcements, and music files for Video contacts. These media files are available to download from the Avaya DevConnect portal at http://www.avaya.com/devconnect.
- Create the Avaya Aura® Media Server content namespace and group if they do not already exist, and upload media prompts into the namespace.

  Without the sample media files for Web Voice, you cannot route Video contacts.

Note:

For PSTN calls, Avaya Aura® Media Server for Avaya Breeze® platform is not required. Customers can have IVR on Experience Portal to play wait treatment and route the call to an agent.

Configuring audio codecs for Web Voice in Avaya Aura® Media Server

About this task

Use this procedure to configure audio codecs for Web Voice in Avaya Aura® Media Server for Avaya Breeze® platform.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

`https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the login page, enter the login credentials and click **Sign In**.
3. On the Avaya Aura® Media Server Element Manager interface, click **System Configuration** > **Media Processing** > **Audio Codes**.
4. Use the **Up** button to move the G.711-ULAW and G.711-ALAW codecs to the top of the **Enabled** list.
5. Click **Save**.

Configuring video codecs for Web Video in Avaya Aura® Media Server

About this task

Use this procedure to configure video codecs for Web Video in Avaya Aura® Media Server for Avaya Breeze® platform.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the login page, enter the login credentials and click **Sign In**.
3. On the Avaya Aura® Media Server Element Manager interface, click **System Configuration** > **Media Processing** > **Video Codes**.
4. Select the **Firewall NAT Tunneling Media Processor** and **Video Media Processor** check boxes.
5. Click **Save**.

Deploying Web Voice and Video prompts to Avaya Aura® Media Server

About this task

Use this procedure to deploy Web Voice and Video prompts to Avaya Aura® Media Server.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the login page, enter the login credentials and click **Sign In**.
3. On the Avaya Aura® Media Server Element Manager interface, click **Tools** > **Media Management**.
4. On the Media Management page, click **Add**.
5. In the **Name** field, type `workflow`.

6. On the Media Management page, select the check box for the workflow namespace and click **Browse**.
7. On the Provision Media page, select the workflow namespace and click **Add Content Group**.
8. In the New Content Group dialog box, in the **Name** field, type `media` and click **Save**.
9. On the Provision Media page, select the media content group and click **Add Content Group**.
10. In the New Content Group dialog box, in the **Name** field, type `en_us` and click **Save**.
11. On the Provision Media page, select the en_us content group and click **Add Media**.
12. In the Add Media dialog box, add all the media `.wav` files.

Configure Avaya Aura® Media Server for Avaya Aura® Web Gateway

Configuring server profile and video codecs for Web Video

About this task

Use this procedure to configure server profile and video codecs for Web Video.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server FQDN>:8443/emlogin`
2. On the login page, enter the login credentials and click **Sign In**.
3. On the Avaya Aura® Media Server Element Manager interface, click **System Configuration** > **Service Profile** > **General Settings**.
4. Select the **Firewall NAT Tunneling Media Processor** and **Video Media Processor** check boxes.
5. Click **System Configuration** > **Service Profile** > **Advanced Settings**.
6. Select the following check boxes:
   - **Firewall NAT Tunneling Media Processor**
   - **Media Server**
   - **Reporting Agent**
   - **SIP UserAgent**
   - **Video Media Processor**
   - **VoiceXML Interpreter**
7. Click **Save**.

Configuring network settings

About this task

Use this procedure to configure network settings for Avaya Aura® Media Server.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the login page, enter the login credentials and click **Sign In**.
3. On the Avaya Aura® Media Server Element Manager interface, click **System Configuration** > **Network Settings** > **General Settings**.
4. Select the following check boxes:
   - **Verify Host Name on HTTPS Client Connections**
   - **Verify Host Name of the Remote DB secure connection**
5. Click **Save**.

Configuring signaling protocols

About this task

Use this procedure to configure signaling protocols in Avaya Aura® Media Server.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the login page, enter the login credentials and click **Sign In**.
3. On the Avaya Aura® Media Server Element Manager interface, click **System Configuration** > **Signaling Protocols** > **SIP** > **Nodes and Routes**.
4. On the SIP Nodes and Routes page, in the Trusted Nodes area, verify the Avaya Aura® Web Gateway IP address and cluster FQDNs.
5. Click **System Configuration** > **Signaling Protocols** > **REST** > **General Settings**.
6. Select the **Enable TLS Mutual Authentication** check box.
7. Click **Save**.

Avaya Aura® Web Gateway deployment and configuration

Avaya Oceana® requires Avaya Aura® Web Gateway to provide WebRTC Connect Signaling Gateway services to Video-enabled SIP agents through a browser endpoint.

Prerequisites for Avaya Aura® Web Gateway

The following are the prerequisites for Avaya Aura® Web Gateway:

- Avaya Aura® Media Server
- LDAP/Active Directory

  You can also use a shared Active Directory.
- System Manager details
- Avaya Aura® Device Services

Important:

To support external mobile client access for Voice and Video, you must install the latest compatible patch of Avaya Aura® Web Gateway over Avaya Aura® Web Gateway 3.8.

Deploying Avaya Aura® Web Gateway

For more information about how to deploy and administer Avaya Aura® Web Gateway, see the following documents on Avaya Support website at http://support.avaya.com:

- *Deploying the Avaya Aura® Web Gateway*
- *Administering the Avaya Aura® Web Gateway*

Important:

- Use lowercase FQDNs and hostnames while deploying Avaya Aura® Web Gateway.
- To use Avaya Aura® Web Gateway, you must have a valid license installed in System Manager. If you do not have a previously installed license, generate a new license and load the license in System Manager.

Adding a device to System Manager

About this task

Use this procedure to add the Avaya Aura® Web Gateway element in System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, click **New**.
3. On the New Elements page, in the **Type** field, select `Avaya Aura Web Gateway`.
4. In the **Name** field, enter the name of your device.
5. In the **Node** field, enter the IP address of your device.

6. In the **Name** field, type `SSO`.
7. In the **Access Profile Type** field, select `EMURL`.
8. In the **Host** field, enter the FQDN of the server.
9. In the **Port** field, type `8445`.
10. In the **Path** field, type `/admin`.
11. Click **Save**.
12. Click **Commit**.

Configuring Avaya Aura® Web Gateway

About this task

Use this procedure to configure Avaya Aura® Web Gateway.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. Log on to Avaya Aura® Web Gateway administration portal with the credentials of the user assigned to the admin group on LDAP.

   Use the complete login name in the `user@domain` format.

3. In the navigation pane, click **General Network Settings** > **System Manager**.
4. In the **FQDN** field, enter the FQDN of System Manager.
5. In the **Protocol** field, select `https`.
6. In the **Username** field, enter the user name of the System Manager administrator account.
7. In the **Password** field, enter the password of the System Manager administrator account.
8. Click **Save**.
9. In the navigation pane, click **General Network Settings** > **Device Services**.
10. In the **FQDN** field, enter the FQDN of Avaya Aura® Device Services and click **Save**.
11. In the navigation pane, click **General Network Settings** > **LDAP Configuration**.
12. Enter the appropriate value in all fields.

    To enter the value in the fields, see the Avaya Aura® Device Services LDAP configuration.

13. Enter the appropriate value in the **Base Context DN**, **Administrator Role**, and **User Role** fields and click **Save**.
14. In the navigation pane, click **General Network Settings** > **Media Services**.

15. Verify that the page displays the details of the dedicated Avaya Aura® Media Server for Avaya Aura® Web Gateway.
16. In the navigation pane, click **Security Settings** > **HTTP Clients**.
17. In the **REST** field, change the value to `OPTIONAL` and click **Save**.
18. In the navigation pane, click **External Access** > **Guest SIP Proxy**.
19. In the Guest SIP Domain area, in the **Default Guest Sip Domain** field, enter the appropriate SIP domain and click **Save**.
20. In the Guest SIP Proxy area, do the following:
    a. Click **Add**.
    b. In the **SIP Address** field, enter the SIP IP Address of Session Manager.
    c. In the **Weight** field, type `100`.
    d. In the **SIP Port** field, type `5061`.
    e. In the **SIP Protocol** field, select `TCP`.
    f. In the **Location** field, select the appropriate location.
    g. Click **Save**.
21. In the navigation pane, click **Security Settings** > **Trusted Hosts**.
22. In the Trusted Hosts area, add the following entries by clicking **Add**:
    - IP address of Avaya Aura® Device Services
    - FQDN of Avaya Aura® Device Services
    - IP address of Session Manager
    - Self FQDN of Avaya Aura® Web Gateway
    - FQDN of System Manager
    - FQDNs of Avaya Breeze® platform nodes
23. Click **Save**.
24. In the navigation pane, click **Security Settings** > **Session Security**.
25. In the Cipher Support area, select all ciphers for media encryption and click **Save**.
26. In the navigation pane, click **Advanced** > **CORS Configuration**.
27. Select the **Enable Cross-Origin Resource Sharing** and **Allow access from any origin** check boxes and click **Save**.
28. In the navigation pane, click **General Network Settings** > **Location**.
29. In the Web Gateway Locations area, select a location for the Web Gateway and click **Save**.

    The location might take some time to appear because it must be synchronized from System Manager.

30. In the navigation pane, click **Advanced** > **Media Settings** > **Audio**.
31. In the WebRTC Audio Codecs area, verify that G711A and G711MU are prioritized and placed on the top.
32. In the navigation pane, click **Advanced** > **Media Settings** > **Video**.
33. In the **Call Maximum Video Bandwidth (kbps)** field, change the value to `768`.

Verifying the components connected to Avaya Aura® Web Gateway

About this task

Use this procedure to verify that all configured components are successfully connected to Avaya Aura® Web Gateway.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. Log on to Avaya Aura® Web Gateway administration portal with the credentials of the user assigned to the admin group on LDAP.

   Use the complete login name in the `user@domain` format.

3. In the content pane, in the Solution Servers area, verify that the status of the following components is `Connected`:

   - **LDAP Configuration**
   - **Device Services**
   - **System Manager**
   - **Media Services**

Configuring Avaya Aura® for Avaya Aura® Web Gateway

About this task

Use this procedure to configure Avaya Aura® components for Avaya Aura® Web Gateway through System Manager.

Procedure

1. On the System Manager web console, click **Elements** > **Media Server** > **Application Assignment**.
2. On the Application Assignment page, select **Avaya Aura Web Gateway** and click **Edit**.
3. Select an available Avaya Aura® Media Server cluster.

   Select a cluster that does not have an asterisk (*) mark.

4. Click **Commit**.
5. On the System Manager web console, click **Elements** > **Media Server** > **Server Administration**.
6. On the Server Administration page, ensure that the location of each media server in the new Avaya Aura® Web Gateway media server cluster is set.
7. In your web browser, enter the following URL to log on to Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`
8. Log on to Avaya Aura® Web Gateway administration portal with the credentials of the user assigned to the admin group on LDAP.

   Use the complete login name in the `user@domain` format.
9. In the navigation pane, click **Security Settings** > **Trusted Hosts**.
10. In the Trusted Hosts area, add the following entries by clicking **Add**:
    - FQDN of Avaya Aura® Web Gateway
    - FQDN of Avaya Aura® Device Services
    - FQDN of System Manager
    - FQDNs of the media servers in the cluster assigned to Avaya Aura® Web Gateway
11. On the System Manager web console, click **Elements** > **Routing** > **SIP Entities**.
12. On the SIP Entities page, click **New**.
13. In the **Name** field, enter a name for the Avaya Aura® Web Gateway entity.
14. In the **IP address** field, enter the IP address if Avaya Aura® Web Gateway.
15. In the **Type** field, select `SIP Trunk`.
16. In the **Location** field, select the appropriate location.
17. In the **Time Zone** field, select the appropriate time zone.
18. In the **SIP Link Monitoring** field, select `Link Monitoring Disabled`.
19. In the **CRLF Keep Alive Monitoring** field, select `CRLF Monitoring Disabled`.
20. In the Entity Links area, click **Add**.
21. In the **SIP Entity 1** field, select the Session Manager SIP entity.
22. Click **Commit**.

Enabling Token Service and TestApp

About this task

Use this procedure to enable Token Service and TestApp in Avaya Aura® Web Gateway.

Procedure

1. Using an SSH client, log on to Avaya Aura® Web Gateway.
2. Run the following commands:

   cdto active

   cd mss/*/telportal/webapps

   sudo mv devclient.undeploy devclient.war; sudo mv token-generation-service.undeploy token-generation-service.war
3. Run the following command to restart Avaya Aura® Web Gateway services:

   svc CSA restart

   The restart process might take several minutes to complete.

Testing the installation of Avaya Aura® Web Gateway

About this task

Use this procedure to test the installation of Avaya Aura® Web Gateway through TestApp.

Before you begin

Enable Avaya Aura® Web Gateway Token Service and TestApp.

Procedure

1. In your web browser, enter the following URL to start Avaya Aura® Web Gateway TestApp:

   `https://<Avaya Aura Web Gateway_FQDN>/devclient/testapp/index.html`

   Where *<Avaya Aura Web Gateway_FQDN>* is the FQDN of the Avaya Aura® Web Gateway server.
2. When prompted, enter the login credentials of a valid agent as defined in LDAP.

   The browser displays the Avaya Aura® Web Gateway TestApp console with some text in green.
3. Type **ac<return>**.

   The browser displays several lines of text in green.

   For example, `<= serviceStatusChanged: calls service activated`.

   The lines indicate that Avaya Aura® Web Gateway is installed correctly.

Enabling port for remote access on Avaya Aura® Web Gateway HTTP Reverse Proxy

About this task

Use this procedure to enable port for remote access on Avaya Aura® Web Gateway HTTP Reverse Proxy.

This procedure is required only for the remote worker agent configuration.

Procedure

1. In your web browser, enter the following URL:

   https://<Avaya Aura Web Gateway_FQDN>:8445/admin
2. On the Avaya Aura® Web Gateway administration portal, click **External Access** > **HTTP Reverse Proxy**.
3. Select the **Use Front-end Host from a client request** check box.
4. Select the **Enable port for remote access** check box.
5. In the **Front-end port for remote access** field, enter a port number.

   For example, enter a port number similar to 8444.

   Avaya Aura® Web Gateway uses this port number to distinguish between clients on the internal network and external clients on the internet. Internal clients use the standard 443 port whereas external clients such as Browsers, Android, and iOS use the port specified in this field to access Avaya Aura® Web Gateway. Based on the port number, Avaya Aura® Web Gateway sets the media paths.
6. Click **Save**.

Troubleshooting the TestApp issues

Troubleshooting Error 401

Condition

Error 401 unauthorized.

Cause

The port number in the earlier release of Avaya Aura® Web Gateway was 8443, which is no longer valid for the latest release.

Solution

Change the port number to 8445.

Troubleshooting the activation issue

Condition

Unable to activate.

Cause

Session Manager might not be configured to use System Manager certificates.

Solution

Configure Session Manager to use System Manager certificates.

Avaya Aura® Web Gateway authorization

When a request is made between a client and the Avaya Aura® Web Gateway server, an authorization token is passed with the request. This authorization token is the same token that Avaya Workspaces passes with the requests to Unified Agent Controller (UAC). The authorization is handled through AuthorizationService.

Avaya Aura® Web Gateway is a third-party server. Therefore, you must configure the Avaya Breeze® platform Authorization Certificate on Avaya Aura® Web Gateway. However, it creates a conflict because each Avaya Breeze® platform node in the cluster has a different Authorization Certificate.

When load balancing is enabled between the nodes, some requests are rejected because they cannot be authorized. Therefore, you must create a single, shared certificate that you can use for authorization on all nodes in the cluster.

For information about how to create the common certificate and import it in Avaya Breeze® platform nodes, see:

- Creating the common client certificate on page 427
- Creating the common server certificate on page 428
- Importing the authorization certificate on page 88

Configure the voice media path

Configuring codecs in Avaya Aura® Web Gateway

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. On the Avaya Aura® Web Gateway administration portal, click **Advanced** > **Media Settings** > **Audio**.
3. Click **Custom SIP Audio Coded Preference**.
4. From the **SIP Audio Codecs** list, remove all codecs except your preferred G711 codec, such as G711A or G711MU.
5. From the **WebRTC Audio Codecs** list, remove all codecs except your preferred G711 codec, such as G711A or G711MU.
6. Click **Save**.
7. On the Avaya Aura® Web Gateway administration portal, click **Advanced** > **Media Settings** > **Video**.
8. From the **SIP Video Codecs** list, remove all codecs except the H264 codec.

9. From the **WebRTC Audio Codecs** list, remove all codecs except the H264 codec.
10. Set the **Call Maximum Video Bandwidth** field to `768` kbps.
11. Click **Save**.

Prioritizing codecs in Avaya Aura® Media Server

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server Gateway_FQDN>:8443/emlogin`

2. On the Avaya Aura® Media Server Element Manager interface, click **System Configuration** > **Media Processing** > **Audio Codecs**.
3. Use the **Up** button to move your preferred G711 codec to the top of the **Enabled** list.
4. Click **Save**.

Prioritizing codecs in Communication Manager

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Identify the Far-end Network Region assigned to the signaling group intended to process calls from Avaya Aura® Web Gateway.
3. Identify the ip-codec-set associated with the Far-end Network Region that you identify.
4. Run the **`change ip-codec-set <codec set number used by the SIP signaling group>`** command.
5. On page 1, in the **Audio Codec** area, verify that your preferred G711 codec (G.711A or G.711MU) is at number on the list.
6. **(Optional)** If the signaling group intended to process calls from or to Avaya Breeze® platform is different, repeat Step 1 to Step 5 for that signaling group.

Creating Avaya WebRTC Connect agents for Avaya Oceana®

Creating a user in Active Directory

About this task

Use this procedure to create a user in Active Directory who can act as a general user for Avaya Aura® Device Services, and can also administer Avaya Aura® Device Services and Avaya Aura® Web Gateway.

Procedure

1. Log in to the server containing the Active Directory.
2. Click **Start** > **Administrative Tools** > **Active Directory Users and Computers**.
3. In the navigation pane, expand the domain that you created for the users.
4. Right-click the Active Directory organizational unit (OU) and click **New** > **User**.
5. In the **New Object - User** dialog box, do the following:
    a. In the **First name** field, enter the first name of the user.
    b. In the **Last name** field, enter the surname of the user.
    c. In the **User logon name** field, enter the user name.
    d. Click **Next**.
    e. In the **Password** field, enter a password for the user.
    f. In the **Confirm Password** field, re-enter the password.
    g. Clear the **User must change password at next logon** check box.
    h. Select the **Password never expires** check box.
    i. Click **Next**.
    j. Click **Finish**.

    The server displays the new user in the list in the content pane.
6. In the content pane, right-click the new user and click **Add to a group**.
7. In the Select Groups dialog box, add the user to the standard users group and the appropriate administrator group, and click **OK**.

Create a user in System Manager and Communication Manager

The following are the two methods that you can use to create users:

- Create users manually through System Manager
- Create an XML file containing users and import them into System Manager through the bulk import utility

Creating a user through System Manager

About this task

Use this procedure to manually create a user through System Manager.

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, click **New**.

   System Manager displays the User Profile | Add page.
3. In the **Last Name** field, enter the surname of the user.
4. In the **First Name** field, enter the first name of the user.
5. In the **Login Name** field, enter the login name of the user, including the domain name.
6. In the **Password** and **Confirm Password** fields, enter the password.
7. In the **Language Preference** field, select the preferred language of the user.
8. In the **Timezone** field, select the timezone of the user.
9. Click **Commit and Continue**.
10. In the **Communication Profile Password** field, click **Edit** and enter the password.
11. In the Communication Address area, click **New**.
12. Leave the **Type** field as `Avaya SIP`.
13. In the **Fully Qualified Address** field, enter the SIP address of the user station.
14. In the **Domain** field, choose the appropriate domain.
15. Click **Add**.
16. Select the **Session Manager Profile** check box.
17. In the Primary Session Manager field, select the primary Session Manager.
18. In the **Originating Sequence** and **Terminating Sequence** fields, select `CMApp`.
19. In the **Home Location** field, select the appropriate value.
20. Select the **CM Endpoint Profile** check box.
21. In the **System** field, select `CM`.
22. Leave the **Profile Type** field as `Endpoint`.
23. In the **Extension** field, enter the SIP address of the user station.
24. In the **Template** field, select the appropriate template based on the version of Communication Manager.
25. In the **Preferred Handle** field, select the communication address of the user.
26. Click **Endpoint editor**.

27. On the General Options tab, ensure that the **Type of 3PCC Enabled** field is set to `Avaya`.
28. On the Feature Options tab, do the following:
    a. Select the **IP Softphone** check box.
    b. Select the **IP Video Softphone** check box.
    c. Clear the **H.320 Conversion** check box.
    d. Select the **Direct IP-IP Audio Connections** check box.
29. On the Button Assignment tab, set the button features in the following way:

Button Feature	Argument-1	Argument-2
manual-in		
call-appr		
call-appr		
call-appr		
aux-work		
auto-in		
agnt-login		

30. Click **Done**.
31. Click **Commit**.

Creating System Manager users through bulk import utility

About this task

Use this procedure to create System Manager users through bulk import utility.

Procedure

1. Create a user bulk import XML file using the template.
2. Save the XML file on your local machine.
3. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
4. On the Manage Users page, click **More Actions** > **Import Users**.
5. Click **Browse** and select the XML file.
6. Click **Import**.

Creating users in Avaya Control Manager

Synchronizing users with Avaya Control Manager

About this task

The synchronization process synchronizes the user information from Communication Manager in to the Avaya Control Manager database.

Procedure

1. Log in to the Avaya Control Manager server.
2. On the Avaya Control Manager server, go to the `<install_path>\Avaya\Avaya Control Manager <version>\Services\ACCCM Synchronizer` folder.
3. Right-click the `NAV360_Synchronizer` file and click **Run as administrator**.
4. In the **Sync Type** field, select `CM`.
5. In the **Import Mode** field, select `Sync`.

   Important:

   Do not start the synchronization process with the **Import Mode** field set to `Initial`.
6. Click **Start** to start the synchronization process.
7. Click **Yes** on the confirmation screen.

Making the user station available

About this task

Use this procedure to make the user station available.

Procedure

1. Log on to Avaya Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. Double-click the administered Avaya Oceana® UCA server, or select the administered Avaya Oceana® UCA server and click **Edit**.
4. On the Avaya Oceana Server Edit page, click the **Extensions** tab.
5. Move the stations for the newly created users from the **Available Extensions** list to the **Selected Extensions** list.
6. Click **Save**.

Creating attributes for the users in Avaya Control Manager

About this task

Use this procedure to create attributes for the users in Avaya Control Manager.

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™** > **Work Assignment**.
2. On the Attribute Categories tab, click **Add**.
3. On the Attribute Category tab, do the following:
   a. In the **Name** field, enter the name of the category.

      For example, Language.

b. Click **Save**.

4. On the Attributes tab, click **Add**.
5. On the Attribute tab, do the following:
   a. In the **Attribute Category** field, select the attribute category that you create.

      For example, type `Language` or `Location`.

   b. In the **Attribute Value** field, enter a value for the attribute.

      For example, type `English` or `Inhouse`.

   c. Click **Save**.

Creating a user in Avaya Control Manager

Before you begin

- Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.
- For each Avaya WebRTC Connect agent, ensure the following on Communication Manager:
  - On page 2 of the STATION screen, the **Auto Answer** field is set to `none`.
  - On page 1 of the AGENT LOGINID screen, the **Auto Answer** field is set to `none`.

Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.
3. Click **Add**.
4. Enter appropriate value in each of the following fields:
   a. In the Available applications section, select the **Avaya Oceana** check box.
   b. In the **Team** field, select the available option.
   c. In the **First Name (English)** field, enter the first name of the user in English.
   d. In the **Surname (English)** field, enter the surname of the user in English.
   e. In the **LDAP Username** field, enter the LDAP user name of the user.

      The LDAP user name must be in the username@domain.com format. This user name is used for logging on to Avaya Workspaces.

   f. In the **Username** field, enter a user name.

      In this release, the user name is the internal handle.

   g. In the **Password** field, enter a password.

      This password is used for logging on to Avaya Control Manager.

   h. In the **Confirm Password** field, re-enter the password.
   i. In the **AVAYA Login** field, enter the SIP address of the agent.

      When creating an agent, if the **Profile** field is set to **Agent** and the **AVAYA Login** field is populated, then this agent is added to Elite. However, if the **AVAYA Login** field

is not populated, then this agent is not added to Elite. Therefore, the agent cannot handle Avaya Oceana® Voice contacts. This type of agent can handle only Multimedia contacts.

j. In the **Extension** field, enter the station associated with this agent.

This is used when logging on to Avaya Workspaces.

Note:

You must enter a value in this field only if the agent has to handle Voice contacts.

k. Click **Save**.

5. Scroll to the right and select the **Avaya Oceana** tab.
6. Select the channels to be assigned to the WebRTC Connect agent.

For example, select the **Video** check box to allow receipt of video calls.

7. Select the **Allow browser only login** check box.
8. Click **Save**.
9. Scroll to the right and select the **Attributes** tab.
10. Move the required attributes from the **Available Attributes** list to the **Agent Attributes** list.
11. Click **Save**.

Upgrading an existing agent for Web Video

About this task

Use this procedure to upgrade an existing agent so that the agent can receive video calls.

Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.
3. Select a user and click **Edit User**.
4. Scroll to the right and select the **Avaya Oceana** tab.
5. Select the **Video** check box.
6. Click **Save**.
7. Click **OK**.

Removing video capability from an existing agent

About this task

Use this procedure to remove the video capability from an existing agent so that the agent does not receive video calls.

Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.
3. Select the required user and click **Edit User**.
4. Scroll to the right and select the **Avaya Oceana** tab.
5. Clear the **Video** check box.
6. Click **Save**.
7. Click **OK**.

Chapter 25: Configure Avaya Oceana® with web and mobile voice calls

Checklist for configuring Avaya Oceana® with web and mobile voice calls

Use the following checklist to configure Avaya Oceana® with web and mobile voice calls so that phone-enabled agents can answer web and mobile voice calls:

No.	Task	Description	✔
1	Install and configure Avaya Aura® Web Gateway and Avaya Aura® Media Server.	See the following: • Avaya Aura Web Gateway deployment and configuration on page 400. • Avaya Aura Media Server deployment on page 386.	
2	Install and configure web and mobile applications to make anonymous calls to Avaya Aura® Web Gateway.	See Install and configure web and mobile applications on page 417.	
3	Install and configure Avaya Aura® Session Border Controller to enable calls from the public internet.	See Install and configure Avaya Aura Session Border Controller on page 425.	
4	Configure Avaya Breeze® platform so that voice calls can be anchored on Avaya Breeze® platform with wait treatment.	See Install and configure Avaya Aura Media Server for Avaya Breeze platform on page 386.	
5	Route web and mobile voice calls to Avaya WebRTC Connect Engagement Designer workflows sequencing the AvayaMobileCommunications service.	See Route web and mobile voice calls to Avaya WebRTC Connect workflows on page 443.	

Table continues…

No.	Task	Description	✔
6	Configure the voice media path.	See the following: • Configuring codecs in Avaya Aura Web Gateway on page 407. • Prioritizing codecs in Avaya Aura Media Server on page 408. • Prioritizing codecs in Communication Manager on page 408.	
7	Configure the transfer to service feature for web and mobile voice calls.	See Configure the transfer to service feature for web and mobile voice calls on page 452.	

Install and configure web and mobile applications

Avaya supplies the following web and mobile applications or reference clients for making anonymous calls to Avaya Aura® Web Gateway:

- Javascript reference client for web browsers

  Note:

  Web browsers are supported on the Windows desktop platform only.
- iOS reference client for iOS devices
- Android reference client for Android devices

To make anonymous calls to Avaya Aura® Web Gateway, you must install and configure these applications on the relevant platform.

Installing the Javascript reference client

Before you begin

Ensure that you have the free base-level registered membership of Avaya DevConnect Program. For information about Avaya DevConnect, see *Avaya DevConnect Program Guide* available on https://support.avaya.com.

Procedure

1. Download the JavaScript reference client, `OceanaReferenceClient.zip`, from the Avaya DevConnect portal at http://www.avaya.com/devconnect.
2. To use the JavaScript reference client, extract the relevant archive retrieved in the previous step and copy the folder to the customer-provided web server.

   The JavaScript reference client is now reachable on the customer web server.

Configuring the Javascript reference client and making a call

Before you begin

Ensure that the following certificates are installed on the client computer:

- A trust certificate for System Manager that manages the cluster containing Avaya Mobile Communications Snap-in.
- A trust certificate for Avaya Aura® Device Services using the link: `https://<Avaya Aura Device Services_FQDN>/acs/resources`.
- A trust certificate for Avaya Aura® Web Gateway using the link: `https://<Avaya Aura Web Gateway_FQDN/csa/resources/tenants/default`.

Procedure

1. In your web browser, enter the following URL:

   `https://<IP Address>/OceanaReferenceClient/index.html`

   `<IP Address>` is the IP address of the server hosting the Reference Client web application.
2. On the Click to Call screen, click the Hamburger menu on the left.
3. In the navigation pane, click **Settings**.
4. In the CONFIG section, do the following:
   a. In the **AMC Cluster Address** field, enter the address of the cluster containing Avaya Mobile Communications Snap-in.
   b. In the **AMC Cluster Port** field, type one of the following values based on the protocol that the reference client uses when connecting to the cluster containing Avaya Mobile Communications Snap-in:
      - Type `80` for HTTP.
      - Type `443` for HTTPS.
   c. In the **AMC Url Path** field, leave the default value, `services/AvayaMobileCommunications/sessions/`.
   d. In the **Display Name** field, enter the customer display name.
   e. In the **From Address** field, enter the customer address.

      The from address must be a numeric value. If you do not specify a from address, it is randomly assigned for each call.
   f. In the **Destination Address (Optional)** field, enter the number to make direct station/agent calls.

      The direct station/agent calls are the calls that are not routed through Avaya Oceana®.

      Important:

      This step is for debug purposes only and must be left empty by default.

g. In the **Context (Optional)** field, enter the customer specific information.

h. In the **Topic (Optional)** field, enter the customer specific information.

5. In the AAWG CONFIG section, do the following:

   a. In the **AAWG Server Address** field, enter the FQDN of the Avaya Aura® Web Gateway server.

   b. In the **AAWG Server Port** field, type one of the following values:

      - Type `80` for HTTP.
      - Type `443` for HTTPS.

   c. Configure the **Use HTTPS** field to enable security.

6. In the SERVICE section, configure appropriate values in the **Priority**, **Locale**, and **Strategy** fields and also configure the routing attributes for the selection of an agent.

   - To add an attribute, click the plus icon (**+**) in the table header row and enter the attribute details.
   - To delete an attribute, click the bin icon in the attribute row.
   - To edit an existing attribute, click the pencil icon in the attribute row.

7. **(Optional)** In the RESOURCE section, do the following:

   a. In the **Source Name** field, enter the name of the Voice provider to which the agent is associated.

   b. In the **Resource Id** field, enter the Native Resource ID of the agent.

      To get the Voice provider name, you must log on to Avaya Control Manager and access the Providers tab on the Avaya Oceana Server Edit page.

   Perform this step only if you use the Specified (Required or Preferred) Resource or Coverage feature for Web Voice.

8. In the TOKEN CONFIG section, do the following:

   a. In the **Token Service Address** field, enter the FQDN of the web server that is hosting the token service.

   b. In the **Token Service Port** field, enter the port number of the web server that is hosting the token service.

   c. In the **Use HTTPs** field, do one of the following based on the protocol that the reference client uses when connecting to the web server that is hosting the token service:

      - Move the slider to the left for HTTP.
      - Move the slider to the right for HTTPS.

   d. In the **Token Server Url Path** field, enter the URL path to connect to the token service hosted on a web server

9. Click **Save**.
10. Click the Hamburger menu on the left and then select **Web Voice** or **Web Video**.
11. Click **Click to Call** to initiate a Avaya WebRTC Connect Voice/Video call.

    For a Voice call, ensure that you have a microphone connected and the browser has access to the microphone. For a Video call, ensure that you have a webcam and a microphone connected and the browser has access to the webcam and the microphone.

Installing the iOS reference client

Before you begin

- Ensure that you have the free base-level registered membership of Avaya DevConnect Program. For information about Avaya DevConnect, see *Avaya DevConnect Program Guide* available on https://support.avaya.com.
- Ensure that the following certificates are installed and trusted on the iOS device:
  - A trust certificate for System Manager that manages the cluster containing Avaya Mobile Communications Snap-in.
  - A trust certificate for Avaya Aura® Device Services using the link: `https://<Avaya Aura Device Services_FQDN>/acs/resources`.
  - A trust certificate for Avaya Aura® Web Gateway using the link: `https://<Avaya Aura Web Gateway_FQDN/csa/resources/tenants/default`.

Procedure

1. Download the iOS reference client from the Avaya DevConnect portal at http://www.avaya.com/devconnect.
2. To use the iOS reference client, extract the relevant archive retrieved in the previous step on an Apple Mac and double-click on the `.xcodeproj` file.

   This opens the XCode project. The reference client can now be built from XCode and can be run on an iOS device.

Configuring the iOS reference client and making a call

Procedure

1. Open the iOS reference client for Avaya Oceana®.
2. Tap **Settings** > **OceanaReferenceClient**.
3. In the CLIENT CONFIG section, do the following:
   a. In the **AMC Cluster address** field, enter the address of the cluster containing Avaya Mobile Communications Snap-in.

b. In the **AMC Cluster Port** field, type one of the following values based on the protocol that the reference client uses when connecting to the cluster containing Avaya Mobile Communications Snap-in:

- Type `80` for HTTP.
- Type `443` for HTTPS.

c. In the **Use HTTPS** field, do one of the following based on the protocol that the reference client uses when connecting to the cluster containing Avaya Mobile Communications Snap-in:

- Move the slider to the left for HTTP.
- Move the slider to the right for HTTPS.

d. In the **AMC Url Path** field, leave the default value, `services/AvayaMobileCommunications/sessions`.

e. In the **Display Name** field, enter the customer display name to be displayed on Avaya Workspaces.

f. In the **From Address** field, enter the customer from address to be displayed on Avaya Workspaces.

The customer from address must be a numeric value. If you do not specify a from address, it is randomly assigned for each call.

g. In the **Destination Address (Optional)** field, enter the number to make direct station/agent calls.

The direct station/agent calls are the calls that are not routed through Avaya Oceana®.

Important:

This step is for debug purposes only and must be left empty.

h. In the **Context (Optional)** field, enter the customer specific information.

i. In the **Topic (Optional)** field, enter the customer specific information.

4. In the AAWG CONFIG section, do the following:

a. In the **AAWG Server Address** field, enter the FQDN of the Avaya Aura® Web Gateway server.

b. In the **AAWG Server Port** field, type one of the following values:

- Type `80` for HTTP.
- Type `443` for HTTPS.

c. In the **Use HTTPs** field, move the slider to the right.

5. In the TOKEN CONFIG section, do the following:

a. In the **Token Service Address** field, enter the FQDN of the web server that is hosting the token service.

b. In the **Token Service Port** field, enter the port number of the web server that is hosting the token service.

c. In the **Use HTTPs** field, do one of the following based on the protocol that the reference client uses when connecting to the web server that is hosting the token service:

- Move the slider to the left for HTTP.
- Move the slider to the right for HTTPS.

d. In the **Token Server Url Path** field, enter the URL path to connect to the token service hosted on a web server

6. In the SERVICE section, leave the default values in the **Priority**, **Locale**, and **Strategy** fields.
7. In the ATTRIBUTE ONE, ATTRIBUTE TWO, and ATTRIBUTE THREE sections, enter the names and values of the routing attributes to select an agent.

   You can configure maximum three attributes.
8. **(Optional)** In the RESOURCE section, do the following:

   a. In the **Source Name** field, enter the Voice provider name to which the agent is associated.

   b. In the **Resource Id** field, enter the Native Resource ID of the agent.

      To get the Voice provider name, you must log on to Avaya Control Manager and access the Providers tab on the Avaya Oceana Server Edit page.
9. Return to **Home** screen.
10. Select the speech icon and then select **Audio Call** or **Video Call** to initiate a Avaya WebRTC Connect Voice/Video call.

Installing the Android reference client

Before you begin

- Ensure that you have the free base-level registered membership of Avaya DevConnect Program. For information about Avaya DevConnect, see *Avaya DevConnect Program Guide* available on https://support.avaya.com.
- Ensure that the following certificates are installed and trusted on the iOS device:
  - A trust certificate for System Manager that manages the cluster containing Avaya Mobile Communications Snap-in.
  - A trust certificate for Avaya Aura® Device Services using the link: `https://<Avaya Aura Device Services_FQDN>/acs/resources`.
  - A trust certificate for Avaya Aura® Web Gateway using the link: `https://<Avaya Aura Web Gateway_FQDN/csa/resources/tenants/default`.

Procedure

1. Download the Android reference client from the Avaya Devconnect portal at http://www.avaya.com/devconnect.
2. To use the Android reference client, extract the relevant archive retrieved in the previous step.
3. Using Android Studio, import the project.

   The reference client can now be built from Android Studio and can be run on an Android device.

Configuring the Android reference client and making a call

Procedure

1. Open the Avaya Oceana® Reference Client.
2. Select the menu icon and then select **Settings**.
3. In the CLIENT CONFIG section, do the following:
   a. In the **AMC Cluster address** field, enter the address of the cluster containing Avaya Mobile Communications Snap-in.
   b. In the **AMC Cluster Port** field, type one of the following values based on the protocol that the reference client uses when connecting to the cluster containing Avaya Mobile Communications Snap-in:
      - Type `80` for HTTP.
      - Type `443` for HTTPS.
   c. In the **Use HTTPS** field, do one of the following based on the protocol that the reference client uses when connecting to the cluster containing Avaya Mobile Communications Snap-in:
      - Clear the check box for HTTP.
      - Select the check box for HTTPS.
   d. In the **AMC Url Path** field, leave the default value, `services/AvayaMobileCommunications/sessions`.
   e. In the **Display Name** field, enter the customer display name to be displayed on Avaya Workspaces.
   f. In the **From Address** field, enter the customer from address to be displayed on Avaya Workspaces.

      The customer from address must be a numeric value. If you do not specify a from address, it is randomly assigned for each call.
   g. In the **Destination Address (Optional)** field, enter the number to make direct station/agent calls.

      The direct station/agent calls are the calls that are not routed through Avaya Oceana®.

Important:

This step is for debug purposes only and must be left empty.

h. In the **Context (Optional)** field, enter the customer specific information.

i. In the **Topic (Optional)** field, enter the customer specific information.

4. In the AAWG CONFIG section, do the following:
   a. In the **AAWG Server Address** field, enter the FQDN of the Avaya Aura® Web Gateway server.
   b. In the **AAWG Server Port** field, type one of the following values:
      - Type `80` for HTTP.
      - Type `443` for HTTPS.
   c. In the **Use HTTPs** field, move the slider to the right.
5. In the TOKEN CONFIG section, do the following:
   a. In the **Token Service Address** field, enter the FQDN of the web server that is hosting the token service.
   b. In the **Token Service Port** field, enter the port number of the web server that is hosting the token service.
   c. In the **Use HTTPs** field, do one of the following based on the protocol that the reference client uses when connecting to the web server that is hosting the token service:
      - Move the slider to the left for HTTP.
      - Move the slider to the right for HTTPS.
   d. In the **Token Server Url Path** field, enter the URL path to connect to the token service hosted on a web server
6. In the SERVICE section, leave the default values in the **Priority**, **Locale**, and **Strategy** fields.
7. **(Optional)** In the RESOURCE section, do the following:
   a. In the **Source Name** field, enter the Voice provider name to which the agent is associated.
   b. In the **Resource Id** field, enter the Native Resource ID of the agent.

   To get the Voice provider name, you must log on to Avaya Control Manager and access the Providers tab on the Avaya Oceana Server Edit page.
8. Return to the **Home** screen.
9. Select the menu icon and then select **Attributes**.
10. In the ATTRIBUTE ONE, ATTRIBUTE TWO, and ATTRIBUTE THREE sections, enter the names and values of the routing attributes to select an agent.

    You can configure maximum three attributes.

11. Return to the **Home** screen.
12. Select the menu icon and then select **Audio** or **Video**.
13. Select **Click to Call** to initiate a Avaya WebRTC Connect Voice/Video call.

Install and configure Avaya Aura® Session Border Controller

Avaya Oceana® requires Avaya Aura® Session Border Controller to enable calls from the public internet. Therefore, you must install Avaya Aura® Session Border Controller as part of your solution. For information about how to install Avaya Aura® Session Border Controller, see *Deploying Avaya Session Border Controller on a Hardware Platform*.

For information about how to configure Avaya Aura® Session Border Controller to enable calls from the public internet, complete the tasks described in this section.

Configuring Avaya Aura® Session Border Controller networks

About this task

Use this procedure to configure Avaya Aura® Session Border Controller.

This procedure is required only for the remote worker agent configuration.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **Network Management** > **Interfaces**.
3. On the Interfaces page, enable the following interfaces:
   - A1 internal interface
   - B1 external interface
4. On the Networks tab, configure the following networks:
   - A1 internal network
   - B1 external network
5. For external web and mobile access, assign three IP addresses to each network as follows:

   Three external IP addresses:

   - One IP address for the Avaya Aura® Web Gateway reverse proxy
   - One IP address for the AvayaMobileCommunications reverse proxy
   - One IP address for the TURN relay service

Three internal IP addresses:

- One IP address for the Avaya Aura® Web Gateway reverse proxy
- One IP address for the AvayaMobileCommunications reverse proxy
- One IP address for the TURN relay service

Creating a reverse proxy policy

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Global Profiles** > **Reverse Proxy Policy**.
3. Click **Add**.
4. In the **Rule Name** field, type the name of the reverse proxy policy and click **Next**.
5. In the General area, select the **Allow Web Socket** check box.
6. Keep the default values in the other fields.
7. Click **Finish**.

Creating a reverse proxy service for Avaya Aura® Web Gateway

Before you begin

Create a reverse proxy policy through the EMS web interface, ensuring that the **Allow Web Socket** field for the reverse proxy policy is set to `Y`.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.
3. On the Reverse Proxy tab, click **Add**.
4. On the Add Reverse Proxy Profile page, do the following:
   a. In the **Service Name** field, type the reverse proxy profile name.
   b. Select the **Enabled** check box.
   c. In the **Listen IP** field, click the external IP address of Avaya SBC.
   d. In the **Listen Port** field, type the port number as 443.
   e. In the **Listen Protocol** field, click `HTTP/HTTPS`.
   f. In the **Listen TLS Profile** field, click the relevant TLS Profile.
   g. In the **Server Protocol** field, click `HTTP/HTTPS`.
   h. In the **Connect IP** field, click the internal IP address of Avaya SBC.
   i. In the **Reverse Proxy Policy Profile** field, click the reverse proxy policy that you created.

j. In the **Server Addresses** field, type *<Avaya Aura Web Gateway IP/FQDN>*:*<port number>*.

The value of *<Avaya Aura Web Gateway IP/FQDN>* must be based on the value that you used in the SAN name while creating the TLS certificate.

The value of *<port number>* must be same as the port number configured in the **Front-end port for remote access** field on the HTTP Reverse Proxy page in Avaya Aura® Web Gateway. Avaya Aura® Web Gateway uses this port to identify requests from an external or remote user.

To go to the HTTP Reverse Proxy page, you must log on to the Avaya Aura® Web Gateway administration portal and click **External Access** > **HTTP Reverse Proxy**.

k. Click **Finish**.

Deploying Identity Certificate on Avaya Aura® Session Border Controller

Creating the common client certificate

About this task

Use this procedure to create the common client certificate that you require while creating a client profile for Avaya Aura® Session Border Controller.

Procedure

1. Create an end entity by performing the following steps:
   a. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
   b. In the navigation pane, in the RA Functions section, click **Add End Entity**.
   c. In the **End Entity Profile** field, select `INBOUND_OUTBOUND_TLS`.
   d. In the **Username** field, enter a user name.

      For example, SBCINT.

   e. In the **Password (or Enrollment Code)** field, enter a password.

      Ensure that you make a note of the user name and password. The user name and password are required when creating a certificate for this server.

   f. In the **Confirm Password** field, re-enter the password.
   g. In the **CN, Common name** field, enter the FQDN of Session Border Controller.

      For example, Subject: CN=sbc1.apac.avaya.com, CN=secondary_sbc.apac.avaya.com, OU=SDP, O=AVAYA, C=US

   h. In the first **DNS Name** field, enter the domain name of the first node of the cluster.

      For example, DNS1: apac.avaya.com.

i. In the second **DNS Name** field, enter the domain name of the second node of the cluster.

   For example, DNS2: apac.avaya.com

j. In the **IP Address** field, enter the IP address of the Session Border Controller internal interface.

k. In the **Token** field, select `P12 file`.

l. Click **Add**.

2. Create a keystore by performing the following steps:

   a. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.

   b. In the navigation pane, click **Public Web**.

   c. On the EJBCA welcome page, in the navigation pane, click **Create Keystore**.

   d. On the Keystore Enrollment page, enter the user name and password that you specified while creating the end entity.

   e. Click **OK**.

   f. Select the **Key Length** as 2048 bits.

   g. Click **Enroll**.

   h. Save the certificate file.

Creating the common server certificate

About this task

Use this procedure to create the common server certificate that you require while creating a server profile for Avaya Aura® Session Border Controller.

Procedure

1. Create an end entity by performing the following steps:

   a. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.

   b. In the navigation pane, in the RA Functions section, click **Add End Entity**.

   c. In the **End Entity Profile** field, select `INBOUND_OUTBOUND_TLS`.

   d. In the **Username** field, enter a user name.

      For example, SBCEXT.

   e. In the **Password (or Enrollment Code)** field, enter a password.

      Ensure that you make a note of the user name and password. The user name and password are required when creating a certificate for this server.

   f. In the **Confirm Password** field, re-enter the password.

g. In the **CN, Common name** field, enter the FQDN of Session Border Controller.

   For example, Subject: CN=primary_sbc.apac.avaya.com, CN=secondary_sbc.apac.avaya.com, OU=SDP, O=AVAYA, C=US

h. In the first **DNS Name** field, enter the enter the FQDN for Avaya Aura® Web Gateway of the cluster.

   For example, DNS1: aawg.apac.avaya.com.

i. In the second **DNS Name** field, enter the domain name of the second node of the cluster.

   For example, DNS2: apac.avaya.com

j. In the **IP Address** field, enter the IP address of the external interface.

k. In the **Token** field, select `P12 file`.

l. Click **Add**.

2. Create a keystore by performing the following steps:

   a. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.

   b. In the navigation pane, click **Public Web**.

   c. On the EJBCA welcome page, in the navigation pane, click **Create Keystore**.

   d. On the Keystore Enrollment page, enter the user name and password that you specified while creating the end entity.

   e. Click **OK**.

   f. Select the **Key Length** as 2048 bits.

   g. Click **Enroll**.

   h. Save the certificate file.

Creating a client profile for the Avaya Aura® Web Gateway reverse proxy

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **TLS Management** > **Client Profiles**.
3. On the Client Profiles page, click **Add**.
4. In the **Profile Name** field, type the name of the profile.
5. In the **Certificate** field, select the common client certificate that you created.

   The certificate must include the internal interface IP that you need to specify in the **Connect IP** field while creating a reverse proxy service for Avaya Aura® Web Gateway.

6. In the **Peer Verification** field, click **Required**.
7. In the **Peer Certificate Authority** field, use the CA that is used to sign your certificates.

8. In the **Verification Depth** field, type `1`.
9. Keep the default values in the other fields.
10. Click **Finish**.

Creating a server profile for the Avaya Aura® Web Gateway reverse proxy

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **TLS Management** > **Server Profiles**.
3. On the Server Profiles page, click **Add**.
4. In the **Profile Name** field, type the name of the profile.
5. In the **Certificate** field, select the common server certificate that you created.

   The certificate must include:

   - The external interface IP that you need to specify in the **Listen IP** field while creating a reverse proxy service for Avaya Aura® Web Gateway
   - Avaya Aura® Web Gateway FQDN because external clients use this FQDN to access Avaya Aura® Web Gateway
6. In the **Peer Verification** field, click **None**.
7. Keep the default values in the other fields.
8. Click **Finish**.

Generating Identity Certificate from the System Manager Certificate Authority

About this task

Use this procedure generate Identity Certificate from the System Manager Certificate Authority (CA) in the P12 format.

Procedure

1. **Create an end entity**: Log on to Avaya Aura® System Manager.
2. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
3. In the navigation pane, in the RA Functions section, click **Add End Entity**.
4. In the **End Entity Profile** field, select `INBOUND_OUTBOUND_TLS`.
5. In the **Username** field, enter a user name.
6. In the **Password (or Enrollment Code)** field, enter a password.

   Ensure that you make a note of the user name and password. The user name and password are required when generating the certificate.

7. In the **Confirm Password** field, re-enter the password.
8. Complete any other fields that you want in your certificate.
9. In the **CN, Common name** field, enter the FQDN of Session Border Controller.
10. In the **IP Address** field, enter the IP address of Session Border Controller.
11. In the **Certificate Profile** field, select `ID_CLIENT_SERVER`.
12. In the **CA** field, select `tmdefaultca`.
13. In the **Token** field, select `P12 file`.
14. Click **Add**.
15. **Create a keystore**: On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
16. In the navigation pane, click **Public Web**.
17. On the EJBCA welcome page, in the navigation pane, click **Create Keystore**.
18. On the Keystore Enrollment page, enter the user name and password that you specified while creating the end entity.
19. Click **OK**.
20. Select the **Key Length** as 2048 bits.
21. Click **Enroll**.
22. Save the certificate file in the P12 format.

Extracting the certificate and private key in Session Border Controller

About this task

Use this procedure to extract the certificate and private key from the P12 file in Session Border Controller.

Procedure

1. Log in to Session Border Controller as root user by using an SSH client application, such as PuTTy.
2. Run the following command to extract the certificate from the P12 file:

   openssl pkcs12 –in <filename>.p12 -out <filename>.pem -nokeys –clcerts

3. Run the following command to extract the private key from the P12 file:

   openssl pkcs12 –in <filename>.p12 -out <filename>.key –nocerts

Installing the client and server certificates on Session Border Controller

About this task

Use this procedure to install the client and server certificates on Session Border Controller.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **TLS Management** > **Certificates**.
3. On the Certificates page, click **Install**.
4. In the **Type** field, select `Certificate`.
5. In the **Name** field, type the name of the profile.

   For example, sbc_cert.
6. In the **Certificate File** field, select the certificate that you extracted in Session Border Controller.

   For example, cert.pem.
7. In the **Key** field, select **Upload Key File**.
8. Select the private key that you extracted in Session Border Controller.
9. In the **Key Passphrase** field, enter the password that you provided during private key generation.
10. Click **Upload File**.
11. Check the certificate to verify all details that you provided when creating the p12 file.
12. Click **Install**.

Creating a client profile for the AvayaMobileCommunications reverse proxy relay

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **TLS Management** > **Client Profiles**.
3. On the Client Profiles page, click **Add**.
4. In the **Profile Name** field, type the name of the profile.
5. In the **Certificate** field, select a certificate.

   The certificate must include the internal interface IP address that acts as a **Connect IP** for the AvayaMobileCommunications Reverse Proxy Profile.
6. In the **Peer Certificate Authority** field, select the CA that is used to sign your certificates.
7. In the **Verification Depth** field, type 1.
8. Keep other fields at default values.
9. Click **Next**.
10. Click **Finish**.

Creating a server profile for the AvayaMobileCommunications reverse proxy relay

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **TLS Management** > **Server Profiles**.
3. On the Server Profiles page, click **Add**.
4. In the **Profile Name** field, type the name of the profile.
5. In the **Certificate** field, select a certificate.

   The certificate must include the external interface IP that you need to specify in the **Listen IP** field while creating a reverse proxy service for the AvayaMobileCommunications snap-in.
6. In the **Peer Verification** field, click **None**.
7. Keep the default values in the other fields.
8. Click **Finish**.

Creating a reverse proxy service for the AvayaMobileCommunications snap-in

Before you begin

Create the reverse proxy policy with the **Allow Web Socket** field set to `Y`.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.
3. On the Reverse Proxy tab, click **Add**.
4. On the Add Reverse Proxy Profile page, do the following:
   a. In the **Service Name** field, type the reverse proxy profile name.
   b. Select the **Enabled** check box.
   c. In the **Listen IP** field, click the external Avaya SBCE IP address.
   d. In the **Listen Port** field, type the port number as 443.
   e. In the **Listen Protocol** field, click HTTP/HTTPS.
   f. In the **Listen TLS Profile** field, click the relevant TLS Profile.
   g. In the **Server Protocol** field, click HTTP/HTTPS.
   h. In the **Connect IP** field, click the internal Avaya SBCE IP address.

i. In the **Reverse Proxy Policy Profile** field, click the reverse proxy policy that you have created.

j. In the **Server Addresses** field, type `<AvayaOceanaCluster2_FQDN>:443`.

Use the FQDN based on what you used in the SAN name while creating the TLS certificate.

k. Click **Finish**.

Configure the Avaya WebRTC Connect client side TURN

Avaya Oceana® supports the client side TURN for WebRTC Connect calls from the public internet.

Creating a server profile for the TLS TURN relay

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **TLS Management** > **Server Profiles**.
3. Click **Add** to add a new TLS server profile.
4. In the **Profile Name** field, enter a name for the profile.
5. In the **Certificate** field, select the appropriate certificate.

   Important:

   Ensure that the certificate associated with the profile includes the external (B1) Interface IP. The B1 IP acts as the listen IP for TLS client TURN requests. Therefore, port 443 must not be in use on the B1 IP for any other Session Border Controller function such as reverse proxy.
6. In the **Peer Verification** field, select **None**.
7. Leave all other fields to default values.
8. Click **Next**.
9. Click **Finish**.

Adding a TURN/STUN service for Avaya WebRTC Connect clients

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **DMZ Services** > **TURN/STUN Service** > **TURN/STUN Profiles**.
3. On the TURN/STUN Profiles tab, click **Add** and do the following:
   a. In the **Profile Name** field, type an appropriate name.
   b. In the **UDP Listen Port** field, type `3478`.
   c. In the **TCP/TLS Listen Port** field, type `443`.

d. In the **TLS Server Profile** field, select the profile create in Creating a server profile for the TLS TURN relay on page 434.

e. In the **Media Relay Port Range** field, type a value between 50000 to 55000.

f. In the **Authentication** field, enable the authentication.

g. In the **Client Authentication** field, enable the authentication.

h. In the **Realm** field, specify the SIP domain.

i. In the **UDP Relay** field, enable the UDP relay.

j. Click **Finish**.

4. On the TURN Relay tab, click **Add** and do the following:

a. In the **Listen IP** field, enter the external interface IP configured on Avaya Aura® Session Border Controller that external clients use.

b. In the **Media Relay IP** field, enter the internal IP configured on Avaya Aura® Session Border Controller that Avaya Aura® Web Gateway Avaya Aura® Media Server uses for media.

c. Keep the **Service FQDN** field blank.

d. In the **TURN/STUN Profile** field, select the TURN/STUN profile that you created.

e. Click **Finish**.

Enabling Avaya WebRTC Connect client-side TURN on Avaya Aura® Web Gateway

Procedure

1. In your web browser, enter the following URL to log on to the Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. Log on to Avaya Aura® Web Gateway administration portal with your administrator credentials.
3. On the Avaya Aura® Web Gateway administration portal, click **External Access** > **Session Border Controller**.
4. Select the **Enable TURN in WebRTC Client** check box.
5. Click **Save**.

Creating a server profile for the Avaya Aura® Session Border Controller signaling interface

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.

3. In the navigation pane, click **TLS Management** > **Server Profiles**.
4. On the Server Profiles page, click **Add**.
5. In the **Profile Name** field, type the name of the profile.
6. In the **Certificate** field, select a certificate.

   The certificate must include the internal interface IP that is to be used to communicate with Session Manager.
7. In the **Peer Verification** field, click **None**.
8. Keep the default values in the other fields.
9. Click **Finish**.

Creating the Avaya Aura® Session Border Controller signaling interface

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **Signaling Interface**.
3. Click **Add**.
4. In the **Name** field, enter an appropriate name for the signaling interface.
5. In the **IP Address** field, enter the internal IP address that is allocated for communication with Session Manager.
6. In the **TCP Port** field, type `5060`.
7. Keep the **UDP Port** field blank.
8. In the **TLS Port** field, type `5061`.
9. In the **TLS Profile** field, select the server profile that you created for the Avaya Aura® Session Border Controller signaling interface.
10. Keep the default values in the other fields.
11. Click **Finish**.

Configuring the Avaya Aura® Session Border Controller external media interface

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **Media Interface**.
3. Click **Add**.
4. In the **Name** field, enter an appropriate name for the media interface.

5. In the **IP Address** field, enter the external IP address that is allocated for external media.
6. Leave the **TLS Profile** field as None.
7. Keep the default values in the other fields.
8. Click **Finish**.

Configuring the Avaya Aura® Session Border Controller internal media interface

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **Media Interface**.
3. Click **Add**.
4. In the **Name** field, enter an appropriate name for the media interface.
5. In the **IP Address** field, enter the internal IP address that is allocated for internal media.
6. In the **Port** field, enter any value between 35000 to 40000.
7. Leave the **TLS Profile** field as None.
8. Keep the default values in the other fields.
9. Click **Finish**.

Creating an application rule

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Domain Policies** > **Application Rules**.
3. In the Application Rules pane, click **Add**.
4. On the Application Rule page, enter a name for the new application rule and click **Next**.
5. Select the following check boxes:
   - **In**
   - **Out**
   - **Audio**
   - **Video**
6. In the **Maximum Concurrent Sessions** field, enter the appropriate value.
7. In the **Maximum Sessions Per Endpoint** field, enter the appropriate value.
8. Keep the default values in the other fields.
9. Click **Finish**.

Creating an endpoint policy group

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Domain Policies** > **End Point Policy Group**.
3. In the Application pane, click **Add**.
4. In the **Group Name** field, type a name for the new policy group, and click **Next**.
5. Assign the newly created video-enabled application rule to the policy group.
6. Click **Finish**.

Creating a client profile for the Avaya Aura® Session Border Controller signaling interface

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **TLS Management** > **Client Profiles**.
3. On the Client Profiles page, click **Add**.
4. In the **Profile Name** field, type the name of the profile.
5. In the **Certificate** field, select a certificate.

   The certificate must include the internal interface IP that is to be used to communicate with Session Manager.
6. In the **Peer Verification** field, click **Required**.
7. In the **Peer Certificate Authority** field, use the CA that is used to sign your certificates.
8. In the **Verification Depth** field, type `1`.
9. Keep the default values in the other fields.
10. Click **Finish**.

Creating an interworking profile without remote Avaya Aura® Session Border Controller

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Global Profiles** > **Server Interworking**.
3. In the Interworking Profiles area, select **avaya-ru** and click **Clone**.

   The EMS web interface displays the Clone Profile dialog box.
4. In the **Clone Name** field, enter a name for the new profile.

For example, avaya-no-sbc.

5. Click **Finish**.
6. In the Interworking Profiles area, select the new profile.
7. Click the **Advanced** tab and click **Edit**.

   The EMS web interface displays the Editing Profile dialog box.
8. Ensure that the **Has Remote SBC** check box is cleared.
9. Click **Finish**.

Adding a server configuration for Avaya Aura® Web Gateway

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Global Profiles** > **Server Configuration**.
3. Click **Add**.
4. In the **Profile Name** field, type a name for the new server profile and click **Next**.
5. In the **Server Type** field, select `Trunk server`.
6. Leave the **SIP Domain** field blank.
7. In the **DNS Query Type** field, select `NONE/A`.
8. In the **TLS Client Profile** field, enter the client profile that you created for the Avaya Aura® Session Border Controller signaling interface.
9. In the **IP Addresses/FQDNs** field, enter the IP address of the Avaya Aura® Web Gateway server node.
10. In the **Port** field, type `5061`.
11. In the **Transport** field, select `TLS`.
12. Keep the default values in the other fields and click **Next**.
13. On the Add Server Configuration Profile - Advanced page, do the following:
    a. Select the **Enable Grooming** check box.
    b. In the **Interworking Profile** field, select the newly created interworking profile with remote SBC disabled.
    c. Keep the default values in the other fields.
    d. Click **Finish**.
14. If the Avaya Aura® Web Gateway server is part of a cluster, repeat this procedure to add a server configuration for each server node in the cluster.

    Do not add Server Configuration for the shared virtual IP.

Adding a server configuration for Session Manager

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Global Profiles** > **Server Configuration**.
3. Click **Add**.
4. In the **Profile Name** field, type a name for the new server profile and click **Next**.
5. In the **Server Type** field, select `Trunk server`.
6. Leave the **SIP Domain** field blank.
7. In the **DNS Query Type** field, select `NONE/A`.
8. In the **TLS Client Profile** field, enter the client profile that you created for the Avaya Aura® Session Border Controller signaling interface.
9. In the **IP Addresses/FQDNs** field, enter the IP address of the Session Manager server.
10. In the **Port** field, type `5061`.
11. In the **Transport** field, select `TLS`.
12. Keep the default values in the other fields and click **Next**.
13. On the Add Server Configuration Profile - Advanced page, do the following:
    a. Select the **Enable Grooming** check box.
    b. In the **Interworking Profile** field, select the newly created interworking profile with remote SBC disabled.
    c. Keep the default values in the other fields.
    d. Click **Finish**.

Adding a server flow for Avaya Aura® Web Gateway

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **End Point Flows** > **Server Flows**.
3. Click **Add**.
4. In the **Flow Name** field, type an appropriate name for the flow.
5. In the **Server Configuration** field, select the configuration for the Avaya Aura® Web Gateway server node.
6. Keep the default values for the **URI Group**, **Transport**, and **Remote Subnet** fields.
7. In the **Received Interface** field, specify the internal SIG interface.
8. In the **Signaling Interface** field, specify the internal SIG interface.

9. In the **Media Interface** field, specify the external media interface.
10. In the **End Point Policy Group** field, select the video-enabled endpoint policy group.
11. Keep the default values in the other fields.
12. Click **Finish**.
13. If the Avaya Aura® Web Gateway server is part of a cluster, repeat this procedure to add a server flow for each server node in the cluster.

Adding a server flow for Session Manager

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **End Point Flows** > **Server Flows**.
3. Click **Add**.
4. In the **Flow Name** field, type an appropriate name for the flow.
5. In the **Server Configuration** field, select the configuration for the Session Manager server.
6. Keep the default values for the **URI Group**, **Transport**, and **Remote Subnet** fields.
7. In the **Received Interface** field, specify the internal SIG interface.
8. In the **Signaling Interface** field, specify the internal SIG interface.
9. In the **Media Interface** field, specify the internal media interface.
10. In the **End Point Policy Group** field, select the video-enabled endpoint policy group.
11. Keep the default values in the other fields.
12. Click **Finish**.

Configuring Avaya Aura® Session Border Controller for load monitoring

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **Advanced Options** > **Load Monitoring**.
3. Click **Add**.
4. In the **Load Balance Type** field, select `INTERNAL`.
5. In the **Transport** field, select `TCP`.
6. In the **Listen IP** field, select an internal SIG IP that can be used.
7. In the **TLS Profile** field, select the Avaya Aura® Web Gateway server profile if TLS is used.

8. Click **Finish**.

Adding Avaya Aura® Session Border Controller as a SIP entity in System Manager

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **SIP Entities**.
2. On the SIP Entities page, click **New**.
3. In the **Name** field, enter a name for the SIP entity.
4. In the **FQDN or IP Address** field, enter the IP address of the Avaya Aura® Session Border Controller internal interface that you specified while creating the Avaya Aura® Session Border Controller signaling interface. For more information see, Creating the Avaya Aura® Session Border Controller signaling interface. on page 436
5. In the Type field, enter **SIP Trunk**.
6. Configure the appropriate **Location** and **Time Zone**.
7. Leave all other fields with default values.
8. In **Entity Links** click **Add**.
9. Modify the Entity Link name if required.
10. In the **SIP Entity 1** field, select the Session Manager entity.
11. In the **Protocol** field, select **TLS**.
12. In the **Port** field, enter **5061**.
13. In the **SIP Entity 2** field, select the Session Border Controller entity.
14. In the **Port** field, enter **5061**.
15. In the **Connection Policy** field, select **trusted**.
16. Click **Commit**.

Adding the Avaya Aura® Session Border Controller configuration to Avaya Aura® Web Gateway

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. On the Avaya Aura® Web Gateway administration portal, click **External Access** > **Session Border Controller**.
3. Click **Add**.

4. In the **SIP Address** field, type the address of the Avaya Aura® Session Border Controller internal interface that you specified while creating the Avaya Aura® Session Border Controller signaling interface.
5. In the **SIP Port** field, type `5061`.
6. In the **SIP Protocol** field, select `TLS`.
7. In the **HTTP Address** field, type the address of the Avaya Aura® Session Border Controller internal interface that you specified while configuring Avaya Aura® Session Border Controller for load monitoring.
8. In the **HTTP Port** field, type 80 if you are using HTTP protocol or 443 if you are using HTTPS protocol.
9. In the **HTTP Protocol** field, select http or https.
10. In the **Location** field, specify the location of the Avaya Aura® Session Border Controller server.
11. Click **Save**

Route web and mobile voice calls to Avaya WebRTC Connect workflows

Configuring routing to Engagement Designer

About this task

In a typical Avaya Oceana®, Avaya Oceana® Cluster 1 has three Avaya Breeze® platform nodes that host the Engagement Designer SVAR. To ensure Session Manager can route Web Voice contacts to an active Engagement Designer workflow, you first must configure an Engagement Designer load balancer, and then configure a SIP Entity and Entity Link for this load balancer.

Procedure

1. On the System Manager web console, click **Elements** > **Session Manager** > **Network Configuration** > **Local Host Name Resolution**.
2. On the Local Host Name Resolution page, click **New**.
3. On the New Local Host Name Entries page, perform the following steps:
   a. In the **Host Name (FQDN)** field, enter a valid FQDN for the Engagement Designer load balancer.

      The host name can be mapped to more than one IP addresses and each of these mappings is a separate entry.

Important:

For all Local Host Name Resolution Entries for Avaya Breeze® platform nodes, the host name must be the same.

b. In the **IP Address** field, enter the security IP address of an Avaya Breeze® platform node which is running Engagement Designer.

c. In the **Port** field, enter the port number 5090 for TCP or 5091 for TLS.

d. In the **Priority** field, enter the priority number for the Avaya Breeze® platform node.

If there are multiple IP address entries for a host, Session Manager uses the IP addresses in the order of the priority.

e. In the **Weight** field, enter the weight number for the Avaya Breeze® platform node.

If there are multiple IP address entries for a host and some entries have the same priority, Session Manager chooses a host according to the specified weights for each priority level.

f. In the **Transport** field, enter the type of transport protocol.

g. Repeat steps a to f to create Local Host Name Resolution Entries for the remaining Avaya Breeze® platform nodes that host Engagement Designer.

h. Click **Commit**.

4. On the System Manager web console, click **Elements** > **Routing**.
5. In the navigation pane, click **SIP Entities**.
6. On the SIP Entities page, click **New**.
7. On the SIP Entity Details page, perform the following steps:

a. In the **Name** field, enter a name for the Engagement Designer load balancer SIP Entity.

b. In the **FQDN or IP Address** field, enter an FQDN.

This FQDN must be the same as the FQDN that you entered while creating the Local Host Name Resolution entry for Engagement Designer load balancer.

c. In the **Type** field, select **Other**.

d. In the **SIP Timer B/F (in seconds)** field, enter the time for which Session Manager waits before receiving a response from SIP Entity.

The range is 1-32. The default value is 4 seconds.

e. Click **Commit**.

8. In the navigation pane, click **Entity Links**.
9. On the Entity Links page, click **New**.
10. On the Entity Links page, perform the following steps:

a. In the **Name** field, enter an appropriate name.

b. In the **SIP Entity 1** field, select the Session Manager entity.

c. In the **Protocol** field, select a communication protocol.

   If you select TCP, the port number changes to 5060. If you select TLS, the port number changes to 5061.

   For SIP Entity 1, set a port number other than 5060 or 5061. The port number selected must be the same port number that was used when configuring the Engagement Designer load balancer FQDN in **Session Manager** > **Network Configuration** > **Local Host Name Resolution**.

d. In the **SIP Entity 2** field, select the load balancer entity.

   For SIP Entity 2, keep the default port number.

e. Click **Commit**.

11. On the SIP Entities page, perform the following steps:
    a. Select the Session Manager SIP entity to which you created a link and click **Edit**.
    b. In the Listen Port section, click **Add**.
    c. In the **Listen Ports** field, enter a new port number such as 5090 or 5091.
    d. In the **Protocol** field, select the protocol that you used for SIP Entity 1.
    e. In the **Default Domain** field, select the root domain used for call routing.
    f. Click **Commit**.
12. In the navigation pane, click **Routing Policies**.
13. On the Routing Policies page, click **New**.
14. On the Routing Policy Details page, perform the following steps:
    a. In the **Name** field, enter a name for Routing Policy.
    b. In the SIP Entity as Destination section, click **Select**.
    c. Select the Engagement Designer load balancer SIP Entity hosting the Web Voice workflow and click **Select**.
    d. Click **Commit.**
15. In the navigation pane, click **Dial Patterns**.
16. On the Dial Patterns page, click **New**.

    System Manager displays the Dial Pattern Details page.
17. In the **Pattern** field, enter a pattern that Web Voice users dial to access Engagement Designer workflows.

Important:

At the end of this Avaya WebRTC Connect Routing pattern, you must include a wildcard x to allow multiple numbers to access Engagement Designer. For example, enter `87400x` to allow numbers 874000 to 874009 to access Engagement Designer.

18. In the **Min** field, enter the minimum number of digits to match in the Dial Pattern.
19. In the **Max** field, enter the maximum number of digits to match in the Dial Pattern.
20. In the Originating Locations and Routing Policies section, click **Add**.
21. On the Originating Location page, perform the following steps:
    a. In the Originating Location section, select the appropriate location.
    b. In the Routing Policies section, select the routing policy to route to the Engagement Designer load balancer SIP Entity hosting the Web Voice workflow.
    c. Click **Select**.
22. Click **Commit**.

Configuring Engagement Designer Event Mapper to trigger the Web Voice workflow

Procedure

1. In your web browser, enter the following URL to open Engagement Designer **Admin Console**:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

2. On the Workflows tab, verify that the OceanaWebVoiceAssistedService workflow is available in the list of deployed workflows.
3. On the Workflows tab, select the Web Voice workflow and click **Attributes**.
4. On the Workflow Attributes tab, do the following:
   a. In the **CoverageDestination** field, enter the value in the following format:

      <Number>@*<Domain.com>*

      The *<Number>* is the Coverage VDN that you created previously.

      Enter the value in this field only if you use Coverage.

   b. In the **DefaultDestination** field, enter the value in the following format:

      <Number>@*<Domain.com>*

      The *<Number>* is the Fallback VDN that you created previously. For example, 8284103@domain.com.

   c. In the **MaintenanceMode** field, replace the default value `False` with the value `True` if your site is down for maintenance.

d. In the **UseCoverage** field, enter one of the following values:
   - If you do not use Coverage, enter the value `False`.
   - If you use Coverage, enter the value `True`.

e. Click **Close**.

5. Click the **Routing** tab.
6. Click **Create**.
7. In the **Select event** field, click **CALL_INTERCEPT_TO_CALLED_PARTY**.
8. In the **Select workflows** field, click the sample Web Voice workflow.

   Note:

   Ensure that you click the workflow ending with the term `Latest`. For example, OceanaWebVoiceAssistedService:Latest.

9. In the **Enter rule name** field, type `WebVoice`.
10. Click **Add Rule**.
11. In the **Select schema attribute** field, click **CallEvent.calledParty.handle:string**.
12. In the **Select function** field, click **is equal to**.
13. In the **Enter value** field, enter the number that Web Voice calls use to trigger the Engagement Designer workflow.

    This number must be a specific number within the range defined in the Avaya WebRTC Connect Routing pattern that triggers the Web Voice workflow.

14. Click **Save**.

    The system displays the newly created rule in the list of rules.

15. Click **OK**.

Creating an Avaya Breeze® platform Implicit User Profile for the Web Voice service profile

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Implicit User Profiles**.
2. On the Implicit User Profiles page, click **New**.
3. On the Implicit User Profile Rule Editor page, perform the following steps:
   a. In the **Service Profile** field, select the Avaya WebRTC Connect service profile that you have already created.
   b. In the **Pattern** field, enter the pattern as defined when configuring the WebRTC Connect Routing pattern to Engagement Designer.

This allows multiple numbers within the defined WebRTC Connect Routing pattern range to share the same Implicit User Profile/Service Profile.

c. In the **Min** and **Max** fields, ensure that the values are auto-populated based on the pattern.

d. In the **Desc** field, enter a description for the Implicit User Profile.

e. Click **Commit**.

Configuring routing for the AvayaMobileCommunications SVAR

About this task

In a typical Avaya Oceana®, Avaya Oceana® Cluster 2 has two Avaya Breeze® platform nodes that host the AvayaMobileCommunications SVAR. For Session Manager to communicate with the AvayaMobileCommunications SVAR, you must first configure an Avaya Mobile Communications load balancer and then configure a SIP Entity and Entity Link for the load balancer.

Important:

Skip this section for an Avaya Oceana® deployment that supports up to 100 active agents.

Procedure

1. On the System Manager web console, click **Elements** > **Session Manager** > **Network Configuration** > **Local Host Name Resolution**.
2. On the Local Host Name Resolution page, click **New**.
3. On the New Local Host Name Entries page, perform the following steps:
   a. In the **Host Name (FQDN)** field, enter a valid FQDN for the Avaya Mobile Communications load balancer.

      The host name can be mapped to more than one IP addresses and each of these mappings is a separate entry.

      Important:

      For all Local Host Name Resolution Entries for Avaya Breeze® platform nodes, the host name must be the same.

   b. In the **IP Address** field, enter the security IP address of an Avaya Breeze® platform node which is running the AvayaMobileCommunications SVAR.

   c. In the **Port** field, enter the port number 5090 for TCP or 5091 for TLS.

   d. In the **Priority** field, enter the priority number for the Avaya Breeze® platform node.

      If there are multiple IP address entries for a host, Session Manager uses the IP addresses in the order of the priority.

   e. In the **Weight** field, enter the weight number for the Avaya Breeze® platform node.

      If there are multiple IP address entries for a host and some entries have the same priority, Session Manager chooses a host according to the specified weights for each priority level.

f. In the **Transport** field, enter the type of transport protocol.

g. Repeat steps a to f to create Local Host Name Resolution Entries for the other Avaya Breeze® platform node that hosts the AvayaMobileCommunications SVAR.

h. Click **Commit**.

4. On the System Manager web console, click **Elements** > **Routing**.
5. In the navigation pane, click **SIP Entities**.
6. On the SIP Entities page, click **New**.
7. On the SIP Entity Details page, perform the following steps:

   a. In the **Name** field, enter a name for the Avaya Mobile Communications load balancer SIP Entity.

   b. In the **FQDN or IP Address** field, enter an FQDN.

      This FQDN must be the same as the FQDN that you entered while creating the Local Host Name Resolution entry for the Avaya Mobile Communications load balancer.

   c. In the **Type** field, select **Other**.

   d. In the **SIP Timer B/F (in seconds)** field, enter the time for which Session Manager waits before receiving a response from SIP Entity.

      The range is 1-32. The default value is 4 seconds.

   e. Click **Commit**.

8. In the navigation pane, click **Entity Links**.
9. On the Entity Links page, click **New**.
10. On the Entity Links page, perform the following steps:

    a. In the **Name** field, enter an appropriate name.

    b. In the **SIP Entity 1** field, select the Session Manager entity.

    c. In the **Protocol** field, select a communication protocol.

       If you select TCP, the port number changes to 5060. If you select TLS, the port number changes to 5061.

       For SIP Entity 1, set a port number other than 5060 or 5061. The port number selected must be the same port number that was used when configuring the Avaya Mobile Communications load balancer FQDN in **Session Manager** > **Network Configuration** > **Local Host Name Resolution**.

    d. In the **SIP Entity 2** field, select the load balancer entity.

       For SIP Entity 2, keep the default port number.

    e. Click **Commit**.

11. On the SIP Entities page, perform the following steps:

    a. Select the Session Manager SIP entity to which you created a link and click **Edit**.

b. In the Listen Port section, click **Add**.
c. In the **Listen Ports** field, enter a new port number such as 5090 or 5091 If the port number is not already added.
d. In the **Protocol** field, select the protocol that you used for SIP Entity 1.
e. In the **Default Domain** field, select the root domain used for call routing.
f. Click **Commit**.

Creating an application and application sequence

About this task

Use this procedure to create an application and application sequence through System Manager.

Important:

Skip this procedure for an Avaya Oceana® deployment that supports up to 100 active agents.

Procedure

1. On the System Manager web console, click **Elements** > **Session Manager** > **Application Configuration** > **Applications**.
2. On the Applications page, click **New**.
3. On the Application Editor page, do the following:
   a. In the **Name** field, enter a name for the application.

      For example, `WebRTC`.

   b. In the **SIP Entity** field, select the Avaya Mobile Communications load balancer SIP Entity.
   c. Click **Commit**.
4. On the System Manager web console, click **Elements** > **Session Manager** > **Application Configuration** > **Application Sequences**.
5. On the Application Sequences page, click **New**.
6. On the Application Sequence Editor page, do the following:
   a. In the **Name** field, enter a name for the application sequence.

      For example, `WebRTCAppSeq`.

   b. In the **Available Applications** list, click the plus sign (**+**) for each Avaya Breeze® platform application that you created.
   c. Click **Commit**.

      Note:

      For information about SIP load balancing, see the SIP high availability section in *Deploying Avaya Breeze® platform*.

Administering implicit sequencing for Avaya Mobile Communications

About this task

Use this procedure to administer implicit sequencing for Avaya Mobile Communications

Important:

- Skip this section for an Avaya Oceana® deployment that supports up to 100 active agents.
- Configure implicit user number for Session Manager according to the dial pattern and ensure that it matches the same pattern as configured in the Engagement Designer workflow.

Procedure

1. On the System Manager web console, click **Elements** > **Session Manager** > **Application Configuration** > **Implicit Users**.
2. On the Implicit Users page, click **New**.
3. On the Implicit User Profile Rule Editor page, perform the following steps:
   a. In the **Pattern** field, enter the Avaya WebRTC Connect Routing pattern as defined when configuring routing to Engagement Designer.

      This allows multiple numbers within the defined WebRTC Connect Routing pattern range to share the Avaya Mobile Communications Implicit sequencing.

   b. In the **Min** and **Max** fields, ensure that the values are auto-populated based on the pattern.
   c. In the **SIP Domain** field, ensure that you do not change the default value `-ALL-`.
   d. In the **Termination Application Sequence** field, select the application sequence that you have created.

      For example, `WebRTCAppSeq`.

   e. Click **Commit**.

Configuring an Implicit User Route Point for inbound Web Voice

About this task

Use this procedure to create an Implicit User Route Point for Inbound Web Voice using Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Route Points**.

2. On the Route Points List page, click **Add**.
3. To add the Inbound Voice Implicit User, perform the following steps:
    a. In the **Type** field, select `Implicit User`.
    b. In the **Sub Type** field, select `Ingress`.
    c. In the **Name** field, enter a name for the Implicit User.
    d. In the **Address** field, enter a number based on the pattern that you specified while configuring the Avaya Breeze® platform Implicit User Profile in System Manager.

    For example, if you specified the pattern as 999x, then enter a number such as 9990, 9992, or 9999. This number must correspond with the number used to trigger the Engagement Designer Web Voice workflow.
    e. Click **Save**.

Configure the transfer to service feature for web and mobile voice calls

Configuring Communication Manager settings to transfer web and mobile voice calls

About this task

Use this procedure to configure Communication Manager settings to web and mobile voice calls.

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run the **`change uniform-dialplan <dialplan number>`** command.

3. Add the dial pattern to use as the dial pattern for implicit user:

```
change uniform-dialplan 1                                    Page   1 of   2
                        UNIFORM DIAL PLAN TABLE
                                                              Percent Full: 0

 Matching                          Insert                          Node
 Pattern            Len Del        Digits          Net Conv        Num
 56                 8   0                          aar n
 7                  4   0                          aar n
 88                 7   0                          aar n
                                                       n
                                                       n
                                                       n
                                                       n
                                                       n
                                                       n
                                                       n
                                                       n
                                                       n
                                                       n
                                                       n
                                                       n
                                                       n
                                                       n
```

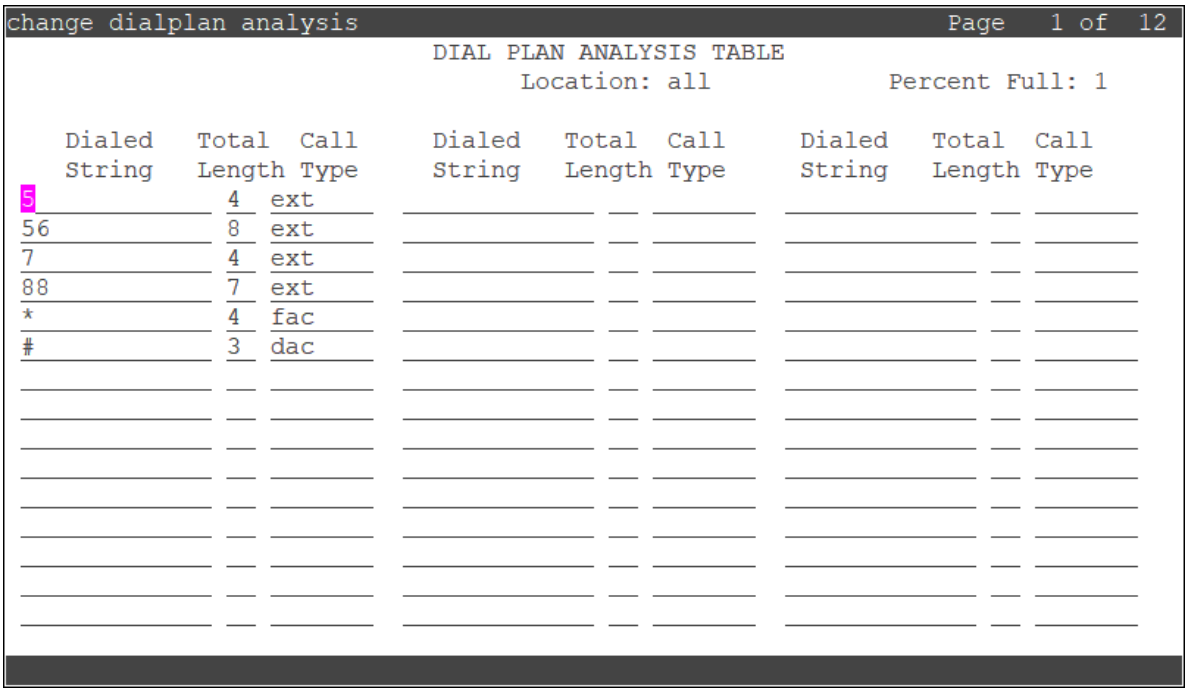
4. Run the **`change aar analysis <number>`** command.
5. Add the dialed string in the aar analysis table:

```
change aar analysis 1                                        Page   1 of   2
                        AAR DIGIT ANALYSIS TABLE
                                Location: all            Percent Full: 0

      Dialed            Total      Route     Call     Node   ANI
      String          Min  Max   Pattern   Type     Num    Reqd
 2                    7    7     4000      aar             n
 3                    7    7     4000      aar             n
 4                    7    7     4000      aar             n
 45                   8    8     1         lev0            n
 5                    7    7     4000      aar             n
 6                    7    7     4000      aar             n
 7                    4    4     1         aar             n
 88                   7    7     1         lev0            n
 9                    7    7     4000      aar             n
                                                           n
                                                           n
                                                           n
                                                           n
                                                           n
                                                           n
```

6. Run the **`change dialplan analysis`** command.

7. Add the dialed string in the dialplan analysis table:



```
change dialplan analysis                                    Page   1 of  12
                          DIAL PLAN ANALYSIS TABLE
                               Location: all            Percent Full: 1

   Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
   String   Length Type      String   Length Type      String   Length Type
5           4      ext
56          8      ext
7           4      ext
88          7      ext
*           4      fac
#           3      dac
```

Deploying the sample Transfer to Service workflow for Web Voice

About this task

Avaya provides a sample Transfer to Service workflow for the Web Voice channel. With this procedure, you can deploy the sample Transfer to Service workflow and configure the workflow attributes.

Before you begin

- Download the latest version of the sample workflow from PLDS.
- In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Designer Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. On the toolbar, click **Import Workflow from File**.
3. In the Import Workflow dialog box, click **Choose File**.
4. Browse to the folder containing the sample workflow, select the workflow, and click **Import**.
5. Click **Save Workflow**.

6. In the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaWebVoiceTransfer`.

      You can provide any name for the workflow.

   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.
8. In the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`
10. On the Workflows tab, verify that the OceanaWebVoiceTransfer workflow is available in the list of deployed workflows.
11. On the Workflows tab, select the OceanaWebVoiceTransfer workflow and click **Attributes**.
12. In the Workflow Attributes dialog box, do the following:
    a. In the **DefaultDestination** field, enter the value in the following format:

       <Number>@<Domain.com>

       The *<Number>* is the Fallback VDN that you created previously. For example, 8284103@domain.com.

    b. Click **Close**.

Configuring Engagement Designer Event Mapper to trigger the Web Voice Transfer to Service workflow

Procedure

1. In your web browser, enter the following URL to open Engagement Designer **Admin Console**:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`
2. On the Workflows tab, verify that the OceanaWebVoiceTransfer workflow is available in the list of deployed workflows.
3. Click the **Routing** tab.
4. Click **Create**.
5. In the **Select event** field, click **CALL_INTERCEPT_TO_CALLED_PARTY**.
6. In the **Select workflows** field, select the OceanaWebVoiceTransfer workflow.

Note:

Ensure that you click the workflow ending with the term `Latest`. For example, OceanaWebVoiceTransfer:Latest.

7. In the **Enter rule name** field, type `WebVoiceTransfer`.
8. Click **Add Rule**.
9. In the **Select schema attribute** field, click **CallEvent.calledParty.handle:string**.
10. In the **Select function** field, click **is equal to**.
11. In the **Enter value** field, enter the number that Web Voice calls use to trigger the Engagement Designer Transfer to Service workflow.

    This number must be a specific number within the range defined in the Avaya WebRTC Connect Routing pattern that triggers the Web Voice Transfer to Service workflow.
12. Click **Save**.

    The system displays the newly created rule in the list of rules.

Configuring the first Transfer to Service Implicit User for Web Voice

About this task

Use this procedure to create a new Transfer to Service Implicit User for Web Voice through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Route Points**.
2. On the Route Points List page, click **Add**.
3. To add the Transfer to Service Implicit User, perform the following steps:
   a. In the **Type** field, select `Implicit User`.
   b. In the **Sub Type** field, select `Transfer`.
   c. In the **Name** field, enter a name for the Implicit User.
   d. In the **Address** field, enter a number based on the pattern that you specified while configuring the Avaya Breeze® platform Implicit User Profile in System Manager.

      For example, if you specified the pattern as 999x, then enter a number such as 9990, 9992, or 9999.
   e. Click **Save**.

Creating a Vector Directory Number for Web Voice Transfer

About this task

Use this procedure to create a Vector Directory Number (VDN) for Web Voice Transfer.

Procedure

1. Run **`add vdn next`** or **`add vdn n`**.

   n is the extension that you want to use for the VDN.

2. On page 1 of the VECTOR DIRECTORY NUMBER screen, perform the following steps:
   a. In the **Name** field, enter the name of the VDN.
   b. In the **Destination** field, set the destination to a vector number which is not in use.
   c. In the **1st Skill*** field, enter the Hunt Group that you created as the default Work Assignment Hunt Group.
3. Save the settings.

Configuring a vector for the Web Voice Transfer VDN

About this task

Use this procedure to configure a vector for the Web Voice Transfer VDN.

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Web Voice Transfer VDN.

3. On page 1 of the CALL VECTOR screen, perform the following steps:
   a. In the **Name** field, enter the name of the vector as `WebVoiceXfer`.

      This standard name makes maintenance and troubleshooting easier.

b. Enter the details required from line 01 to line 02 as shown in the following screen:

```
change vector 6                                              Page   1 of   6


    Number: 6                Name: WebVoiceXfer
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    1   secs hearing ringback
02 route-to     number  xxxx             with cov n if unconditionally   EDIT
03 _____________
04 _____________
05 _____________
06 _____________
07 _____________
08 _____________
09 _____________
10 _____________
11 _____________
12 _____________
```

Important:

The number *xxxx* in the **`route-to`** command must be the same number that you configured while configuring the Transfer to Service Implicit User in System Manager and Avaya Control Manager.

4. Save the settings.

Configuring the second Transfer to Service Implicit User for Web Voice

About this task

Use this procedure to create another Transfer to Service Implicit User for Web Voice through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Route Points**.
2. On the Route Points List page, click **Add**.

3. To add the Transfer to Service Implicit User, perform the following steps:
    a. In the **Type** field, select `Implicit User`.
    b. In the **Sub Type** field, select `Transfer`.
    c. In the **Name** field, enter a name for the Implicit User.
    d. In the **Address** field, enter the VDN that you created for Web Voice Transfer.
    e. Click **Save**.

Creating a Transfer Target service for Web Voice

About this task

Use this procedure to create a Transfer Target service for Web Voice through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™** > **Work Assignment**.
2. Select the **Services** tab.
3. On the Services tab, click **Add**.
4. To add a Transfer Target service, perform the following steps:
    a. In the **Service Name** field, enter the name of the service.
    b. Select the **Available for Transfer** check box.

        The system automatically selects the **Agent Display** check box.
    c. Move the required attributes from the **Available Attributes** list to the **Included Attributes** list.
    d. In the Transfer Routepoints section, in the **Web Voice** field, select the second Implicit User that you created for Web Voice Transfer.
    e. Click **Save**.

Chapter 26: Configure Avaya Oceana® with web and mobile voice calls and Avaya WebRTC Connect agents

Checklist for configuring Avaya Oceana® with web and mobile voice calls and Avaya WebRTC Connect agents

Use the following checklist to configure Avaya Oceana® with web and mobile voice calls and WebRTC Connect agents so that WebRTC Connect and phone-enabled agents can answer PSTN, web, and mobile voice calls.:

No.	Task	Description	✔
1	Install and configure Avaya Aura® Web Gateway, Avaya Aura® Media Server, and Avaya Aura® Device Services.	See the following: • Avaya Aura Web Gateway deployment and configuration on page 400. • Avaya Aura Media Server deployment on page 386. • Avaya Aura Device Services deployment on page 380.	
2	Configure authorization on Avaya Aura® Web Gateway.	See Avaya Aura Web Gateway authorization on page 407.	
3	Create WebRTC Connect agents that can use media in browsers.	See Creating a user in Avaya Control Manager on page 413.	

Table continues…

No.	Task	Description	✔
4	Configure the voice media path.	See the following: • Configuring codecs in Avaya Aura Web Gateway on page 407. • Prioritizing codecs in Avaya Aura Media Server on page 408. • Prioritizing codecs in Communication Manager on page 408.	
5	Install and configure web and mobile applications to make anonymous calls to Avaya Aura® Web Gateway.	See Install and configure web and mobile applications on page 417.	
6	Install and configure Avaya Aura® Session Border Controller to enable calls from the public internet.	See Install and configure Avaya Aura Session Border Controller on page 425.	
7	Configure Avaya Breeze® platform so that voice calls can be anchored on Avaya Breeze® platform with wait treatment.	See Install and configure Avaya Aura Media Server for Avaya Breeze platform on page 386.	
8	Route web and mobile voice calls to WebRTC Connect Engagement Designer workflows sequencing the AvayaMobileCommunications service.	See Route web and mobile voice calls to Avaya WebRTC Connect workflows on page 443.	
9	Configure the transfer to service feature for web and mobile voice calls.	See Configure the transfer to service feature for web and mobile voice calls on page 452.	

Chapter 27: Configure Avaya Oceana® with web and mobile video calls and Avaya WebRTC Connect agents

Checklist for configuring Avaya Oceana® with web and mobile video calls and Avaya WebRTC Connect agents

Use the following checklist to configure Avaya Oceana® with web and mobile video calls and WebRTC Connect agents so that WebRTC Connect agents can answer web and mobile video calls:

No.	Task	Description	✔
1	Install and configure Avaya Aura® Web Gateway, Avaya Aura® Media Server, and Avaya Aura® Device Services.	See the following: • Avaya Aura Web Gateway deployment and configuration on page 400. • Avaya Aura Media Server deployment on page 386. • Avaya Aura Device Services deployment on page 380.	
2	Configure authorization on Avaya Aura® Web Gateway.	See Avaya Aura Web Gateway authorization on page 407.	
3	Create WebRTC Connect agents that can use media in browsers.	See Creating a user in Avaya Control Manager on page 413.	

Table continues…

No.	Task	Description	✔
4	Configure the voice media path.	See the following: • Configuring codecs in Avaya Aura Web Gateway on page 407. • Prioritizing codecs in Avaya Aura Media Server on page 408. • Prioritizing codecs in Communication Manager on page 408.	
5	Install and configure web and mobile applications to make anonymous calls to Avaya Aura® Web Gateway.	See Install and configure web and mobile applications on page 417.	
6	Install and configure Avaya Aura® Session Border Controller to enable calls from the public internet.	See Install and configure Avaya Aura Session Border Controller on page 425.	
7	Configure Avaya Breeze® platform so that voice calls can be anchored on Avaya Breeze® platform with wait treatment.	See Install and configure Avaya Aura Media Server for Avaya Breeze platform on page 386.	
8	Route web and mobile voice calls to WebRTC Connect Engagement Designer workflows sequencing the AvayaMobileCommunications service.	See Route web and mobile voice calls to Avaya WebRTC Connect workflows on page 443.	
9	Configure the transfer to service feature for web and mobile voice calls.	See Configure the transfer to service feature for web and mobile voice calls on page 452.	
10	Configure Avaya Breeze® platform so that video calls can be anchored on Avaya Breeze® platform with voice wait treatment.	See Deploying the sample Web Video workflow on page 464.	
11	Route web and mobile video calls to WebRTC Connect Engagement Designer workflows sequencing the AvayaMobileCommunications service.	See Route web and mobile video calls to Avaya WebRTC Connect workflows on page 465.	
12	Create WebRTC Connect video agents.	See Create Avaya WebRTC Connect video agents on page 467.	

Table continues…

No.	Task	Description	✔
13	Configure the video media path.	See Configure the video media path on page 469.	
14	Configure the transfer to service feature for web and mobile video calls.	See Configure the transfer to service feature for web and mobile video calls on page 471.	

Deploying the sample Web Video workflow

About this task

Avaya provides a sample workflow for the Web Video channel. With this procedure, you can deploy the sample Web Video workflow and configure the workflow attributes.

Before you begin

- Download the latest version of the sample workflow from PLDS.
- In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Designer Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. In the Import Workflow dialog box, click **Choose File**.
4. Browse to the folder containing the sample workflow, select the workflow, and click **Import**.
5. Click **Save Workflow**.
6. In the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaVideoAssistedService`.

      You can provide any name for the workflow.

   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.
8. In the Deployment Details dialog box, click **OK**.

Important:

Ensure that you do not add unique information in the first five seconds of the initial announcement.

A setup time associated with the STUN (Session Traversal Utilities for NAT) server specifies that the client cannot hear the first five seconds of the initial announcement. However, in the first five seconds of the initial announcement, you can add ring back or play music.

9. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

10. On the Workflows tab, verify that the OceanaVideoAssistedService workflow is available in the list of deployed workflows.
11. On the Workflows tab, select the OceanaVideoAssistedService workflow and click **Attributes**.
12. On the Workflow Attributes tab, do the following:
    a. In the **MaintenanceMode** field, replace the default value `False` with the value `True` if your site is down for maintenance.
    b. In the **DefaultDestination** field, enter the value in the following format:

       <Number>@<Domain.com>

       The *<Number>* is the Default Destination number to which the calls must be transferred if a problem occurs in the workflow.
    c. Click **Close**.

Route web and mobile video calls to Avaya WebRTC Connect workflows

Configuring Engagement Designer Event Mapper to trigger the Web Video workflow

Procedure

1. In your web browser, enter the following URL to open Engagement Designer **Admin Console**:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

2. On the Workflows tab, verify that the OceanaVideoAssistedService workflow is available in the list of deployed workflows.
3. Click the **Routing** tab.
4. Click **Create**.
5. In the **Select event** field, click **CALL_INTERCEPT_TO_CALLED_PARTY**.
6. In the **Select workflows** field, click the sample Web Video workflow.

   Note:

   Ensure that you click the workflow ending with the term `Latest`. For example, OceanaVideoAssistedService:Latest.
7. In the **Enter rule name** field, type `WebVideo`.
8. Click **Add Rule**.
9. In the **Select schema attribute** field, click **CallEvent.calledParty.handle:string**.
10. In the **Select function** field, click **is equal to**.
11. In the **Enter value** field, enter the number that Web Video calls use to trigger the Engagement Designer workflow.

    This number must be a specific number within the range defined in the Avaya WebRTC Connect Routing pattern that triggers the Web Video workflow.
12. Click **Save**.

    The system displays the newly created rule in the list of rules.
13. Click **OK**.

Configuring an Implicit User Route Point for inbound Web Video

About this task

Use this procedure to create an Implicit User Route Point for Inbound Web Video using Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Route Points**.
2. On the Route Points List page, click **Add**.
3. To add the Inbound Video Implicit User, perform the following steps:
   a. In the **Type** field, select `Implicit User`.
   b. In the **Sub Type** field, select `Ingress`.

c. In the **Name** field, enter a name for the Implicit User.

d. In the **Address** field, enter a number based on the pattern that you specified while configuring the Avaya Breeze® platform Implicit User Profile in System Manager.

For example, if you specified the pattern as 999x, then enter a number such as 9990, 9992, or 9999. This number must correspond with the number used to trigger the Engagement Designer Web Video workflow.

e. Click **Save**.

Create Avaya WebRTC Connect video agents

For Web Video, you must install Avaya Aura® Communication Manager 7.1.2 or later version.

Configuring customer options

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run the **`change system-parameters customer-options`** command.
3. On page 5, verify that the **Multimedia IP SIP Trunking** field is set to `y`.
4. Save the settings.

Configuring the signaling group for Web Video

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change signaling-group n`**.

   n is the number of the signaling group that you need to configure.
3. On the SIGNALING GROUP screen, perform the following steps:
   a. In the **IP Video** field, type `yes`.
   b. In the **Priority Video** field, type `yes`.
   c. In the **Initial IP-IP Direct Media** field, type `yes`.
4. Save the settings.

Enabling Video on a Communication Manager SIP station

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change station n`**.

   n is the number of the SIP for which you want to enable Video.
3. On page 1, perform the following steps:
   a. In the **IP Softphone** field, type `Y`.
   b. In the **IP Video Softphone** field, type `Y`.
4. On page 2, perform the following steps:
   a. In the **H.320 Conversion** field, type `n`.
   b. In the **Direct IP-IP Audio Connections** field, type `Y`.
5. Save the settings.

Enable Video for Avaya Oceana® SIP agents

In Avaya Oceana®, agents handle Video contacts using a Video enabled SIP station. Therefore, you must first configure SIP agents for Avaya Oceana® and then enable Video for those SIP agents.

Configuring a provider to support Video

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Server Details**.
2. On the Avaya Oceana Server List page, double-click the UCAServer server.
3. Select the **Providers** tab.
4. Select the check box for the Voice provider (Type:CM) and click **Edit**.
5. Select the **Video Enabled** check box.
6. Click **Save**.

Enabling Video for an Avaya Oceana® agent

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.
3. Select the check box for the user for which you want to enable Video, and click **Edit User**.
4. Scroll to the right and select the **Avaya Oceana** tab.
5. Clear the **Voice** check box.
6. Select the **Video** check box.
7. Click **Save**.
8. Click **OK** when the system displays a message to indicate that the attribute is set successfully.

Configure the video media path

Configuring media servers for Web Video

About this task

Use this procedure to configure media servers for Web Video.

Note:

Perform this procedure for all Avaya Breeze® platform and Avaya Aura® Web Gateway media servers.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager.

   `https://<AMS_EM_FQDN>:8443/emlogin/`

2. Click **System Configuration** > **Server Profile** > **General Settings**.
3. Select the **Video Media Processor** check box and click **Save**.

Configuring an IP codec set for Video

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change ip-codec-set`**.
3. On page 2, perform the following steps:
   a. In the **Allow Direct-IP Multimedia** field, type `yes`.

b. In the **Maximum Call Rate for Direct-IP Multimedia** field, type `768 kbps`.

c. In the **Maximum Call Rate for Priority Direct-IP Multimedia** field, type `768 kbps`.

4. Save the settings.

Configuring codecs in Avaya Aura® Web Gateway

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. On the Avaya Aura® Web Gateway administration portal, click **Advanced** > **Media Settings** > **Audio**.
3. Click **Custom SIP Audio Coded Preference**.
4. From the **SIP Audio Codecs** list, remove all codecs except your preferred G711 codec, such as G711A or G711MU.
5. From the **WebRTC Audio Codecs** list, remove all codecs except your preferred G711 codec, such as G711A or G711MU.
6. Click **Save**.
7. On the Avaya Aura® Web Gateway administration portal, click **Advanced** > **Media Settings** > **Video**.
8. From the **SIP Video Codecs** list, remove all codecs except the H264 codec.
9. From the **WebRTC Audio Codecs** list, remove all codecs except the H264 codec.
10. Set the **Call Maximum Video Bandwidth** field to `768` kbps.
11. Click **Save**.

Prioritizing codecs in Avaya Aura® Media Server

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server Gateway_FQDN>:8443/emlogin`

2. On the Avaya Aura® Media Server Element Manager interface, click **System Configuration** > **Media Processing** > **Audio Codecs**.
3. Use the **Up** button to move your preferred G711 codec to the top of the **Enabled** list.
4. Click **Save**.

Prioritizing codecs in Communication Manager

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Identify the Far-end Network Region assigned to the signaling group intended to process calls from Avaya Aura® Web Gateway.
3. Identify the ip-codec-set associated with the Far-end Network Region that you identify.
4. Run the **`change ip-codec-set <codec set number used by the SIP signaling group>`** command.
5. On page 1, in the **Audio Codec** area, verify that your preferred G711 codec (G.711A or G.711MU) is at number on the list.
6. **(Optional)** If the signaling group intended to process calls from or to Avaya Breeze® platform is different, repeat Step 1 to Step 5 for that signaling group.

Configure the transfer to service feature for web and mobile video calls

Configuring Communication Manager settings to transfer web and mobile video calls

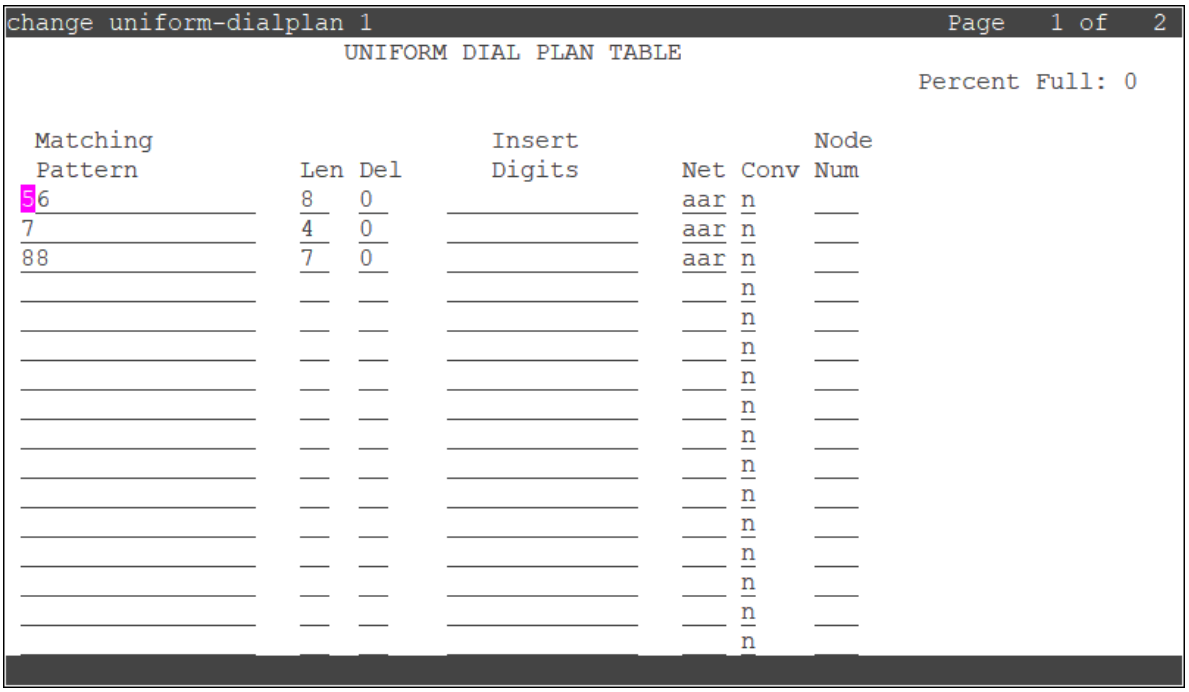
About this task

Use this procedure to configure Communication Manager settings to web and mobile video calls.

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run the **`change uniform-dialplan <dialplan number>`** command.

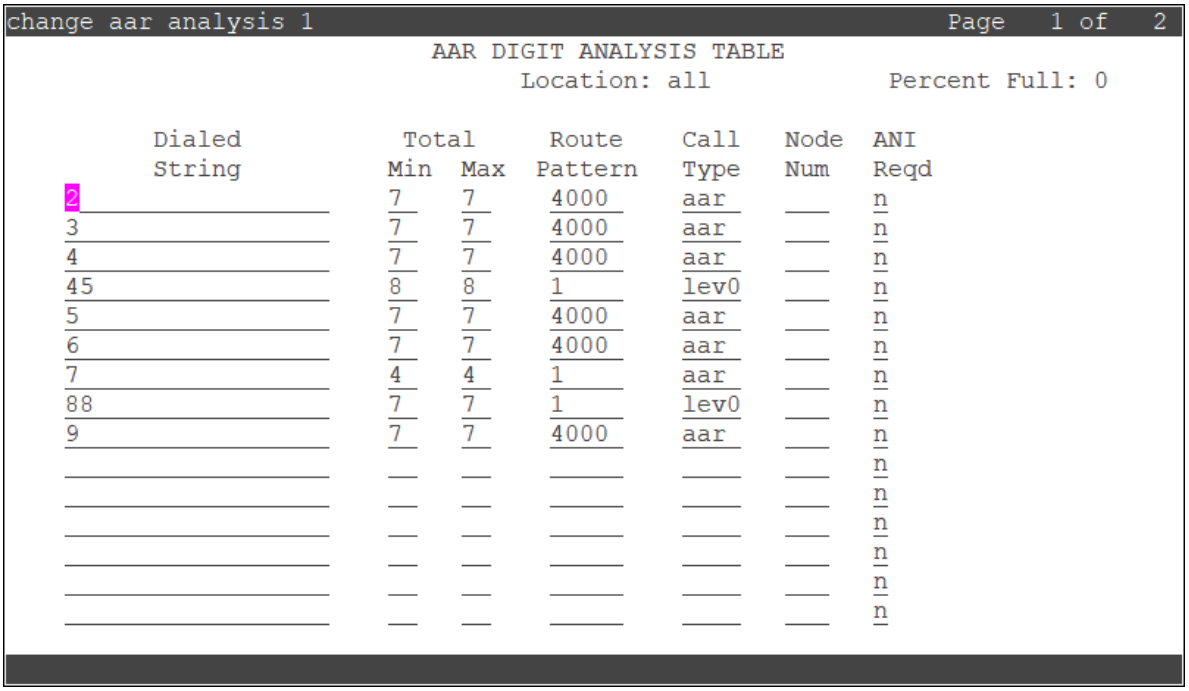
3. Add the dial pattern to use as the dial pattern for implicit user:



```
change uniform-dialplan 1                                    Page   1 of   2
                        UNIFORM DIAL PLAN TABLE
                                                          Percent Full: 0

 Matching                          Insert                        Node
 Pattern            Len Del        Digits          Net Conv      Num
56                  8   0                          aar  n
7                   4   0                          aar  n
88                  7   0                          aar  n
                                                        n
                                                        n
                                                        n
                                                        n
                                                        n
                                                        n
                                                        n
                                                        n
                                                        n
                                                        n
                                                        n
                                                        n
                                                        n
                                                        n
```

4. Run the **`change aar analysis <number>`** command.
5. Add the dialed string in the aar analysis table:

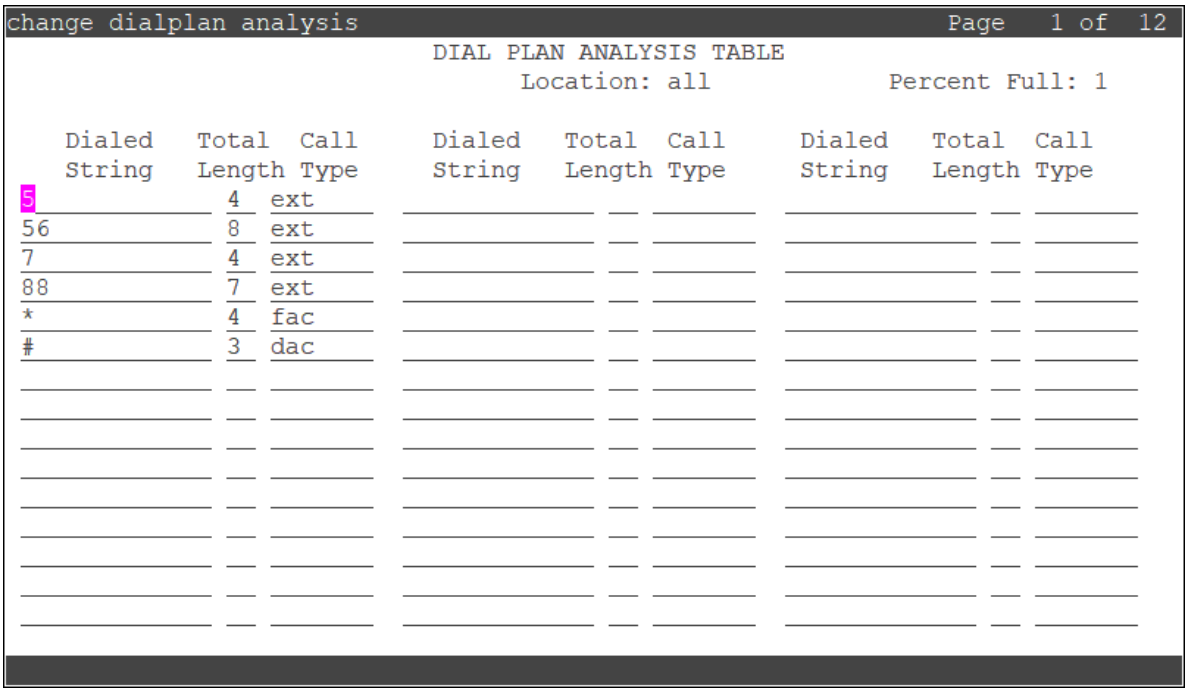


```
change aar analysis 1                                        Page   1 of   2
                        AAR DIGIT ANALYSIS TABLE
                                Location: all            Percent Full: 0

      Dialed            Total     Route    Call    Node   ANI
      String            Min  Max  Pattern  Type    Num    Reqd
2                       7    7    4000     aar            n
3                       7    7    4000     aar            n
4                       7    7    4000     aar            n
45                      8    8    1        lev0           n
5                       7    7    4000     aar            n
6                       7    7    4000     aar            n
7                       4    4    1        aar            n
88                      7    7    1        lev0           n
9                       7    7    4000     aar            n
                                                           n
                                                           n
                                                           n
                                                           n
                                                           n
                                                           n
```

6. Run the **`change dialplan analysis`** command.

7. Add the dialed string in the dialplan analysis table:



```
change dialplan analysis                                    Page   1 of  12
                          DIAL PLAN ANALYSIS TABLE
                               Location: all            Percent Full: 1

   Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
   String   Length Type      String   Length Type      String   Length Type
5           4      ext
56          8      ext
7           4      ext
88          7      ext
*           4      fac
#           3      dac
```

Deploying the sample Transfer to Service workflow for Web Video

About this task

Avaya provides a sample Transfer to Service workflow for the Web Video channel. With this procedure, you can deploy the sample Transfer to Service workflow and configure the workflow attributes.

Before you begin

- Download the latest version of the sample workflow from PLDS.
- In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Designer Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. In the Import Workflow dialog box, click **Choose File**.
4. Browse to the folder containing the sample workflow, select the workflow, and click **Import**.
5. Click **Save Workflow**.

6. In the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaVideoTransfer`.

      You can provide any name for the workflow.

   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.
8. In the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`
10. On the Workflows tab, verify that the OceanaVideoTransfer workflow is available in the list of deployed workflows.
11. On the Workflows tab, select the OceanaVideoTransfer workflow and click **Attributes**.
12. On the Workflow Attributes tab, do the following:
    a. In the **DefaultDestination** field, enter the value in the following format:

       <Number>@<Domain.com>

       The *<Number>* is the Default Destination number to which the calls must be transferred if a problem occurs in the workflow.

    b. Click **Close**.

Configuring Engagement Designer Event Mapper to trigger the Web Video Transfer to Service workflow

Procedure

1. In your web browser, enter the following URL to open Engagement Designer **Admin Console**:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`
2. On the Workflows tab, verify that the OceanaVideoTransfer workflow is available in the list of deployed workflows.
3. Click the **Routing** tab.
4. Click **Create**.
5. In the **Select event** field, click **CALL_INTERCEPT_TO_CALLED_PARTY**.
6. In the **Select workflows** field, select the OceanaVideoTransfer workflow.

Note:

Ensure that you click the workflow ending with the term `Latest`. For example, OceanaVideoTransfer:Latest.

7. In the **Enter rule name** field, type `WebVideoTransfer`.
8. Click **Add Rule**.
9. In the **Select schema attribute** field, click **CallEvent.calledParty.handle:string**.
10. In the **Select function** field, click **is equal to**.
11. In the **Enter value** field, enter the number that Web Video calls use to trigger the Engagement Designer Transfer to Service workflow.

    This number must be a specific number within the range defined in the Avaya WebRTC Connect Routing pattern that triggers the Web Video Transfer to Service workflow.
12. Click **Save**.

    The system displays the newly created rule in the list of rules.

Configuring the first Transfer to Service Implicit User for Web Video

About this task

Use this procedure to create a new Transfer to Service Implicit User for Web Video through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Route Points**.
2. On the Route Points List page, click **Add**.
3. To add the Transfer to Service Implicit User, perform the following steps:
   a. In the **Type** field, select `Implicit User`.
   b. In the **Sub Type** field, select `Transfer`.
   c. In the **Name** field, enter a name for the Implicit User.
   d. In the **Address** field, enter the number that you configured in Engagement Designer Event Mapper to trigger the Web Video Transfer to Service workflow.
   e. Click **Save**.

Creating a Vector Directory Number for Web Video Transfer

About this task

Use this procedure to create a Vector Directory Number (VDN) for Web Video Transfer.

Procedure

1. Run **`add vdn next`** or **`add vdn n`**.

   n is the extension that you want to use for the VDN.
2. On page 1 of the VECTOR DIRECTORY NUMBER screen, perform the following steps:
   a. In the **Name** field, enter the name of the VDN.
   b. In the **Destination** field, set the destination to a vector number which is not in use.
   c. In the **1st Skill*** field, enter the Hunt Group that you created as the default Work Assignment Hunt Group.
3. Save the settings.

Configuring a vector for the Web Video Transfer VDN

About this task

Use this procedure to configure a vector for the Web Video Transfer VDN.

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change vector n`**.

   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Web Video Transfer VDN.
3. On page 1 of the CALL VECTOR screen, perform the following steps:
   a. In the **Name** field, enter the name of the vector as `WebVideoXfer`.

      This standard name makes maintenance and troubleshooting easier.

b. Enter the details required from line 01 to line 02 as shown in the following screen:

```
change vector 6                                              Page   1 of   6


    Number: 6                Name: WebVideoXfer
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    1   secs hearing ringback
02 route-to     number  xxxx             with cov n if unconditionally   EDIT
03 _____________
04 _____________
05 _____________
06 _____________
07 _____________
08 _____________
09 _____________
10 _____________
11 _____________
12 _____________
```

Important:

The number *xxxx* in the **`route-to`** command must be the same number that you configured while configuring the Transfer to Service Implicit User in System Manager and Avaya Control Manager.

4. Save the settings.

Configuring the second Transfer to Service Implicit User for Web Video

About this task

Use this procedure to create another Transfer to Service Implicit User for Web Video through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Route Points**.
2. On the Route Points List page, click **Add**.

3. To add the Transfer to Service Implicit User, perform the following steps:
    a. In the **Type** field, select `Implicit User`.
    b. In the **Sub Type** field, select `Transfer`.
    c. In the **Name** field, enter a name for the Implicit User.
    d. In the **Address** field, enter the VDN that you created for Web Video Transfer.
    e. Click **Save**.

Creating a Transfer Target service for Web Video

About this task

Use this procedure to create a Transfer Target service for Web Video through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™** > **Work Assignment**.
2. Select the **Services** tab.
3. On the Services tab, click **Add**.
4. To add a Transfer Target service, perform the following steps:
    a. In the **Service Name** field, enter the name of the service.
    b. Select the **Available for Transfer** check box.

        The system automatically selects the **Agent Display** check box.
    c. Move the required attributes from the **Available Attributes** list to the **Included Attributes** list.
    d. In the Transfer Routepoints section, in the **Video** field, select the second Implicit User that you created for Web Video Transfer.
    e. Click **Save**.

Chapter 28: Remote worker solution

Remote worker solution overview

Avaya Oceana® supports the remote worker functionality for Web Voice, Web Video, and Multimedia channels. With this functionality, remote agents and supervisors who are located outside the contact center infrastructure can access Avaya Oceana® and Avaya Analytics™ applications and perform their tasks.

A remote worker can be an agent or a supervisor with reporting and agent capabilities. Avaya Analytics™ is required to support all reporting capabilities such as supervisors and reporting-only administrators.

You must deploy Avaya Oceana® and Avaya Analytics™ applications with the standard Avaya Aura® applications for Web Voice and Web Video with Avaya Aura® Session Border Controller. With this type of deployment, remote workers with Internet can access full remote worker capabilities from any location outside the contact center infrastructure.

To use the remote worker functionality, you must:

- Deploy Avaya Oceana® 3.8 and Avaya Analytics™ 4.1 or later
- Deploy and enable Web Voice and Web Video capabilities for all on-premise and remote workers
- Deploy the following applications for Web Voice and Web Video:
  - Avaya Aura® Web Gateway
  - Avaya Aura® Media Server
  - Avaya Aura® Device Services
  - Avaya Aura® Session Border Controller
- Deploy a combination of on-premise workers inside the firewall/Avaya Aura® Session Border Controller and remote workers outside the firewall/Avaya Aura® Session Border Controller
- Deploy and enable Multimedia channels for remote workers

Remote workers capabilities

The capabilities of remote workers are similar to standard on-premise workers.

Avaya Oceana® and Avaya Analytics™ remote workers can perform the following operations:

- Remote Web Voice workers can receive incoming PSTN Voice calls using media in their Avaya Oceana®-supported browsers and process them through Avaya Workspaces.

It implies that the remote workers can initiate outgoing voice contacts to reachable destinations through Avaya Workspaces.

- Remote Web Video workers can receive incoming Web Video calls using media in their Avaya Oceana®-supported browsers and process them through Avaya Workspaces.

  It implies that the remote workers can initiate outgoing video contacts to reachable destinations through Avaya Workspaces.

- Remote Multimedia workers can receive and respond to customer Email, Chat, SMS, Social Media, Generic, and Messaging contacts.

Avaya Oceana® and Avaya Analytics™ remote workers can have the following roles:

Role	Description
Supervisor Agent	Can access all supported supervisor functions of Avaya Oceana® and Avaya Analytics™.
Agent	Can access all supported agent functions of Avaya Oceana® and Avaya Analytics™.
Supervisor Reporting	Can access all supported reporting-only user functions of Avaya Oceana® and Avaya Analytics™.
Administrator	Can access all access to all Avaya Workspaces administration functions, such as adding or changing the widget layouts.
Remote Worker Agent	Can access all supported agent functions of Avaya Oceana® for voice and video calls.

Remote workers limitations

Regardless of the type and roles, remote workers:

- Cannot use Avaya telephony devices at their remote location to handle voice contacts from PSTN customers.

  Remote workers only use their browsers to handle all voice contacts.

- Cannot use the following capabilities for Web Voice:
  - Transfer to User
  - Single Step Transfer
  - Consult Transfer to Service
  - DTMF

    DTMF is supported on the customer side. Customers can send DTMF with limitations.
  - Auto Answer
  - SAML authentication
- Cannot use the following capabilities for Web Video:
  - Consult Transfer

- Consult Conference
- Consult Transfer to Service

• Cannot use the following capabilities of the Supervisor role:

- Observe and barge-in on agent chats
- Team viewer
- Team broadcast messages

Remote worker solution architecture

The following diagram depicts the high-level architecture of the remote worker solution with Avaya WebRTC Connect capabilities:

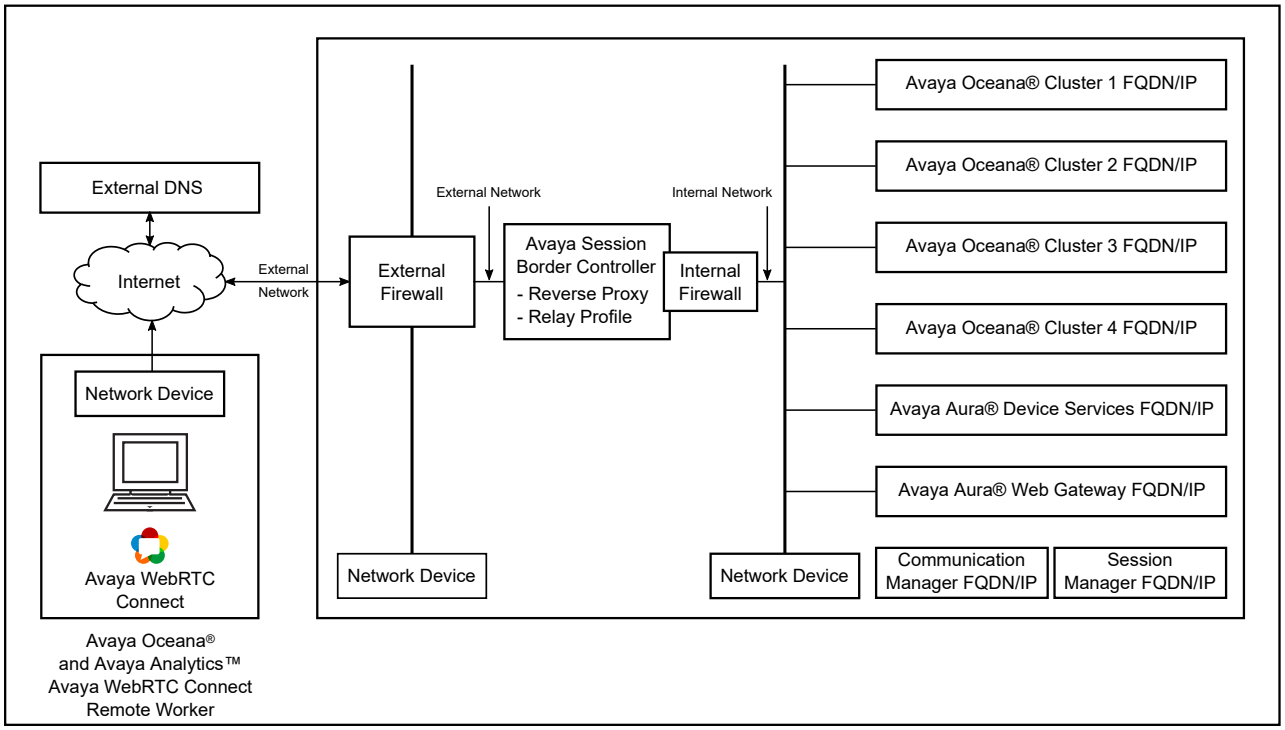


Figure 4: Remote Avaya WebRTC Connect Worker Solution

The following diagram depicts the high-level architecture of the remote worker solution with Multimedia capabilities:

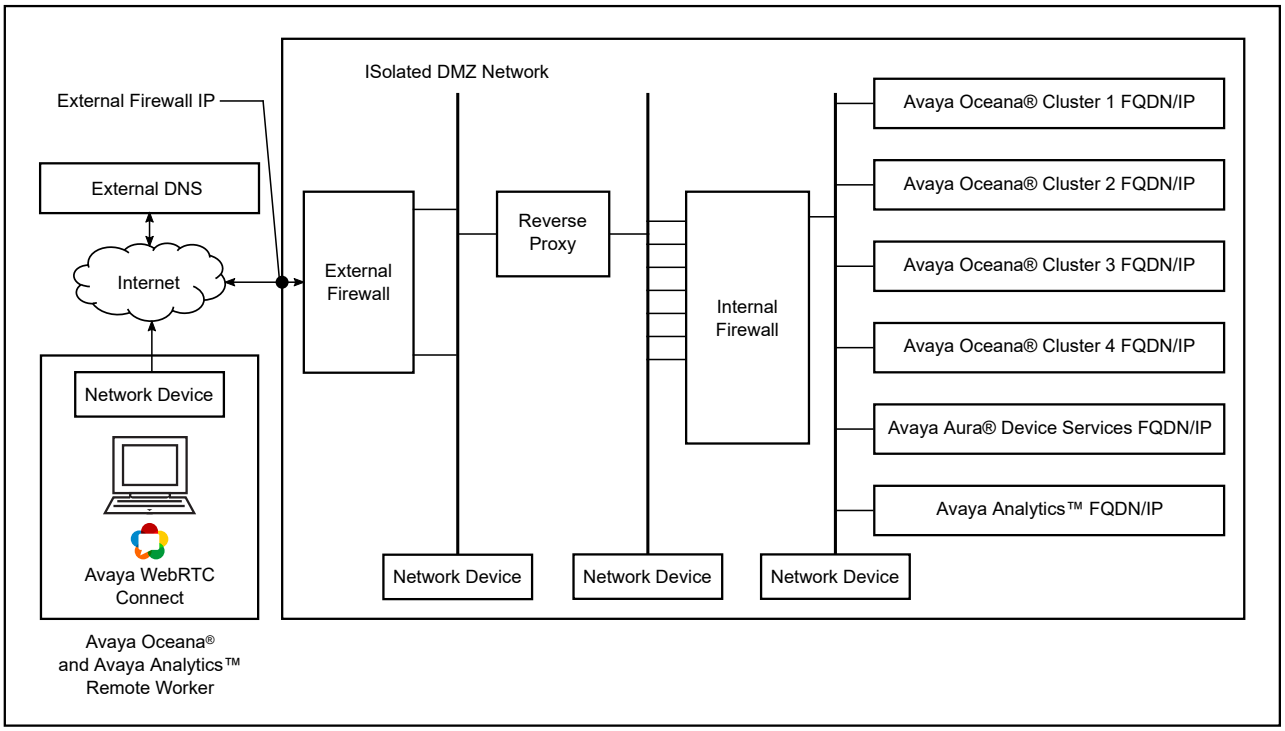


Figure 5: Remote Multimedia Worker Solution

All workers inside the bigger box use Avaya Oceana® FQDNs to directly access solution functionality on the internal LAN. All workers outside the bigger box are considered as external workers. The external workers must transit through firewall layers and network elements by using interfaces on the external firewall to connect to the Avaya Oceana® and Avaya Analytics™ applications. Customers must deploy this level of infrastructure so that remote workers can get secure access to enterprise applications.

For the remote worker capability, you must deploy and provision the following:

- Avaya Aura® Session Border Controller that acts as a TURN relay for the WebRTC Connect voice media of agents.

  You must configure and enable the following on Session Border Controller:

  - One externally facing IP address on its external (B1) side.
  - One internally facing IP address on its internal (A1) side.
  - A certificate for the B1 external interface. You use this certificate for the reverse proxy.
  - A certificate for the A1 internal interface. You use this certificate for the reverse proxy.
- External DNS capability to resolve the Avaya Oceana® and Avaya Analytics™ FQDNs to an IP address that is accessible from the Internet.
- External firewall to provide a double layer of security (DMZ) between the Internet and the backend Avaya Oceana® servers.

You must have an external firewall with the following configured items:

- One external IP address on the WAN side.
- One internal IP address on the LAN side.

You must enable the following ports on the external firewall:

- Port 443 for general signaling of the remote worker devices/clients to Avaya Oceana® AuthorizationService.
- Port 9443 for authorization of the remote worker devices/clients to contact center applications.

- Internal firewall

  You must have an internal firewall with the following configured items:

  - Up to six externally facing IP addresses on the external (WAN) side.
  - One internally facing IP address on the internal (LAN) side.

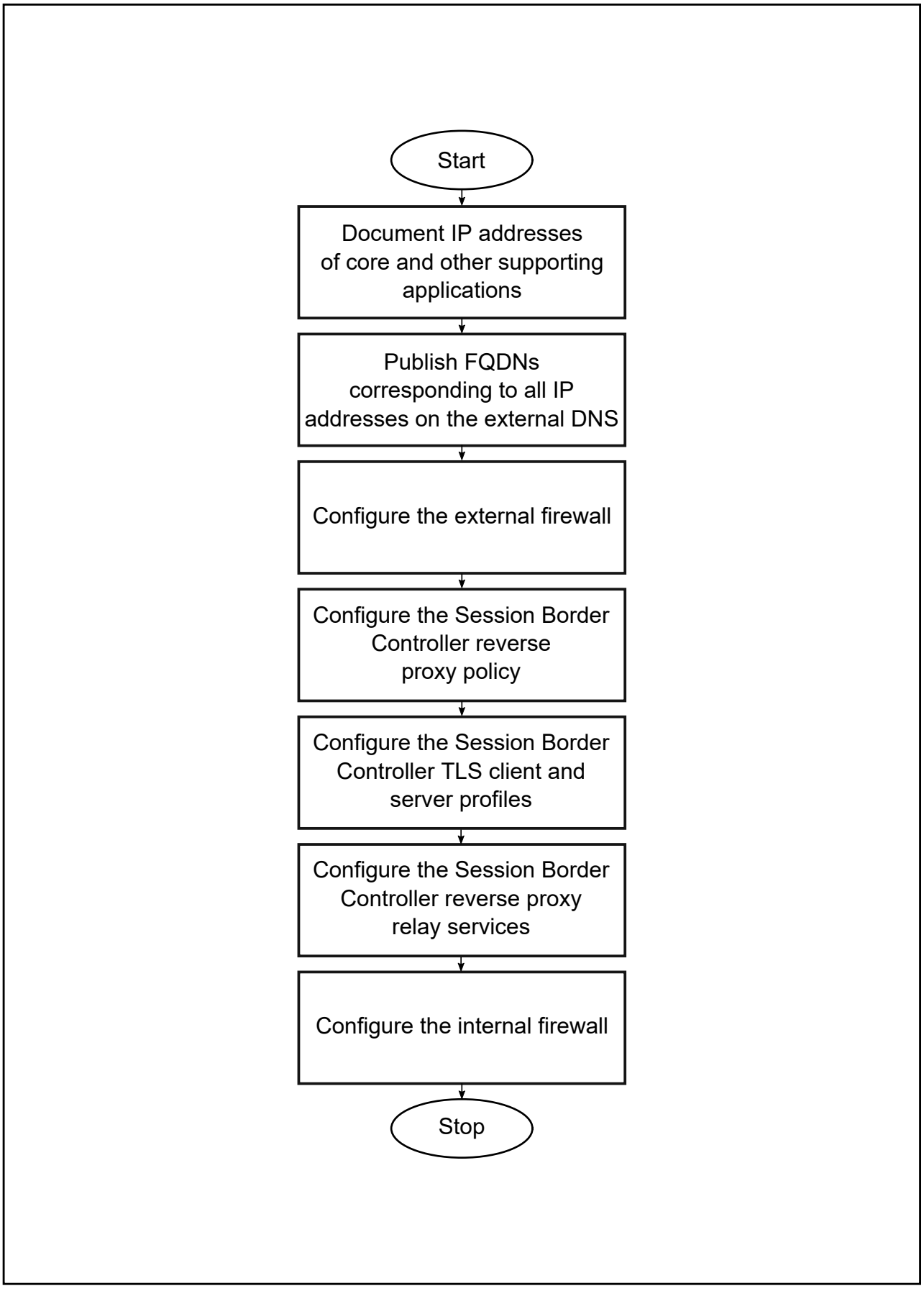
The following are the additional considerations for the remote worker solution:

- You must use the split-horizon DNS so that on-premise and remote workers can use the same FQDNs to use Avaya Oceana®. However, the FQDNs resolve to different IP addresses depending on whether the agent is remote or on-premise.
- All Avaya Oceana® FQDNs resolve to a single IP address on the external firewall and proxies are used internally to the correct Avaya Oceana® server or cluster based on the request URL from the client.
- Minimum network characteristics must be achieved with the internet connection from the remote workers to the on-premise infrastructure containing the contact center.

  Remote workers utilize Avaya Workspaces, and its performance degrades, or it becomes unresponsive on network connections with a latency greater than 300 ms Round Trip Time (RTT). Remote workers must have a reliable internet connection that can deliver an RTT less than 300 ms.
- Avaya Oceana® and Avaya Analytics™ are deployed and operational for all required channels.
- On-premise agents can log in to Avaya Workspaces and process contacts.
- Avaya Oceana® must completely use secure connections:
  - The **Only allow secure web communication** check box must be selected in the cluster attributes of all Avaya Oceana® clusters.
  - The **Secure Communications** attribute must be enabled in the OceanaConfiguration service.
- Any screen-pops required for agents must be externalized so that they are accessible to the remote agents.

Remote worker solution process flow

The following workflow shows the sequence of tasks that you must perform to deploy the remote worker solution:


Start
Document IP addresses of core and other supporting applications
Publish FQDNs corresponding to all IP addresses on the external DNS
Configure the external firewall
Configure the Session Border Controller reverse proxy policy
Configure the Session Border Controller TLS client and server profiles
Configure the Session Border Controller reverse proxy relay services
Configure the internal firewall
Stop

Configuration and deployment details for the remote worker solution

For successful deployment of the remote worker solution, you must gather all configuration and deployment details.

Documentation of FQDNs and IP addresses of solution interfaces

To deploy the remote worker solution, you must document FQDNs and IP addresses of Avaya Oceana® and Avaya Analytics™ interfaces that remote workers access during normal operations.

Publishing of FQDNs external to the enterprise for remote workers

Avaya Oceana® and Avaya Analytics™ users use FQDNs to access the functionality in the solution. In the enterprise, FQDNs are resolved to the IP addresses through the internal Domain Name Server (DNS). For example, Avaya Workspaces users access Avaya Oceana® Cluster 1 or Avaya Oceana® Cluster 2 FQDNs to login and receive basic user functionality depending on the agent footprint size.

Similar to on-premise workers, remote workers must also be able to utilize the same URLs and client requests, even though they are outside of the enterprise. Therefore, customers must publish a DNS entry for each required Avaya Oceana® and Avaya Analytics™ FQDN that remote workers use. The number of FQDNs for publishing depends on customer configuration. For example, if a customer does not require Co-Browsing functionality, then the customer does not need to publish the Avaya Oceana® Cluster 4 FQDN.

When the remote worker accesses or requests a URL containing the Avaya Oceana® FQDNs, the FQDNs are resolved to a single IP, which is the external firewall Listen IP address.

Function and role of the external firewall for remote workers

All remote worker requests terminate on a single IP address on the external firewall. With the configuration rule on the firewall, the requests are translated into internal addresses and ports by using Network Address Translation (NAT). Customers must configure their external firewall to translate requests coming in on different ports towards the next application in the chain, which is the reverse proxy. The external firewall allows the requests to go to the reverse proxy.

The reverse proxy forwards the requests to the unique IP address and port to the internal firewall based on the path in the request URL.

Function and role the reverse proxy for remote workers

The reverse proxy determines which URL requests must be allowed and how the requests must flow into the enterprise applications. It also relays the reverse communications to remote workers.

The reverse proxy is configured with a set of rules that analyze the request URLs and allow the requests to go to the backend Avaya Oceana® servers.

Reverse proxy policies, TLS profiles, and relay services

Session Border Controller and reverse proxy perform many essential functions that must be appropriately configured on each deployment:

- Many whitelist relays require a WebSocket connection. Therefore, on Session Border Controller, you must create a reverse proxy policy with WebSockets enabled.
- Session Border Controller reverse proxy relay requires the following:
  - A TLS client profile for the interface facing the internal Intranet Avaya Oceana® and Avaya Analytics™ servers/clusters
  - A TLS server profile for the interface facing the Internet
- For each server/cluster:port combination, you must configure a reverse proxy relay service. For multiple servers using the same port, such as 443, Session Border Controller directs the requests to the appropriate back-end server/cluster based on the URL in the request.

  For example, you must configure a relay service for each of the following:
  - Avaya Oceana® clusters containing the Authorization service
  - Avaya Analytics™ Real-time and Historical Reporting

Function and role of the internal firewall for remote workers

An internal firewall is the final application before the enterprise applications. On its external (WAN) side, internal firewall communicates with various IP addresses and ports allocated to Avaya Oceana® and Avaya Analytics™ servers/clusters. Using the NAT functionality and preconfigured rules, it routes all allowed requests through to Avaya Oceana® and Avaya Analytics™ servers on the internal network.

Connectivity details of remote workers

Remote workers connect to the Avaya Oceana® contact center similar to how they connect within the enterprise. They access Avaya Workspaces and Avaya Analytics™ clients. Remote workers potentially access admin clients for both of these applications.

Remote workers do not need to log in to an Enterprise VPN to access the Avaya Oceana® and Avaya Analytics™ applications.

Example of remote workers accessing Avaya Workspaces and Avaya Analytics™

A remote worker opens a supported browser and accesses the URL for Avaya Workspaces and Avaya Analytics™.

For example, https://*<AvayaOceanaCluster FQDN Mapped with both IP addresses>*/services/UnifiedAgentController/workspaces/#/login.

Based on the externally published FQDNs, the FQDN is resolved to the external firewall IP address and the request is directed to the external firewall. Functions of the external firewall are:

- External firewall allows the requests from remote workers through to the reverse proxy.
- Reverse proxy already has the configuration information set up to allow the requests to be processed securely. After checking the validity of the requests, the requests are forwarded to an internal IP address and port destination on the internal firewall.

- For any Avaya Oceana® and Avaya Analytics™ solution, the reverse proxy has NAT entries for the different Avaya Oceana® and Avaya Analytics™ servers.

Chapter 29: Deploy Web Voice and Web Video for remote workers

Deploy Web Voice and Web Video for remote workers overview

Avaya Oceana® provides Web Voice and Web Video configurations for remote workers. Based on your requirements, you can choose from the following configurations and complete all tasks:

- Avaya Oceana® with WebRTC Connect agents.

  With this configuration, WebRTC Connect agents can answer PSTN voice calls.

- Avaya Oceana® with web and mobile voice calls.

  With this configuration, phone-enabled agents can answer web and mobile voice calls that customers make through web and mobile devices on the public Internet.

- Avaya Oceana® with web and mobile voice calls and WebRTC Connect agents.

  With this configuration, WebRTC Connect and phone-enabled agents can answer PSTN, web, and mobile voice calls.

- Avaya Oceana® with web and mobile video calls and WebRTC Connect agents.

  With this configuration, WebRTC Connect agents can answer web and mobile video calls.

Important:

WebRTC Connect agents do not support the Auto answer feature. Therefore, do not configure WebRTC Connect agents to use this feature.

Checklist for configuring Avaya Oceana® with remote Avaya WebRTC Connect agents

Use the following checklist to configure Avaya Oceana® with remote WebRTC Connect agents so that the agents can answer PSTN Voice, Web Voice, and Web Video calls:

No.	Task	Description	✔
1	Install and configure Avaya Aura® Device Services, Avaya Aura® Media Server, and Avaya Aura® Web Gateway.	See the following: • Avaya Aura Device Services deployment on page 380. • Avaya Aura Media Server deployment on page 386. • Avaya Aura Web Gateway deployment and configuration on page 400.	
2	Configure authorization on Avaya Aura® Web Gateway.	See Avaya Aura Web Gateway authorization on page 407.	
3	Create Web Voice and Web Video agents that can use media in browsers.	See Creating a user in Avaya Control Manager on page 413.	
4	Install and configure Avaya Aura® Session Border Controller to enable customer PSTN Voice, Web Voice, and Web Video calls from the public internet.	See Install and configure Avaya Aura Session Border Controller on page 490.	
5	Deploy Identity Certificate on Avaya Aura® Session Border Controller.	See Deploying Identity Certificate on Avaya Aura Session Border Controller on page 427.	
6	Configure Avaya Breeze® platform so that voice and video calls can be anchored on Avaya Breeze® platform with wait treatment.	See Install and configure Avaya Aura Media Server for Avaya Breeze platform on page 386.	
7	Route web and mobile voice and video calls to WebRTC Connect Engagement Designer workflows sequencing the AvayaMobileCommunications service.	See Route web and mobile voice calls to Avaya WebRTC Connect workflows on page 443.	
8	Configuring the Javascript web reference client, and making Web Voice and Web Video calls for testing and validation.	See Configuring the Javascript reference client and making a call on page 418.	

Install and configure Avaya Aura® Session Border Controller

Avaya Oceana® requires Avaya Aura® Session Border Controller to enable calls from the public internet. Therefore, you must install Avaya Aura® Session Border Controller as a part of your solution. For information about how to install Avaya Aura® Session Border Controller, see *Deploying Avaya Session Border Controller on a Hardware Platform*.

Checklist for installing and configuring Session Border Controller for remote workers

Use the following checklist to install and configure Session Border Controller for remote workers:

No.	Task	Description	✔
1	Configure Avaya Aura® Session Border Controller networks.	See Configuring Avaya Aura Session Border Controller networks on page 425.	
2	Create a reverse proxy policy.	See Creating a reverse proxy policy on page 426.	
3	Create the common client certificate.	See Creating the common client certificate on page 427.	
4	Create the common server certificate.	See Creating the common server certificate on page 428.	
5	Create a client profile for the Avaya Aura® Web Gateway reverse proxy.	See Creating a client profile for the Avaya Aura Web Gateway reverse proxy on page 429.	
6	Create a server profile for the Avaya Aura® Web Gateway reverse proxy.	See Creating a server profile for the Avaya Aura Web Gateway reverse proxy on page 430.	
7	Configure reverse proxy relay services.	See Configure reverse proxy relay services on page 491.	
9	Configure Avaya WebRTC Connect client-side TURN	See Configure Avaya WebRTC Connect client-side TURN on page 499.	
9	Configure the trunk on Session Border Controller for PSTN customer calls.	See Configure the trunk on Session Border Controller for PSTN customer calls on page 502.	
10	Configure TLS client and server profiles.	See Configure TLS client and server profiles on page 504.	

Configure reverse proxy relay services

For each server/cluster:port combination, you must configure a reverse proxy relay service. For multiple servers using the same port, such as 443, Avaya Aura® Session Border Controller directs the requests to the appropriate back-end server/cluster based on the URL in the request.

Configuring a relay service for Avaya Analytics™ historical reporting

About this task

Use this procedure to configure a reverse proxy relay service for Avaya Analytics™ historical reporting.

Procedure

1. Log on to the EMS web interface with administrator credentials.

2. In the navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.
3. On the Reverse Proxy tab, click **Add**.
4. On the Add Reverse Proxy Profile page, do the following:
    a. In the **Service Name** field, type the reverse proxy profile name.

       For example, analytics-historical.
    b. Select the **Enabled** check box.
    c. In the **Listen IP** field, select the B1 external network and then select the B1 IP address used for the relay.
    d. In the **Listen Port** field, type the Avaya Analytics™ historical port number as 9503.
    e. In the **Listen Protocol** field, click HTTPS.
    f. In the **Listen TLS Profile** field, select the server profile associated with the B1 interface.
    g. Leave the **Listen Domain** field blank.
    h. In the **Connect IP** field, select the internal A1 network and then select the A1 interface IP address used for the relay.
    i. In the **Server Protocol** field, click HTTPS.
    j. In the **Server TLS Profile** field, select the client profile you previously created for the internal A1 interface.
    k. In the **Reverse Proxy Policy Profile** field, select the default reverse proxy policy profile.
    l. In the **Server Addresses** field, type the internal firewall IP address assigned to the Avaya Analytics™ historical reporting server and port number 9503.
    m. In the **Whitelisted URL** field, type `/analytics`.
    n. Click **Finish**.

Configuring a REST relay service for Avaya Analytics™ real-time reporting

About this task

Use this procedure to configure a REST relay service for Avaya Analytics™ real-time reporting.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.
3. On the Reverse Proxy tab, click **Add**.
4. On the Add Reverse Proxy Profile page, do the following:
    a. In the **Service Name** field, type the reverse proxy profile name.

For example, analytics-realtime_8443.

b. Select the **Enabled** check box.

c. In the **Listen IP** field, select the B1 external network and then select the B1 IP address used for the relay.

d. In the **Listen Port** field, type the Avaya Analytics™ real-time REST port number as 8443.

e. In the **Listen Protocol** field, click HTTPS.

f. In the **Listen TLS Profile** field, select the server profile associated with the B1 interface.

g. Leave the **Listen Domain** field blank.

h. In the **Connect IP** field, select the internal A1 network and then select the A1 interface IP address used for the relay.

i. In the **Server Protocol** field, click HTTPS.

j. In the **Server TLS Profile** field, select the client profile you previously created for the internal A1 interface.

k. In the **Reverse Proxy Policy Profile** field, select the default reverse proxy policy profile.

l. In the **Server Addresses** field, type the internal firewall IP address assigned to the Avaya Analytics™ real-time reporting server and port number 8443.

m. In the **Whitelisted URL** field type `/sources`.

n. Click **Finish**.

Configuring a WebSocket relay service for Avaya Analytics™ real-time reporting

About this task

Use this procedure to configure a WebSocket relay service for Avaya Analytics™ real-time reporting.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.
3. On the Reverse Proxy tab, click **Add**.
4. On the Add Reverse Proxy Profile page, do the following:
   a. In the **Service Name** field, type the reverse proxy profile name.

      For example, analytics-realtime_8422.

   b. Select the **Enabled** check box.

   c. In the **Listen IP** field, select the B1 external network and then select the B1 IP address used for the relay.

d. In the **Listen Port** field, type the Avaya Analytics™ real-time WebSocket port number as 8422.
e. In the **Listen Protocol** field, click HTTPS.
f. In the **Listen TLS Profile** field, select the server profile associated with the B1 interface.
g. Leave the **Listen Domain** field blank.
h. In the **Connect IP** field, select the internal A1 network and then select the A1 interface IP address used for the relay.
i. In the **Server Protocol** field, click HTTPS.
j. In the **Server TLS Profile** field, select the client profile you previously created for the internal A1 interface.
k. In the **Reverse Proxy Policy Profile** field, select the reverse proxy policy profile with WebSockets enabled.
l. In the **Server Addresses** field, type the internal firewall IP address assigned to the Avaya Analytics™ real-time reporting server and port number 8422.
m. In the **Whitelisted URL** field type `/advrealtime`.
n. Click **Finish**.

Configuring a relay service for Avaya Oceana® AuthorizationService

About this task

Use this procedure to configure a relay service for the Avaya Oceana® AuthorizationService.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.
3. On the Reverse Proxy tab, click **Add**.
4. On the Add Reverse Proxy Profile page, do the following:
   a. In the **Service Name** field, type the reverse proxy profile name.

      For example, Oceana_AuthService.
   b. Select the **Enabled** check box.
   c. In the **Listen IP** field, select the B1 external network and then select the B1 IP address used for the relay.
   d. In the **Listen Port** field, type the Avaya Oceana® AuthorizationService port number as 9443.
   e. In the **Listen Protocol** field, click HTTPS.
   f. In the **Listen TLS Profile** field, select the server profile associated with the B1 interface.

g. Leave the **Listen Domain** field blank.
h. In the **Connect IP** field, select the internal A1 network and then select the A1 interface IP address used for the relay.
i. In the **Server Protocol** field, click HTTPS.
j. In the **Server TLS Profile** field, select the client profile you previously created for the internal A1 interface.
k. In the **Reverse Proxy Policy Profile** field, select the default reverse proxy policy profile.
l. In the **Server Addresses** field, type *<Avaya Oceana Cluster IP/FQDN>*:*9443*.

   <Avaya Oceana Cluster IP/FQDN> is the internal firewall IP address of the cluster that hosts the UnifiedAgentController service.
m. In the **Whitelisted URL** field type `/services/AuthorizationService`.
n. Click **Finish**.

5. If you get the `specified port overlaps with range (9000-9999) use some different port` error, do the following:
   a. In the navigation pane, click **Network & Flows** > **Advanced Options** > **Port Ranges**.
   b. Change the **Listen Port Range** to 9000-9400.
6. Repeat Steps 2 to 4.

Configuring the relay service for token-generation-service for Avaya Aura® Web Gateway

Before you begin

Create a reverse proxy policy through the EMS web interface, ensuring that the **Allow Web Socket** field for the reverse proxy policy is set to `Y`.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.
3. On the Reverse Proxy tab, click **Add**.

   The Add Reverse Proxy Profile page opens.
4. In the **Service Name** field, type the reverse proxy profile name.
5. Select the **Enabled** check box.
6. In the **Listen IP** field, click the external IP address of Session Border Controller.
7. In the **Listen Port** field, type the port number as 443.
8. In the **Listen Protocol** field, click HTTP/HTTPS.

9. In the **Listen TLS Profile** field, click the relevant TLS Profile.
10. In the **Server Protocol** field, click HTTP/HTTPS.
11. In the **Connect IP** field, click the internal IP address of Session Border Controller.
12. In the **Reverse Proxy Policy Profile** field, click the reverse proxy policy that you create.
13. In the **Server Addresses** field, type `<Avaya Aura Web Gateway_FQDN>:<port number>`.

    Use the FQDN based on what you use in the SAN name when creating the TLS certificate.

    The default port number on Avaya Aura® Web Gateway is 443. The value of *<port number>* must be the same as the port number configured in the **Front-end port** field on the HTTP Reverse Proxy page in Avaya Aura® Web Gateway.

    To go to the **HTTP Reverse Proxy** page, you must log on to the Avaya Aura® Web Gateway administration portal and click **External Access** > **HTTP Reverse Proxy**.
14. In the **Whitelisted URL** field, type `/token-generation-service/`.
15. Click **Finish**.

Configuring the relay service for Avaya Aura® Web Gateway for the external remote access

Before you begin

Create a reverse proxy policy through the EMS web interface, ensuring that the **Allow Web Socket** field for the reverse proxy policy is set to `Y`.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.
3. On the Reverse Proxy tab, click **Add**.

   The Add Reverse Proxy Profile page opens.
4. In the **Service Name** field, type the reverse proxy profile name.
5. Select the **Enabled** check box.
6. In the **Listen IP** field, click the external IP address of Session Border Controller.
7. In the **Listen Port** field, type the port number as 443.
8. In the **Listen Protocol** field, click HTTP/HTTPS.
9. In the **Listen TLS Profile** field, click the relevant TLS Profile.
10. In the **Server Protocol** field, click HTTP/HTTPS.
11. In the **Connect IP** field, click the internal IP address of Session Border Controller.
12. In the **Reverse Proxy Policy Profile** field, click the reverse proxy policy that you create.

13. In the **Server Addresses** field, type *<Avaya Aura Web Gateway_FQDN>*:*<port number>*.

    Use the FQDN based on what you use in the SAN name when creating the TLS certificate.

    The default port number on Avaya Aura® Web Gateway is 8444. The value of *<port number>* must be the same as the port number configured in the **Front-end port for external access** field on the HTTP Reverse Proxy page in Avaya Aura® Web Gateway on **Enable port for external access**.

    To go to the **HTTP Reverse Proxy** page, you must log on to the Avaya Aura® Web Gateway administration portal and click **External Access** > **HTTP Reverse Proxy**.

14. In the **Whitelisted URL** field, type `/csa/`.
15. Click **Finish**.

Configuring a relay service for Avaya Oceana® port 443

About this task

Use this procedure to configure a relay service for Avaya Oceana® port 443.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.
3. On the Reverse Proxy tab, click **Add**.
4. On the Add Reverse Proxy Profile page, do the following:
    a. In the **Service Name** field, type the reverse proxy profile name.

       For example, Oceana_Relay.

    b. Select the **Enabled** check box.
    c. In the **Listen IP** field, select the B1 external network and then select the B1 IP address used for the relay.
    d. In the **Listen Port** field, type the Avaya Oceana® secure port number 443.
    e. In the **Listen Protocol** field, click HTTPS.
    f. In the **Listen TLS Profile** field, select the server profile associated with the B1 interface.
    g. Leave the **Listen Domain** field blank.
    h. In the **Connect IP** field, select the internal A1 network and then select the A1 interface IP address used for the relay.
    i. In the **Server Protocol** field, click HTTPS.
    j. In the **Server TLS Profile** field, select the client profile you previously created for the internal A1 interface.

k. In the **Reverse Proxy Policy Profile** field, select the reverse proxy policy profile with WebSockets enabled.

l. In the **Server Addresses** and **Whitelisted URL** fields, type the address:port and URL combinations that are required for all applicable Avaya Oceana® servers/clusters. The Server Address is the IP address on the internal firewall that is allocated to each server/cluster.

m. Click **Finish**.

For information about mandatory whitelist configuration for Web Voice, see the table in Configure the reverse proxy for Web Voice and Web Video remote workers on page 498.

Configure the reverse proxy for Web Voice and Web Video remote workers

The reverse proxy determines which URL requests is allowed and how the requests must flow into the enterprise applications. They also determine the reverse communications to remote workers.

The reverse proxy is configured with a whitelist. Customers configure the whitelist for their deployment and it has all internal Avaya Oceana® and Avaya Analytics™ URLs that all workers require to access the contact center functionality.

The following table shows a sample whitelist configuration:

Cluster/Server	Whitelist URL in Request	Reverse Proxy Listen IP	Listen Port	Internal Firewall Destination IP	Internal Firewall Port
Avaya Oceana® Cluster 1	/services/CustomerManagement/				
Avaya Oceana® Cluster 1	/services/OCPDataServices/				
Avaya Oceana® Cluster 1	/services/CustomerJourneyService/				
Avaya Oceana® Cluster 2	/services/UnifiedAgentController/				
Avaya Oceana® Cluster 2	/services/Broadcast-UnifiedAgentController/				
Avaya Oceana® Cluster 3	/services/AgentControllerService/				

Table continues…

Cluster/Server	Whitelist URL in Request	Reverse Proxy Listen IP	Listen Port	Internal Firewall Destination IP	Internal Firewall Port
Avaya Oceana® Cluster 3	/services/CustomerControllerService/				
Avaya Oceana® Cluster 4	/services/CoBrowse/				
Avaya Analytics™	/orca-streams-rest/ /orca-streams-data-publisher/ /AvayaAnalytics/				
Avaya Aura® Device Services	/acs/				
Avaya Aura® Device Services	/notification/				
Avaya Oceana® Cluster 2	/services/AuthorizationService				

A remote worker, who requests a destination containing an internal URL in the HTTPS request such as /services/CustomerManagement/, is forwarded to a preconfigured IP address and port on the internal firewall for that URL. The internal firewall uses its own rule (NAT) to allow or deny this request into the final internal destination component in Avaya Oceana® and Avaya Analytics™.

Note:

For the following clusters, reverse proxy relays require you to enable WebSockets on the proxy connection:

- Avaya Oceana® Cluster 2 (UnifiedAgentController)
- Avaya Oceana® Cluster 4 (CoBrowse)
- Avaya Analytics™

Configure Avaya WebRTC Connect client-side TURN

Avaya Oceana® supports the client-side TURN for WebRTC Connect calls from the public internet.

Adding a TURN/STUN service for Avaya WebRTC Connect clients

Procedure

1. Log on to the EMS web interface with administrator credentials.

2. In the navigation pane, click **DMZ Services** > **TURN/STUN Service** > **TURN/STUN Profiles**.
3. On the TURN/STUN Profiles tab, click **Add** and do the following:
   a. In the **Profile Name** field, type an appropriate name.
   b. In the **UDP Listen Port** field, type `3478`.
   c. In the **TCP/TLS Listen Port** field, type `443`.
   d. In the **TLS Server Profile** field, select the profile create in Creating a server profile for the TLS TURN relay on page 434.
   e. In the **Media Relay Port Range** field, type a value between 50000 to 55000.
   f. In the **Authentication** field, enable the authentication.
   g. In the **Client Authentication** field, enable the authentication.
   h. In the **Realm** field, specify the SIP domain.
   i. In the **UDP Relay** field, enable the UDP relay.
   j. Click **Finish**.
4. On the TURN Relay tab, click **Add** and do the following:
   a. In the **Listen IP** field, enter the external interface IP configured on Avaya Aura® Session Border Controller that external clients use.
   b. In the **Media Relay IP** field, enter the internal IP configured on Avaya Aura® Session Border Controller that Avaya Aura® Web Gateway Avaya Aura® Media Server uses for media.
   c. Keep the **Service FQDN** field blank.
   d. In the **TURN/STUN Profile** field, select the TURN/STUN profile that you created.
   e. Click **Finish**.

Enabling Avaya WebRTC Connect client-side TURN on Avaya Aura® Web Gateway

Procedure

1. In your web browser, enter the following URL to log on to the Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. Log on to Avaya Aura® Web Gateway administration portal with your administrator credentials.
3. On the Avaya Aura® Web Gateway administration portal, click **External Access** > **Session Border Controller**.
4. Select the **Enable TURN in WebRTC Client** check box.
5. Click **Save**.

Adding the STUN server configuration to Avaya Aura® Web Gateway

Procedure

1. In your web browser, enter the following URL:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. Log on to the Avaya Aura® Web Gateway administration portal with your administrator credentials.
3. Click **External Access** > **STUN Servers**.
4. Click **Add**.
5. In the **Address** field, enter the address of the STUN server.

   Based on the network configuration of Avaya Aura® Session Border Controller, this address can be one of the following:

   - The external IP address that you use when configuring the TURN Relay in Avaya Aura® Session Border Controller.
   - The address on the external firewall that receives media and directs it to the Avaya Aura® Session Border Controller Relay IP address.

6. In the **Port** field, type `3478`.
7. Click **Save**.
8. To set the STUN priority, select the newly added STUN server and click **Add** to add it to the list of Assigned STUN servers.
9. Click **Save**.

Changing the load balancing configuration in Session Border Controller

About this task

Use this procedure to fix the Avaya Aura® Web Gateway load monitoring by changing the load balancing configuration in Session Border Controller.

Procedure

1. Log in to the Avaya Aura® Session Border Controller web administration portal.
2. In the navigation pane, click **Device Specific Settings** > **Advanced Options** > **Load Monitoring**.
3. On the Edit Load Balancer Config dialog box, do the following:
   a. In the **Transport** field, select `TCP`.
   b. In the **Service Type** field, select `Turn`.

Configuring the HTTP port and protocol of Avaya Aura® Session Border Controller

About this task

Use this procedure to configure the HTTP port and protocol of Avaya Aura® Session Border Controller to match the TCP transport type configured on Session Border Controller.

Procedure

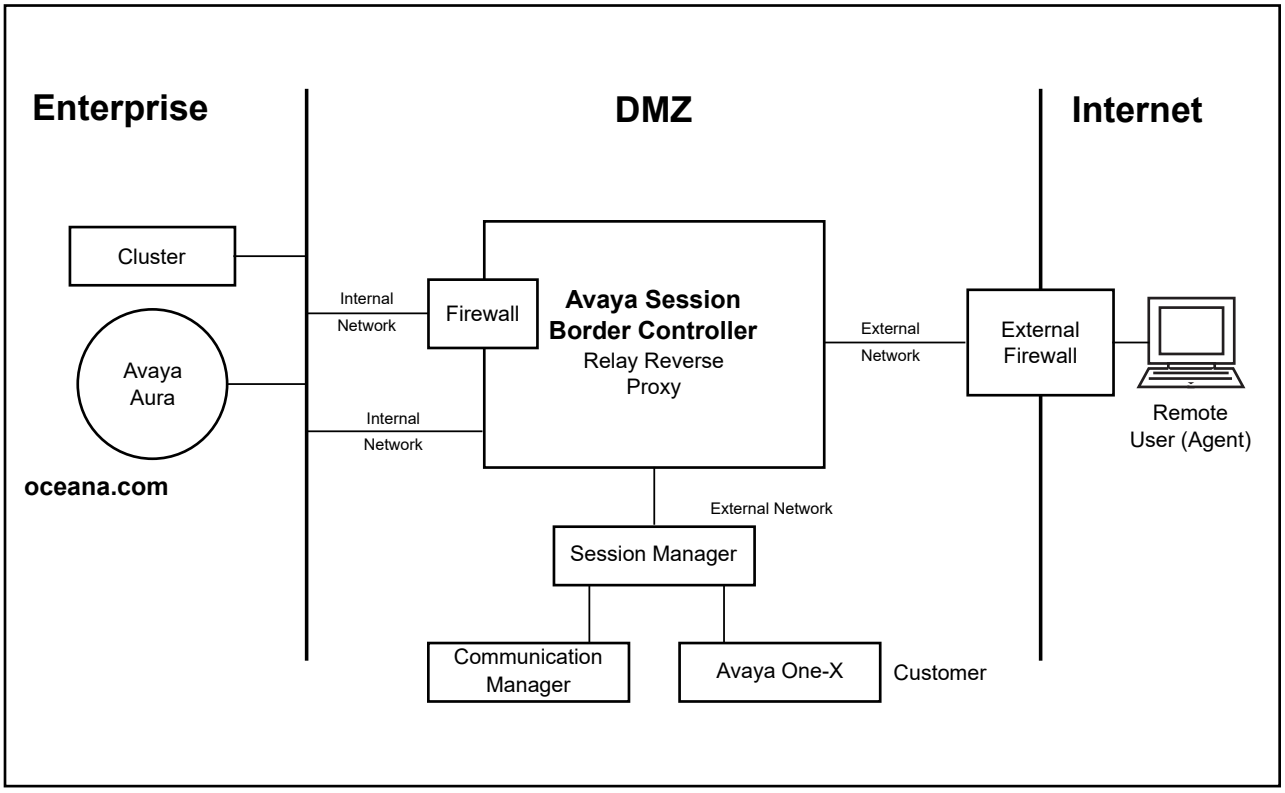
1. In your web browser, enter the following URL:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. On the Avaya Aura® Web Gateway administration portal, click **External Access** > **Session Border Controller**.
3. Select the Session Border Controller and click **Edit**.
4. In the **HTTP Port** field, type `80`.
5. In the **HTTP Protocol** field, select `http`.
6. Click **Save**

Configure the trunk on Session Border Controller for PSTN customer calls

The following diagram depicts the architecture for PSTN call to remote workers:



Configuring Avaya Aura® Session Border Controller networks for PSTN calls

About this task

Avaya Oceana® exclusively supports on-premise Avaya Workspaces agents. It specifies that the agents must be on-site, behind the enterprise firewalls to log on to Avaya Workspaces and accept contacts. This procedure has a reference configuration where the PSTN customers make calls through the Session Border Controller trunk. Session Border Controller can be configured to allow external agents to access Avaya Oceana® from a remote location with Internet access, so that

PSTN trunk calls are routed to the remote location agent through the Session Border Controller trunk.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **Network Management** > **Interfaces**.
3. On the Interfaces page, enable the following interfaces:
   - A1 internal interface
   - B1 external interface
4. On the Networks tab, configure the following networks:
   - A1 internal network
   - B1 external network
5. For external PSTN trunk access, assign the IP addresses to each network as follows:

   The external IP address:

   - One IP address for the external network.

   Three internal IP address:

   - One IP address for the internal network.

Creating a routing profile for customer Session Manager entity on Session Border Controller

About this task

Use this procedure to create a routing profile that creates a trunk between Session Border Controller and customer Session Manager.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Configuration Profiles** > **Routing**.
3. In the content pane, click **Add**.
4. In the **Profile Name** field, enter a name for the customer Session Manager trunk.

   For example, SM2_Trunk.
5. Set the **Time of Day** field to `default`.
6. Set the **Load Balancing** field to `Priority`.
7. Set the **Next Hop Address** field to customer Session Manager.
8. Set the **TLS** port to `5061`.
9. Click **Finish**.

Creating a topology hiding profile

About this task

Use this procedure to create a topology hiding between the agent and customer domains on Session Border Controller.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Configuration Profiles** > **Topology Hiding**.
3. In the content pane, click **Add**.
4. In the **Profile Name** field, enter a name for the customer domain trunk.

   For example, wslab.com.
5. Enter relevant details in the **From**, **To**, **Request Line**, and **SDP Headers** fields.
6. Click **Finish**.

Configure TLS client and server profiles

The Session Border Controller PSTN trunk requires a TLS client and a TLS server profile. The client profile is for the interface facing towards the internal Avaya Oceana®/Avaya Analytics™ servers/clusters, and the server profile is for the interface facing the Internet.

Creating a TLS client profile

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **TLS Management** > **Client Profiles**.
3. On the Client Profiles page, click **Add**.
4. In the **Profile Name** field, type the name of the profile.

   For example, client_sm247.
5. In the **Certificate** field, select a certificate corresponding to the internal interface IP address that acts as a **Connect IP** for SIP Trunk.

   For this reference configuration, the certificate used has the Session Border Controller FQDN as the CN and included the FQDN and the A1 interface IP address in the Subject Alternate Name (SAN).
6. In the **Peer Certificate Authority** field, select the CA that is used to sign the identity certificates for the internal Avaya Oceana®/Avaya Analytics™ servers/clusters.
7. In the **Verification Depth** field, type 1.
8. Keep other fields at default values.
9. Click **Next**
10. Click **Finish**

Creating a TLS server profile

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **TLS Management** > **Server Profiles**.
3. On the Server Profiles page, click **Add**.
4. In the **Profile Name** field, type the name of the profile.

   For example, Server_sm247.
5. In the **Certificate** field, select a certificate corresponding to the external interface IP that you need to specify in the **Listen IP** field for the SIP Trunk.

   For this reference configuration, the certificate used has the Session Border Controller FQDN as the CN and included the FQDN and the B1 interface IP address in the Subject Alternate Name (SAN).
6. In the **Peer Verification** field, click **None**.
7. Keep the default values in the other fields.
8. Click **Next**
9. Click **Finish**.

Creating a SIP entity between the Session Border Controller external interface and customer Session Manager

About this task

Use this procedure to create a SIP entity between the Session Border Controller external interface and customer Session Manager on the customer System Manager.

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **SIP Entities**.
2. On the SIP Entities page, click **New**.
3. In the **Name** field, enter a name for the SIP entity.
4. In the **FQDN or IP Address** field, enter the FQDN or IP address of the SIP entity.
5. In the **Type** field, select **SIP Trunk**.
6. Click **Commit**.

Creating a routing policy for the Session Border Controller external interface SIP entity link

About this task

A routing policy defines how Session Manager routes calls between SIP network elements. Session Manager uses the data configured in the routing policy to find the best match against the number or address of the called party.

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **Routing Policies**.
2. Verify the routing policy for the Experience Portal Media Processing Platform entity link.

   If the routing policy does not exist, complete the remainder of this procedure.
3. On the Routing Policies page, click **New**.
4. In the **Name** field, enter a name for the routing policy.

   For example, SBC_Trunk.
5. In the **Retries** field, enter the number of retries.
6. In the SIP Entity as Destination section, click **Select**.
7. Select the Session Border Controller external interface SIP entity as the destination for the routing policy and click **Select**.
8. Click **Commit**.

Creating a SIP entity between the Session Border Controller internal interface and agent Session Manager

About this task

Use this procedure to create a SIP entity between the Session Border Controller internal interface and agent Session Manager on the agent System Manager.

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **SIP Entities**.
2. On the SIP Entities page, click **New**.
3. In the **Name** field, enter a name for the SIP entity.
4. In the **FQDN or IP Address** field, enter the FQDN or IP address of the SIP entity.
5. In the **Type** field, select **SIP Trunk**.
6. Click **Commit**.

Creating a routing policy for the Session Border Controller internal interface SIP entity link

About this task

A routing policy defines how Session Manager routes calls between SIP network elements. Session Manager uses the data configured in the routing policy to find the best match against the number or address of the called party.

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **Routing Policies**.
2. Verify the routing policy for the Experience Portal Media Processing Platform entity link.

   If the routing policy does not exist, complete the remainder of this procedure.

3. On the Routing Policies page, click **New**.
4. In the **Name** field, enter a name for the routing policy.

   For example, SBC_Trunk.
5. In the **Retries** field, enter the number of retries.
6. In the SIP Entity as Destination section, click **Select**.
7. Select the Session Border Controller internal interface SIP entity as the destination for the routing policy and click **Select**.
8. Click **Commit**.

Chapter 30: Configure Avaya Session Border Controller for external mobile client access

Overview

Avaya Aura® Session Border Controller supports incoming calls from WebRTC-enabled web browsers to an internal Avaya Aura® network with SIP at the core. For example, a consumer can call an Avaya Aura® network by using a WebRTC-enabled browser from an external network.

This chapter describes the Avaya Aura® Session Border Controller configuration process for external mobile client access.

Configuring the TLS server profile for Avaya Aura® Session Border Controller external communication

About this task

Avaya Aura® Session Border Controller uses a TLS server profile to process an incoming connection over TLS from a remote client.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. In the navigation pane, click **TLS Management** > **Server Profiles**.
4. On the Server Profiles page, click **Add**.
5. In the **Profile Name** field, type the name of the profile.
6. In the **Certificate** field, select the certificate for external communication.
7. In the **SNI Options** field, click **None**.
8. In the **Peer Verification** field, click **None**.
9. Leave the **Extended Hostname Verification** check box cleared.

10. In the **Renegotiation Time** field, set the value to `0`.
11. In the **Renegotiation Byte Count** field, set the value to `0`.
12. In the **Version of handshake options** field, select `TLS 1.2`.
13. In the **Ciphers** field, set the value to `Default`.

    For more information, see *Administering Avaya Session Border Controller*.
14. Click **Finish**.

Configuring the TLS server profile for Avaya Aura® Session Border Controller media tunneling

About this task

With a TLS profile, Avaya Aura® Session Border Controller can control parameters when it performs a TLS handshake with a remote entity. HTTPS media tunneling requires its own TLS server profile. Session Border Controller supports media tunneling for sign-in and guest users. This configuration is required only for external mobile calls that are inbound towards Session Border Controller.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. In the navigation pane, click **TLS Management** > **Server Profiles**.
4. On the Server Profiles page, click **Add**.
5. In the **Profile Name** field, type the name of the profile.
6. In the **Certificate** field, select the certificate that the TLS server profile uses for external communication.
7. In the **SNI Options** field, click **None**.
8. In the **Peer Verification** field, click **Optional**.
9. Leave the **Peer Certificate Authorities** field empty.
10. Leave the **Peer Certificate Revocation Lists** field empty.
11. In the **Verification Depth** field, set the value to `1`.
12. Leave the **Extended Hostname Verification** check box cleared.
13. In the **Renegotiation Time** field, set the value to `0`.
14. In the **Renegotiation Byte Count** field, set the value to `0`.
15. In the **Version of handshake options** field, select `TLS 1.2`.

16. In the **Ciphers** field, set the value to `Default`.

    For more information, see *Administering Avaya Session Border Controller*.

17. Click **Finish**.

Configuring the TLS client profile on Avaya Aura® Session Border Controller

About this task

A TLS client profile is used when Avaya Aura® Session Border Controller starts an outgoing connection towards a remote entity over TLS.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. In the navigation pane, click **TLS Management** > **Server Profiles**.
4. On the Server Profiles page, click **Add**.
5. In the **Profile Name** field, type the name of the profile.
6. In the **Certificate** field, select the certificate for internal communication.
7. In the **SNI Options** field, click **None**.
8. In the **Peer Verification** field, click **Required**.
9. In the **Peer Certificate Authorities** field, select the System Manager Certificate Authority certificate.
10. Leave the **Peer Certificate Revocation Lists** field empty.
11. In the **Verification Depth** field, set the value to `1`.
12. Leave the **Extended Hostname Verification** check box cleared.
13. In the **Renegotiation Time** field, set the value to `0`.
14. In the **Renegotiation Byte Count** field, set the value to `0`.
15. In the **Version of handshake options** field, select `TLS 1.2`.
16. In the **Ciphers** field, set the value to `Default`.

    For more information, see *Administering Avaya Session Border Controller*.

17. Click **Finish**.

Configuring Avaya Aura® Session Border Controller network interfaces

About this task

Use this procedure to configure Avaya Aura® Session Border Controller network interfaces.

For detailed information about system configuration, server and network configuration, device configuration, and WebRTC-enabled call processing, see *Administering Avaya Session Border Controller*.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. In the navigation pane, click **Network & Flows** > **Network Management** > **Networks**.
4. In addition to the management interface configured during Session Border Controller installation, configure the following interfaces:
   - A1 internal interface with at least two IP addresses associated to it.
   - B1 external IP addresses with at least two IP addresses associated to it.

Configuring the Avaya Aura® Session Border Controller signaling interface

About this task

Use this procedure to configure the external and internal signaling interfaces for your deployment.

For detailed information about signaling interface configuration, see *Administering Avaya Session Border Controller*.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. To configure the external signaling interface, in the navigation pane, click **Network & Flows** > **Signaling Interface**.
4. Click **Add**.
5. In the **Name** field, enter the name for the external signaling interface (B1).
6. In the **IP Address** field, enter the network name and the IP address of the Session Border Controller used by SIP signaling messages traversing the network.

   The network name is identified by the interface name and VLAN tag.

7. Leave the **TCP Port** field blank.
8. Leave the **UDP Port** field blank for a non-tunneled mode.
9. In the **TLS Port** field, type `5061`.
10. In the **TLS Profile** field, select the previously configured TLS profile.
11. Keep the **Enable Shared Control** check box cleared.
12. Leave the **Shared Control Port** field blank.
13. Click **Finish**.
14. To configure the internal signaling interface, in the navigation pane, click **Network & Flows** > **Signaling Interface**.
15. Click **Add**.
16. In the **Name** field, enter the name for the internal signaling interface (A1).
17. In the **IP Address** field, enter the network name and the IP address of the Session Border Controller used by SIP signaling messages traversing the network.

    The network name is identified by the interface name and VLAN tag.
18. Leave the **TCP Port** field blank.
19. Leave the **UDP Port** field blank for a non-tunneled mode.
20. In the **TLS Port** field, type `5061`.
21. In the **TLS Profile** field, select the previously configured TLS profile.
22. Keep the **Enable Shared Control** check box cleared.
23. Leave the **Shared Control Port** field blank.
24. Click **Finish**.

Configuring the Avaya Aura® Session Border Controller media interface for external mobile client

About this task

Use this procedure to configure the media interface for external mobile client.

For detailed information about media tunneling, media interface, media video, and end point policy groups, see *Administering Avaya Session Border Controller*.

Before you begin

To configure the media interface, you must use the same listen IP interface that is selected for STUN/TURN. Therefore, ensure that you take a note of the listen IP interface.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. In the navigation pane, click **Network & Flows** > **Advanced Options**.
4. On the Feature Control tab, select the **Media Tunneling** check box and click **Save**.
5. Click **Add**.
6. **Configure the external media interface**: In the navigation pane, click **Network & Flows** > **Media Interface**.
7. Click **Add** or clone an existing media rule.
8. In the **Name** field, enter the name for the external media interface.
9. In the **IP Address** field, enter the B1 IP address ensuring that you:
   - Do not use this IP address for any other interface bound to port 443 (HTTP tunneling configuration).
   - Do not use VLAN tag for media tunneled interface.
10. In the **Port Range** field, enter a range such as `35000-40000`.
11. In the **TLS Profile** field, select the TLS server profile for the media interface that you created. For self-signed certificates on the client, use the TLS server profile created for the external media interface.

    If media tunneling is disabled, keep the value `None`.
12. In the **Buffer Size** field, select the buffer size from the list containing values from 400 to 1000 in KB.
13. Click **Finish**.
14. **Configure the internal media interface**: In the navigation pane, click **Network & Flows** > **Media Interface**.
15. Click **Add** or clone an existing media rule.
16. In the **Name** field, enter the name for the internal media interface.
17. In the **IP Address** field, enter the A1 IP address for media tunneling.
18. In the **Port Range** field, enter a range such as `35000-40000`.
19. In the **TLS Profile** field, select the TLS server profile for the media interface that you created. For self-signed certificates on the client, use the TLS server profile created for the internal media interface.
20. In the **Buffer Size** field, select the buffer size from the list containing values from 400 to 1000 in KB.
21. Click **Finish**.
22. **Enable video media**: In the navigation pane, click **Domain Policies** > **Application Rules**.

23. Clone an existing rule or add a new rule.
24. Enable **In/Out Audio/Video** application types.
25. Configure **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** fields.
26. **Configure media encryption and enable BFCP/FECC**: In the navigation pane, click **Domain Policies** > **Media Rules**.
27. Clone an existing rule or add a new rule.
28. On the Encryption tab, in the Miscellaneous section, select the **Capability Negotiation** check box.
29. On the Advanced tab, select the **BFCP Enabled** and **FECC Enabled** check boxes.
30. **Configure the policy group with the newly created application and media rules**: In the navigation pane, click **Domain Policies** > **End Point Policy Groups**.
31. Clone an existing policy group or add a new policy group.
32. **Disable interworking when using HTTP tunneling**: In the navigation pane, click **Domain Policies** > **Media Rules** > **Encryption**.
33. Clear the **Interworking** check box.

Configuring Avaya Aura® Session Border Controller load monitoring for external mobile access

About this task

Use this procedure to configure load monitoring for external mobile access.

For detailed information about load monitoring, see *Administering Avaya Session Border Controller*.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. In the navigation pane, click **Network & Flows** > **Load Monitoring** > **Advanced Options**.
4. Click **Add** to create a new load balancer profile.
5. In the **Load Balancer Type** field, select `INTERNAL`.

   Load Balancer on the A1 side of the network. Avaya Aura® Web Gateway does the load balancing towards the internal side. All HTTP requests sent out for dialing use the internal load balancer logic to identify the appropriate Session Border Controller.
6. In the **Transport** field, select the load balancer protocol.

7. In the **Listen IP** field, select the internal interface (A1) IP address.

   It can be a separate IP address.
8. In the **Service Type** field, select `TURN`.

Configuring Avaya Aura® Session Border Controller server flows for external mobile calls

About this task

Use this procedure to configure the server flows for external mobile calls.

For detailed information about server flows, see *Administering Avaya Session Border Controller*.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. **Create an interworking profile or update an existing profile**: In the navigation pane, click **Configuration Profiles** > **Server Interworking**.
4. Click **Add** to create a new profile.
5. For a new profile, set all options as default.
6. In the Advanced Options section, in the **Has Remote SBC** field, select `No`.
7. In the **Extensions** field, select the correct profile.

   This configuration directs the Session Border Controller security device to use the functionality specific to different environments.
8. Click **Finish**.
9. **Add a configuration for Session Manager**: In the navigation pane, click **Services** > **SIP Servers**.
10. Click **Add**.
11. In the **Server Type** field, select `Call Server`.
12. Leave the **SIP domain** field blank.
13. In the **TLS Client Profile** field, select the previously created client profile if TLS port is specified.

    Add the Session Manager IP or FQDN with port and protocol specified (TCP and/or TLS).
14. In the Advanced Options section, select the **Enable Grooming** check box, and then select the previously created interworking profile.
15. Leave the other settings with their default values.

16. Click **Finish**.
17. **Add a flow for Session Manager**: In the navigation pane, click **Network & Flows** > **End Point Flows** > **Server Flows**.
18. Click **Add**.
19. In the **Flow Name** field, enter a name such as `SM_Flow`.
20. In the **SIP Server Profile** field, select the configuration that you previously created for the SIP Server profile for Session Manager.
21. In the **Received Interface** field, select the internal interface (A1).
22. In the **Signaling Interface** field, select the internal interface (A1).
23. In the **Media Interface** field, select the internal interface (A1).
24. In the **Endpoint Policy Group** field, select the appropriate option.
25. Leave the other settings with their default values.
26. Click **Finish**.
27. **Add a configuration for the Avaya Aura® Web Gateway server**: In the navigation pane, click **Services** > **SIP Servers**.
28. Click **Add**.
29. In the **Server Type** field, select `Trunk Server`.
30. Leave the **SIP domain** field blank.
31. In the **TLS Client Profile** field, select the previously created Avaya Aura® Web Gateway client profile if TLS port is specified.

    Add the Avaya Aura® Web Gateway IP or FQDN with port and protocol specified (TCP and/or TLS). Add all cluster nodes.
32. In the Advanced Options section, select the **Enable Grooming** check box, and then select the previously created interworking profile.
33. Leave the other settings with their default values.
34. Click **Finish**.
35. **Add a flow for the Avaya Aura® Web Gateway server**: In the navigation pane, click **Network & Flows** > **End Point Flows** > **Server Flows**.
36. Click **Add**.
37. In the **Flow Name** field, enter a name such as `AAWGFlow`.
38. In the **SIP Server Profile** field, select the configuration that you previously created for Avaya Aura® Web Gateway.
39. In the **Received Interface** field, select the internal interface (A1).
40. In the **Signaling Interface** field, select the internal interface (A1).
41. In the **Media Interface** field, select the external interface (B1).

42. In the **Endpoint Policy Group** field, select the appropriate option.
43. Leave the other settings with their default values.
44. Click **Finish**.

Configuring Avaya Aura® Session Border Controller STUN TURN server for external mobile calls

About this task

Use this procedure to configure the STUN TURN server for external mobile calls.

For detailed information about WebRTC Connect-enabled call processing, see *Administering Avaya Session Border Controller*.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. In the navigation pane, click **DMZ Services** > **TURN/STUN Service** > **TURN/STUN Profiles**.
4. On the TURN/STUN Profiles tab, click **Add**.
5. In the **Profile Name** field, type an appropriate name.
6. In the **UDP Listen Port** field, type `3478`.
7. In the **Media Relay Port Range** field, type the port range.
8. Select the **Media Learning** check box only for deployments with TURN on Avaya Media Server or MCU.

   Clear this check box for TURN/STUN profile deployment on browser.
9. Click **Finish**.
10. On the TURN Relay tab, click **Add**.
11. In the **Listen IP** field, enter the Listen IP of the TURN server.

    It shows the IP that you created in the TURN/ STUN Profiles tab for the Session Border Controller device.
12. In the **Media Relay IP** field, enter the media relay IP of the TURN server.

    It shows the IP that you created in the TURN/ STUN Profiles tab for the Session Border Controller device.
13. In the **Service FQDN** field, enter the Listen FQDN of the TURN server.
14. In the **TURN/STUN Profile** field, select the TURN/STUN profile that you created.

15. Click **Finish**.

Chapter 31: Deploy Multimedia channels for remote workers

Deploy Multimedia channels for remote workers overview

Avaya Oceana® supports the remote worker functionality for Multimedia channels, such as Email, Chat, SMS, Social, Generic, and Messaging. With this functionality, remote workers who are located outside the contact center infrastructure can access Avaya Oceana® and Avaya Analytics™ applications with an Internet connection and perform agent and supervisor tasks. Remote workers can access the applications through the reverse proxy.

- This functionality requires split-horizon DNS so that on-premise and remote agents can use the same FQDNs to access Avaya Oceana®. However, the FQDNs must resolve to different IP addresses depending on whether the agent is on-premise or remote.
- This functionality utilizes the following two ports on the external firewall:
  - Port 443 for general signaling
  - Port 9443 for authorization.

  Therefore, both the ports must be open on the external firewall.
- The performance of Avaya Workspaces degrades or it becomes unresponsive on network connections with a latency of more than 300 milliseconds (ms) RTT. Therefore, external agents must have a reliable Internet connection that can deliver an RTT below 300 ms.

Prerequisites

Before implementing the configuration to support Multimedia remote workers, you must ensure the following:

- Avaya Oceana® is deployed and configured for all Multimedia channels and is operational for on-premise agents.
- Avaya Oceana® must completely use secure connections through the following:
  - The **Only allow secure web communication** check box must be selected in the cluster attributes of all Avaya Oceana® clusters.
  - The **Secure Communications** attribute must be enabled in the OceanaConfiguration service.
- A reverse proxy and external/internal firewalls are deployed and operational.

  The reverse proxy must have a support for WebSockets and HTTP version 1.1.

- Any screen-pops required for agents must be externalized so that they are accessible to the remote agents.

Checklist for deploying Multimedia channels for remote workers

Use the following checklist to deploy Multimedia channels for remote workers:

No.	Task	Description	✔
1	Document the FQDNs and IP addresses of solution interfaces.	See Documentation of FQDNs and IP addresses of solution interfaces for Multimedia remote workers on page 520.	
2	Publish the FQDNs external to the enterprise.	See Publishing of FQDNs external to the enterprise for Multimedia remote workers on page 521.	
3	Configure the external firewall for remote workers.	See Configure the external firewall for Multimedia remote workers on page 521.	
4	Configure the reverse proxy for Multimedia remote workers.	See Configure the reverse proxy for Multimedia remote workers on page 521.	
5	Configure the internal firewall for remote workers.	See Configure the internal firewall for Multimedia remote workers on page 530.	

Documentation of FQDNs and IP addresses of solution interfaces for Multimedia remote workers

To deploy the Multimedia remote worker solution, you must document FQDNs and IP addresses of Avaya Oceana® and Avaya Analytics™ interfaces that remote workers access during normal operations.

Use the following table to note down the FQDNs and IP addresses:

Component	FQDN	Internal IP address
Avaya Oceana® Cluster 1		
Avaya Oceana® Cluster 2		
Avaya Oceana® Cluster 3		
Avaya Oceana® Cluster 4		
Avaya Analytics™		

Avaya Oceana® Cluster 5 is another optional cluster. If your solution requires Avaya Oceana® Cluster 5, you can configure it similarly as you configure the other clusters.

Publishing of FQDNs external to the enterprise for Multimedia remote workers

To support the Multimedia remote worker functionality, customers must publish a DNS entry for each required Avaya Oceana® and Avaya Analytics™ FQDN that remote workers use.

When the remote worker accesses or requests a URL containing the Avaya Oceana® FQDNs, the FQDNs are resolved to a single IP, which is the external firewall Listen IP address.

Use the following table to map all internal Avaya Oceana® and Avaya Analytics™ interfaces with FQDNs. This table drives the DNS configuration.

Component	FQDN	Internal IP address	External Firewall Listener IP address
Avaya Oceana® Cluster 1			
Avaya Oceana® Cluster 2			
Avaya Oceana® Cluster 3			
Avaya Oceana® Cluster 4			
Avaya Analytics™			
Avaya Aura® Device Services			
The right column contains the external facing IP address of the enterprise firewall that connects the external remote workers to the enterprise applications inside or behind the firewall.			

Configure the external firewall for Multimedia remote workers

The external firewall receives the requests from remote agents and allows the requests to go to the reverse proxy. The external firewall receives the requests from all source addresses and ports on the HTTPS port 443.

After the reception, the requests are translated into the reverse proxy IP addresses and ports by using Network Address Translation (NAT).

The same configuration is repeated for the port 9443 to allow authorization requests for Avaya Oceana® agents.

Configure the reverse proxy for Multimedia remote workers

The reverse proxy determines which URL requests must be allowed and how the requests must flow into enterprise applications. They also determine the reverse communications to remote workers.

The reverse proxy is configured with a whitelist. Customers configure the whitelist for their deployment and it has all internal Avaya Oceana® and Avaya Analytics™ URLs that all workers require to access the contact center functionality.

The following tables shows a sample whitelist configuration:

Cluster/Server	Whitelist URL in Request	Reverse Proxy Listen IP	Listen Port	Internal Firewall Destination IP	Internal Firewall Port
Avaya Oceana® Cluster 1	/services/CustomerManagement/				
Avaya Oceana® Cluster 1	/services/OCPDataServices/				
Avaya Oceana® Cluster 1	/services/CustomerJourneyService/				
Avaya Oceana® Cluster 2	/services/UnifiedAgentController/				
Avaya Oceana® Cluster 2	/services/Broadcast-UnifiedAgentController/				
Avaya Oceana® Cluster 3	/services/AgentControllerService/				
Avaya Oceana® Cluster 3	/services/CustomerControllerService/				
Avaya Oceana® Cluster 4	/services/CoBrowse/				
Avaya Analytics™	/orca-streams-rest/ /orca-streams-data-publisher/ /AvayaAnalytics/				
Avaya Aura® Device Services	/acs/				
Avaya Aura® Device Services	/notification/				

Table continues…

Cluster/Server	Whitelist URL in Request	Reverse Proxy Listen IP	Listen Port	Internal Firewall Destination IP	Internal Firewall Port
Avaya Oceana® Cluster 2	/services/AuthorizationService				

A remote worker who requests a destination containing an internal URL in the HTTPS request, such as /services/CustomerManagement/, gets forwarded to a preconfigured IP address and port on the internal firewall for that URL. The internal firewall uses its own rule (NAT) to allow/deny this request into the final internal destination component in Avaya Oceana® and Avaya Analytics™.

Note:

For the following clusters, reverse proxy relays require you to enable WebSockets on the proxy connection:

- Avaya Oceana® Cluster 2 (UnifiedAgentController)
- Avaya Oceana® Cluster 4 (CoBrowse)
- Avaya Analytics™

Checklist for configuring a sample reverse proxy relay

Use the following checklist to configure a sample reverse proxy relay on a Pulse Secure Virtual Traffic Manager:

Important:

For this sample configuration, Virtual Traffic Manager is deployed with the following three network interfaces:

- One management interface
- One external client-side interface to communicate with the remote agents
- One internal server-side interface to communicate with the back-end servers

No.	Task	Description	✔
1	Deploy Pulse Secure Virtual Traffic Manager and verify that it is operational.	See the Pulse Secure documentation.	
2	Add a Traffic IP group.	See Adding a Traffic IP group on page 524.	
3	Add pools.	See Adding pools on page 524.	
4	Add a pool for authorization.	See Adding a pool for authorization on page 525.	
5	Create an SSL certificate for agent connections.	See Creating an SSL certificate for agent connections on page 526.	

Table continues…

No.	Task	Description	✔
6	Create a virtual server.	See Creating a virtual server on page 526.	
7	Create virtual server rules.	See Creating virtual server rules on page 527.	
8	Create a virtual server for authorization.	See Creating a virtual server for authorization on page 528.	
9	Create a virtual server authorization rule.	See Creating a virtual server authorization rule on page 529.	
10	Download and install the Pulse Secure self-signed certificate.	See Downloading and installing the Pulse Secure self-signed certificate on page 529.	

Adding a Traffic IP group

About this task

A Traffic IP group is the external client-side IP on the Virtual Traffic Manager. It receives requests from the remote agents and proxies them to the internal Avaya Oceana® servers.

Procedure

1. On the Virtual Traffic web admin interface, click **Services** > **Traffic IP Groups**.

   The interface displays the Create a new Traffic IP Group page.
2. In the **Name** field, type a name for the IP group.
3. In the **Traffic Managers** field, select your traffic manager.
4. In the **IP Addresses** field, enter the IP address that the external firewall translates (NAT) external requests to.
5. In the **IP mode** field, select `Raise each address on a single machine (Single-Hosted mode).`
6. Click **Create Traffic IP Group**.

Adding pools

About this task

A pool is a group of servers to which services can be load balanced. In this configuration, each pool is a single IP address on the internal firewall that corresponds to an Avaya Oceana® cluster/server.

Procedure

1. On the Virtual Traffic web admin interface, click **Services** > **Pools**.

   The interface displays the Create a new Pool page.
2. In the **Pool Name** field, enter a name for the pool.

3. In the **Pool Type** field, select `Static`.
4. Under Nodes, enter the unique IP address/port combination on the internal firewall of the destination cluster/server.
5. Click **Create Pool**.

   Virtual Traffic Manager creates the pool and displays the following message:

   ```
   This pool is not yet associated with a virtual server, so settings
   for all protocols are shown below.
   ```
6. Click **SSL Settings** > **SSL Encryption**.
7. In the **ssl_encrypt** field, select `Yes`.
8. Click **Update**.
9. On the **Pools** tab, click **Pools**.
10. Repeat Steps 2 to 9 for each Avaya Oceana® cluster.

    These steps also apply to Avaya Oceana® Cluster 4 for CoBrowse and Avaya Analytics™ cluster for real-time and historical reporting.

Adding a pool for authorization

About this task

For AuthorizationService, you must create a pool using port 9443.

- For Avaya Oceana® deployments that support more than 100 agents, Avaya Oceana® Cluster 2 is the authorization cluster.
- For Avaya Oceana® deployments that support up to 100 agents, Avaya Oceana® Cluster 1 is the authorization cluster.

Procedure

1. On the Virtual Traffic web admin interface, click **Services** > **Pools**.

   The interface displays the Create a new Pool page.
2. In the **Pool Name** field, enter a name for the pool.
3. In the **Pool Type** field, select `Static`.
4. Under Nodes, enter the unique IP address/port combination on the internal firewall of the destination cluster/server.
5. Click **Create Pool**.

   Virtual Traffic Manager creates the pool and displays the following message:

   ```
   This pool is not yet associated with a virtual server, so settings
   for all protocols are shown below.
   ```
6. Click **SSL Settings** > **SSL Encryption**.
7. In the **ssl_encrypt** field, select `Yes`.

8. Click **Update**.
9. On the **Pools** tab, click **Pools**.

Creating an SSL certificate for agent connections

About this task

To secure the connection between the remote agent browser and Pulse Secure Virtual Traffic Manager, you must create an SSL certificate.

Procedure

1. On the Virtual Traffic web admin interface, click **Catalogs** > **SSL Catalogs** > **SSL Server Certificates Catalog** > **Create Self-Signed Certificate / Certificate Signing Request**.

   The interface displays the Create a new Pool page.
2. In the **Name** field, enter a name for the certificate.
3. In the **Subject Alternative Name(s)** field, click the plus sign (**+**), and add the FQDN of Avaya Oceana® Cluster 1.
4. Repeat Step 3 for all server/cluster FQDNs that the remote agents use.
5. In the **Common Name (CN)** field, enter the FQDN of Avaya Oceana® Cluster 1.
6. In the remaining fields, enter the appropriate values based on your organization.
7. In the **Expires in** field, select the required validity length.
8. In the **Key type** field, select `2048 bit RSA`.
9. Click **Create certificate**.

   You can now use this self-signed certificate or follow the Pulse Secure documentation to create a CSR for the certificate, and have it signed by a trusted Certificate Authority.

Creating a virtual server

About this task

Virtual servers accept the network requests from remote clients and assign the requests to the appropriate pool, which forwards them to the designated Avaya Oceana® cluster/server.

Procedure

1. On the Virtual Traffic web admin interface, click **Services** > **Virtual Servers**.

   The interface displays the Create a new Virtual Server page.
2. In the **Name** field, enter a name for the virtual server.
3. In the **Protocol** field, select `HTTP`.
4. In the **Port** field, select `443`.
5. In the **Default Traffic pool** field, select the pool created for Avaya Oceana® Cluster 1.
6. In the Basic Settings area, select `Enabled:Yes`.

7. In the Basic Settings area, select `Listening on: Traffic IP Groups`, and select the Traffic IP group that you created.
8. Click **SSL Decryption**.
9. In the **ssl_decrypt** field, select `Yes`.
10. In the **certificate** field, select the SSL certificate created for agent connections.
11. Leave the other settings to default and click **Update**.
12. On the Virtual Server tab, click the virtual server to return to the Virtual Server configuration page.
13. Click **Protocol Settings** > **HTTP-Specific Settings** .
14. Verify that the **autodetect_upgrade_headers** field is set to `yes`.

    If this field is not set to `yes`, set it to `yes` and apply the changes.
15. On the Virtual Server tab, click the virtual server to return to the Virtual Server configuration page.

Creating virtual server rules

About this task

Use this procedure for adding rules to enable the virtual server to allocate requests to the correct pool based on the URLs on the requests.

Procedure

1. On the Virtual Traffic web admin interface, click **Services** > **Virtual Servers** > ***<Your Virtual Server>***.
2. Click **Rules**.
3. In the Request Rules area, click **Manage Rules in Catalog**.
4. In the Create new rule area, do the following:
   a. In the **Name** field, enter a name for the rule.
   b. Select **Use RuleBuilder**.
   c. Select the check box beside the **Create Rule** button to associate the rule with your virtual server.
   d. Click **Create Rule**.
5. In the navigation pane on the right, click the Conditions tab, and then click **HTTP only**.
6. Click **URL Path**.
7. In the **URL Path** field, select `starts with` and add the Avaya Oceana® Cluster 1 URL, `/services/CustomerManagement/`.
8. Repeat Steps 6 and 7 to add the following Avaya Oceana® Cluster 1 URLs:
   - `/services/OCPDataServices/`

- `/services/CustomerJourneyService/`

9. In the navigation pane on the right, click the Actions tab.
10. In the Requests Only area, click **Choose Pool**.
11. In Actions - Choose Pool, select the pool that you create for Avaya Oceana® Cluster 1.
12. Click **Update**.
13. Click **Services** > **Virtual Servers** > ***<Your Virtual Server>*** to return to the Virtual Server configuration page.
14. Repeat Steps 2 to 13 for each Avaya Oceana® cluster/server that you configure in the pool.

Creating a virtual server for authorization

About this task

Use this procedure to create another virtual server for authorization. This server accepts the network requests on port 9443 from the remote clients and forwards them to the designated Avaya Oceana® Authorization cluster.

Procedure

1. On the Virtual Traffic web admin interface, click **Services** > **Virtual Servers**.

   The interface displays the Create a new Virtual Server page.
2. In the **Name** field, enter a name for the virtual server.
3. In the **Protocol** field, select `HTTP`.
4. In the **Port** field, select `443`.
5. In the **Default Traffic pool** field, select the pool created for authorization.
6. In the Basic Settings area, select `Enabled:Yes`.
7. In the Basic Settings area, select `Listening on: Traffic IP Groups` and select the Traffic IP group that you create.
8. Click **SSL Decryption**.
9. In the **ssl_decrypt** field, select `Yes`.
10. In the **certificate** field, select the SSL certificate created for agent connections.
11. Leave the other settings to default and click **Update**.
12. On the Virtual Server tab, click the virtual server for authorization to return to the Virtual Server configuration page.
13. Click **Protocol Settings** > **HTTP-Specific Settings**.
14. Verify that the **autodetect_upgrade_headers** field is set to `yes`.

    If this field is not set to `yes`, set it to `yes` and apply the changes.

15. On the Virtual Server tab, click the virtual server for authorization to return to the Virtual Server configuration page.

Creating a virtual server authorization rule

About this task

Use this procedure for adding a rule to enable the virtual server for authorization to allocate requests to the correct pool based on the Avaya Oceana® AuthorizationService.

Procedure

1. On the Virtual Traffic web admin interface, click **Services** > **Virtual Servers** > ***<Your Virtual Server for authorization>***.
2. Click **Rules**.
3. In the Request Rules area, click **Manage Rules in Catalog**.
4. In the Create new rule area, do the following:
   a. In the **Name** field, enter a name for the rule.
   b. Select **Use RuleBuilder**.
   c. Select the check box beside the **Create Rule** button to associate the rule with your virtual server for authorization.
   d. Click **Create Rule**.
5. In the navigation pane on the right, click the Conditions tab and click **HTTP only**.
6. Click **URL Path**.
7. In the **URL Path** field, select `starts with` and add the URL for authorization, `/services/CustomerManagement/`.
8. In the navigation pane on the right, click the Actions tab.
9. In the Requests Only area, click **Choose Pool**.
10. In Actions - Choose Pool, select the pool that you create for authorization.
11. Click **Update**.
12. Click **Services** > **Virtual Servers** > ***<Your Virtual Server for authorization>*** to return to the Virtual Server configuration page.

    The Pulse Secure virtual server is now configured to proxy all external agent requests to the internal Avaya Oceana® clusters/servers.

Downloading and installing the Pulse Secure self-signed certificate

About this task

Use the following procedure to download the self-signed certificate and install it on the Windows desktop machines of agents, so that they do not encounter errors in the browser when accessing Avaya Oceana®.

Use this procedure only if you prefer to use the self-signed certificate on Pulse Secure, instead of a certificate signed by a trusted Certificate Authority.

Procedure

1. On a Chrome browser on an external Windows client, enter the following URL:

   `https://<AvayaOceanaCluster1_FQDN>/services/UnifiedAgentController/workspaces/`

   The browser displays an error stating that the connection is not private.
2. Press **F12** to open the Chrome console.
3. On the Chrome console, on the Security tab, click **View Certificate**.
4. In the Certificate dialog box, click the **Details** tab.
5. Click **Copy to File**.
6. In the Certificate Export Wizard dialog box, click **Next**.
7. Select the **Base-64 encoded X.509 (.CER)** format and click **Next**.
8. Enter a name for the certificate and click **Next**.
9. Click **Finish**.
10. Double-click the downloaded certificate and install it for the local Windows machine.

    While installing the certificates on the local Windows machine, ensure that you select **Place all certificates in the following store** and choose **Trusted Root Certification Authorities**.
11. Restart the Windows machine.

Configure the internal firewall for Multimedia remote workers

An internal firewall is the final application before the enterprise applications. On its external (WAN) side, internal firewall communicates with various IP addresses and ports allocated to Avaya Oceana® and Avaya Analytics™ servers/clusters. Using the NAT functionality and preconfigured rules, it routes all allowed requests through to Avaya Oceana® and Avaya Analytics™ servers on the internal network.

Chapter 32: Configure the sample Chat client

Configure the sample Chat client overview

This section describes how to configure an Apache web server to host a sample Chat client for Avaya Oceana®. Use the sample Chat client to test Chat contacts, attribute-based Work Assignment, and Co-browse functionality.

When using the sample Chat client for testing, you must configure certain URLs and also need to change the workflow type or attributes before opening a chat.

Agents engaged with a customer on a Chat can initiate a Co-Browsing session. To initiate a Co-Browsing session, an agent can either click on the Co-Browsing URL or generate a session key and share the key with the customer.

Important:

Chat contacts must be associated with a Route point. You must ensure that the routePointIdentifier parameter in the chatLogin method, is populated in the `webchat.js` file that is part of the sample Chat client.

Deploying the sample Chat client on an Apache HTTP server

About this task

Use this procedure to deploy the sample Chat client on an Apache HTTP server.

Note:

In the sample Chat client, all components are browser-based. Therefore, it is not necessary to deploy the sample Chat client to a server for testing. You can run the sample Chat client locally on your own computer.

Before you begin

Ensure that you download the latest software for the sample Chat client from the Avaya DevConnect portal at http://www.avaya.com/devconnect.

For information about Avaya DevConnect, see *Avaya DevConnect Program Guide* available on https://support.avaya.com.

Procedure

1. Install Apache HTTP Server 2.4.20 or later on a server and configure it so that it can communicate.
2. Copy the `war` file of the sample Chat client to the `<Apache root directory>/htdocs` folder.
3. Create a new folder for the sample Chat client in the `<Apache root directory>/htdocs` folder and name the folder as `webUI`.
4. Extract the contents of the `war` file into the `webUI` folder.

   On a Linux machine, you can run the unzip command to extract the contents. For example, **`unzip ocp-web-ui.war –d webui`**.
5. Browse to the following URL:

   `<Apache HTTP Server IP Address>``:8080/WebUI/home.html`

   The system displays the Live Chat screen.
6. You can use this sample Chat client to verify your solution configuration.

Configuring the solution URLs for testing

Before you begin

Ensure that you download the latest software for the sample Chat client from the Avaya DevConnect portal at http://www.avaya.com/devconnect.

For information about Avaya DevConnect, see *Avaya DevConnect Program Guide* available on https://support.avaya.com.

Procedure

1. Open the *`<Apache HTTP Server IP Address>`*`:8080/WebUI/home.html` page in any browser that supports WebSockets.
2. On the upper-right area of the page, click **Show configuration panel**.
3. On the Configuration dialog box, do the following to configure the URLs for chat and other services:
   a. Click the **Click here to configure URLs** option.
   b. In the **WebChat Host** field, replace the existing entry with the FQDN or IP Address of Avaya Oceana® Cluster 3.

      To use secure connections, click **Enforce Secure Connections**. If you load the page over HTTPS, this is automatically set.
   c. In the **Context Store Host** field, replace the existing entry with the FQDN or IP Address of Avaya Oceana® Cluster 1.
   d. In the **Co-Browsing Host** field, replace the existing entry with the FQDN or IP Address of Avaya Oceana® Cluster 4.

e. Click **Accept Certificates**.

f. Click **Save Configuration**.

The system permanently saves the configuration for your browser.

Note:

You can click **Reset** and reload the page to reset the configuration.

Adding custom attributes

About this task

Avaya Oceana® provides attribute-based work and resource matching capabilities. Attributes are the main basis for selecting from available resources to be assigned work, or to select waiting work to be assigned to newly available resources. When selecting a resource to be assigned to incoming work, the resource must have the desired attributes specified in the work request. When selecting a waiting work request for a newly available resource, the work request must have attributes that match those of the resource.

Add your custom attribute to ensure that Work Assignment assigns appropriate resources to your chat requests during the testing.

Before you begin

Ensure that you download the latest software for the sample Chat client from the Avaya DevConnect portal at http://www.avaya.com/devconnect.

For information about Avaya DevConnect, see *Avaya DevConnect Program Guide* available on https://support.avaya.com.

Procedure

1. Open the `home.html` page in any browser that supports WebSockets.
2. On the upper-right area of the page, click **Show configuration panel**.
3. On the Configuration dialog box, perform the following steps to add an attribute to the chat request:
   a. Click the **Click here to configure attributes** option.
   b. In the text box before the **Add** button, type the attribute that you want to add.

      For example, Services.Testing.

   c. Click **Add**.

      The system adds the attribute in the list in the Click here to configure attributes section.
4. On the Configuration panel, perform the following steps to remove an attribute from the chat request:
   a. In the Click here to configure attributes section, identify the attribute that you want to remove.

b. Click **Remove**.

5. Click **Save Configuration**.
6. If the channelAttribute does not match the server, perform the following steps to edit the HTML pages:
   a. Open the `home.html` page.
   b. Search for a select element with ID contactType.
   c. For each option under the select, change the value to include a capital letter at the start.

      For example, change "chat" to "Chat".

Note:

By default, the attributes include Location.Inhouse. If this is not required, remove it before testing. Any changes to the attributes that are made using the Configuration panel are preserved only for the browser that you are currently using. For example, if you change the attributes in Firefox, they are not applicable for Chrome. To permanently change this for deployment, edit the attributes array in the `webChatLogon.js` file.

Changing the workflow type

Before you begin

Ensure that you download the latest software for the sample Chat client from the Avaya DevConnect portal at http://www.avaya.com/devconnect.

For information about Avaya DevConnect, see *Avaya DevConnect Program Guide* available on https://support.avaya.com.

Procedure

1. Open the `home.html` page in any browser that supports WebSockets.
2. On the upper-right area of the page, click **Show configuration panel**.
3. On the Configuration dialog box, perform the following steps:
   a. Click the **Click here to configure workflow and routepoints** option.
   b. Keep the **Workflow Type** field blank.

      To meet your specific requirements, you can configure a specific Engagement Designer workflow through the Event Catalog tab in the Engagement Designer Admin Console, and specify the name of the workflow in this field.

      If you configure a specific workflow by defining the workflow type and creating suitable Engagement Designer rules, you must also create a default rule to handle all cases that do not meet the criteria.

   c. Click **Save Configuration**.

Note:

Change in the workflow type using the Configuration panel is preserved only for the browser that you are currently using. For example, if you change the workflow type in Firefox, it is not applicable for Chrome. To permanently change this for deployment, change the *workflowType* variable in the `webChat.js` file.

Downloading the root certificate from Avaya Aura® System Manager

About this task

A default root certificate can be generated when Avaya Aura® System Manager is being installed. This section covers how to download and install the default root certificate or any other CA certificate that is loaded in System Manager. System Manager uses a third-party open source application called Enterprise Java Beans Certificate Authority (EJBCA). EJBCA acts as a Certificate Authority for certificate management.

For more information about System Manager, generating the default certificate, and working with certificates, see *Administering Avaya Aura® System Manager*.

Note:

- If you are using System Manager as Certificate Authority (CA) for Avaya Oceana® and Avaya Aura® applications, then the certificate used in the following instructions is the System Manager Root Certificate or CA Certificate.
- If you are using an enterprise or third-party Certificate Authority (CA) and not System Manager as the CA, then the certificate used in the following instructions is the root certificate of the enterprise or third-party CA. The root certificate for the enterprise or third-party CA is obtained from the enterprise or third-party CA and not from System Manager. For more information, consult the enterprise or third-party CA administrator.

Procedure

1. Log in to Avaya Aura® System Manager using your credentials.
2. Navigate to **Services** > **Security** > **Certificates** > **Authority**.
3. On the EJBCA Administration page, on the left pane, click **Public Web**.

   The system displays `Welcome to the public EJBCA pages`.
4. On the public EJBCA screen, on the left pane, in the **Retrieve** section, click **Fetch CA certificates**.
5. To download the certificate, choose any of the following:
   - Download as PEM - To download the certificate `.pem` file.
   - Download to Firefox - To install the certificate in the certificate manager of Firefox browser.
   - Download to Internet Explorer - To install the certificate on a Windows machine containing Microsoft Internet Explorer, Edge, and Chrome browsers.

Installing the root certificate

Before you begin

Download the root certificate.

Procedure

1. Navigate to root certificate location.
2. Right-click the certificate file and click **Install Certificate**.
3. On the Certificate Import Wizard, select **Local Machine** and click **Next**.
4. Select **Place all certificates in the following store** and click **Browse**.
5. Click **Trusted Root Certification Authorities**.
6. Click **OK**.
7. Click **Next**.
8. Click **Finish**.

Verifying to ensure the browser accepts the certificate

Before you begin

Ensure that the certificate is installed.

Procedure

1. Open the Windows hosts file in a text editor such as Notepad.
2. Right-click the text editor and click **Run as Administrator**.
3. Add the host names of the lab to your hosts file in the following format:

   <IP Address> FQDN
4. In your web browser, browse to a known service URL.

   Microsoft Internet Explorer tries to download the JSON response. However, Firefox and Chrome display the result.
5. In your web browser, browse to the chat URL:

   `https://<AvayaOceanaCluster3_Hostname>/services/customer/chat`

   An HTTP 405 error indicates that the request used the wrong method. The error also indicates that the browser has accepted the certificate and can open a WebSocket.

Chapter 33: Configure Chat

Configure Chat overview

This section describes how to configure Chat contacts and the optional Bot and Avaya Co-Browsing Snap-in integration.

Enabling Automation Startup message overview

Avaya Oceana®, provides the ability to control sequence of sending the startup message to bot. This functionality allows you to send initial messages from SMS or Social channels to the BotConnector. For controlling and sending the initial message automatically, after the agent has joined the following two attributes are introduced:

- Toggle sending of _startup sequence: This attribute if set to true by default.
- Toggle sending of initial messages to bot: This attribute if set to false by default.

Configuring BotConnector Snap-in licenses

About this task

Use this procedure to configure the BotConnector Snap-in license in System Manager. To generate the BotConnector Snap-in license, you must obtain the primary HOST ID from System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. Click **Install License**.
3. On the Install License page, perform the following steps:
   a. Browse to the location of the BotConnector Snap-in license and select the license file.
   b. Click **Accept the License Terms & Conditions**.
   c. Click **Install**.

      The system installs the license.
4. In the navigation pane, click **Licensed Products** to view the installed license.
5. Perform the following steps to verify that the license is installed successfully:
   a. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.

b. On the Services page, verify that the **License Mode** column for the BotConnector service displays a check mark.

Deploying the sample Chat workflow

About this task

Avaya provides a sample workflow for the Chat channel. With this procedure, you can deploy the sample Chat workflow and configure the workflow attributes.

Before you begin

- Download the latest version of the sample workflow from PLDS.
- In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Designer Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. In the Import Workflow dialog box, click **Choose File**.
4. Browse to the folder containing the sample workflow, select the workflow, and click **Import**.
5. Click **Save Workflow**.
6. In the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaChatAssistedService`.

      You can provide any name for the workflow.

   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.
8. In the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

10. On the Workflows tab, verify that the OceanaChatAssistedService workflow is available in the list of deployed workflows.

    The OceanaChatAssistedService workflow includes the Bot support.

11. On the Workflows tab, select the check box for the OceanaChatAssistedService workflow and click **Attributes**.
12. In the Workflow Attributes dialog box, do the following:
    a. In the **BotEnabled** field, keep the default value `True`.

       The `True` value specifies that the workflow always attempts to get the Bot. If your solution does not have a BotConnector or you want to skip the Bot, you must manually set this value to `False`.

    b. In the **LastAgentEnabled** field, enter the value `True` to enable the last agent routing for the Chat channel.

       By default, the last agent routing is disabled.

    c. In the **MaintenanceMode**, keep the default value `False`.

       If the site is down for maintenance, you must set this attribute to `True`.

    d. In the **PoolExpansionTime** field, set the amount of time in seconds the caller receives wait treatment before the workflow sends a MatchUpdate to Work Assignment.

    e. Click **Close**.

Adding a rule to the sample Chat workflow for priority, rank, and service

About this task

When you deploy the OceanaChatAssistedService workflow, Engagement Designer creates an empty Oceana Chat Routing Service rule set. This rule set is available on the Rules tab in the Admin Console of Engagement Designer.

You can use this procedure to add rule to sample Chat workflow for priority, rank, and service attributes.

Before you begin

Deploy the sample Chat workflow.

Procedure

1. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

2. Select the **Rules** tab.
3. On the Rules tab, select the check box for the Oceana Chat Routing Service rule set and click **Edit**.

   Engagement Designer displays the Edit Rules Editor dialog box.

4. Click **Add Rule**.
5. In the **Set Rule Name** field, type a name for the rule and click the save icon.
6. Click the **Advance** check box.
7. Click **Condition**.
8. In the **Expression** field, type the attribute based condition for this rule and click **Save**. You can also use the Expression builder to configure your condition.
9. Under **Then**, click **Add More**.
10. In the **Select Variable** field, select the variable for priority, rank, and service.
11. Click **Save**.
12. Click **Done**.

Deploying the sample Transfer to Service workflow for Chat

About this task

Avaya provides a sample Transfer to Service workflow for the Chat channel. With this procedure, you can deploy the sample Transfer to Service workflow and configure the workflow attributes.

Before you begin

- Download the latest version of the sample workflow from PLDS.
- In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Designer Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. In the Import Workflow dialog box, click **Choose File**.
4. Browse to the folder containing the sample workflow, select the workflow, and click **Import**.
5. Click **Save Workflow**.
6. In the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaChatTransfer`.

      You can provide any name for the workflow.

   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.

8. In the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`
10. On the Workflows tab, verify that the OceanaChatTransfer workflow is available in the list of deployed workflows.
11. On the Workflows tab, select the check box for the OceanaChatTransfer workflow and click **Attributes**.
12. **(Optional)** In the Workflow Attributes dialog box, do the following:
    a. In the **BotEnabled** field, replace the default value `False` with the value `True` to enable Bot after Transfer to Service.

       The `False` value specifies that the workflow always attempts to skip the Bot.
    b. Click **Close**.

Configuring the sample Transfer to Service workflow for Chat

Before you begin

In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`
2. On the Workflows tab, verify that the OceanaChatTransfer workflow is available in the list of deployed workflows.
3. Click the **Routing** tab.
4. Click **Create**.
5. In the **Select event** field, click **ROUTE_CONTACT_TRANSFER**.
6. In the **Select workflows** field, select the OceanaChatTransfer workflow.

   Note:

   Ensure that you click the workflow ending with the term `Latest`. For example, OceanaChatTransfer:Latest.
7. In the **Enter rule name** field, type `ChatTransfer`.
8. Click **Add Rule**.

9. In the **Select schema attribute** field, click **RouteContactTransfer.ChannelType:string**.
10. In the **Select function** field, click **is equal to**.
11. In the **Enter value** field, type `Chat`.
12. Click **Save**.

    The system displays the newly created rule in the list of rules.

Configuring a Chat provider

About this task

Use this procedure to create a new Chat provider through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. On the Avaya Oceana Server List page, do one of the following:
   - Double-click the administered Avaya Oceana® server.
   - Select the administered Avaya Oceana® server and click **Edit**.
4. Select the **Providers** tab.
5. Click **Add**.
6. From **Type**, select **Chat**.
7. In **Name**, keep the value `OCP Chat`.
8. In **Address**, `chat`.
9. Click **Save**.
10. Restart the clusters to make the new provider available to Avaya Workspaces agents.

Creating a user to handle Chat contacts

About this task

Use this procedure to create an agent to handle Chat contacts from customers.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.

3. Select the location for your Avaya Oceana®.
4. Perform one of the following steps:
   - Click **Add**.
   - Select an existing user and click **Edit**.
5. Enter appropriate value in each of the following fields:
   a. In the **First Name (English)** field, enter the first name of the user in English.
   b. In the **Surname (English)** field, enter the surname of the user in English.
   c. In the Available applications section, select the **Avaya Oceana** check box.
   d. In the **LDAP Username** field, enter the LDAP user name of the user.

      The LDAP user name must be in the username@domain.com format. This user name is used to log on to Avaya Workspaces.
   e. In the **Username** field, enter a user name.

      In this release, the user name is the internal handle.
   f. In the **Password** field, enter a password.

      This password is used to log on to Avaya Control Manager.
   g. In the **Confirm Password** field, re-enter the password.
   h. In the **Extension** field, enter the station associated with this agent.

      This is used when logging on to Avaya Workspaces.
   i. In the **AVAYA Login** field, enter the Elite agent login ID only if the agent also supports Voice contacts. Otherwise, leave this field blank.
   j. Click **Save**.
6. Scroll to the right and select the **Avaya Oceana** tab.
7. Select the **Chat** check box.

   Important:

   To change the channel of an agent while the agent is live, the agent must be logged out and logged in again.
8. From the **Multiplicity** drop-down list, select `1`.

   The agent can process one Chat at a time.

   You can configure an agent to support multiple simultaneous channel types. For example, an agent can be configured to support both Voice and Chat. This type of agent is sometimes called a Blended Agent. The ability of an agent to handle multiple concurrent multimedia contacts is called Multiplicity.
9. Select the **Attributes** tab.
10. Move the required attributes from the **Available Attributes** list to the **Agent Attributes** list.

11. Click **Save**.

Configuring Chat for Transfer to Service

Configuring a Transfer to Service Route Point for Chat

About this task

Use this procedure to create a new Transfer to Service Route Point for Chat through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Route Points**.
2. On the Route Points List page, click **Add**.
3. To add the Transfer to Service Route Point, perform the following steps:
   a. In the **Type** field, select `Route Point`.
   b. In the **Sub Type** field, select `Transfer to Service`.
   c. In the **Name** field, enter a name for the Route Point.
   d. Click **Save**.

Creating a Transfer Target service for Chat

About this task

Use this procedure to create a Transfer Target service for Chat through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™** > **Work Assignment**.
2. Select the **Services** tab.
3. On the Services tab, click **Add**.
4. To add a Transfer Target service, perform the following steps:
   a. In the **Service Name** field, enter the name of the service.
   b. Select the **Available for Transfer** check box.

      The system automatically selects the **Agent Display** check box.
   c. Move the required attributes from the **Available Attributes** list to the **Included Attributes** list.

d. In the Transfer Routepoints section, in the **Chat** field, select the Route Point that you created for Chat.

e. Click **Save**.

Chat limits

For Chat:

- The length of a text message must be in the range of 1-2500 characters.
- The length of coaching messages, which are sent between the agent and supervisor, must be in the range of 1-2500 characters.

Configuring AgentControllerService to access UnifiedAgentController

About this task

Starting from Avaya Oceana® Release 3.8.0.0, UnifiedAgentController requires all the requests to its internal endpoints to be authenticated using the AuthorizationService token. Use this procedure to configure AgentControllerService to access UnifiedAgentController.

You can also configure AgentControllerService using the OceanaConfiguration service. For more information about the OceanaConfiguration service, see Setting OceanaConfiguration attributes on page 117.

Note:

This procedure is mandatory for Avaya Oceana® to handle contacts properly.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In **Clusters**, click Avaya Oceana® Cluster 3.
   b. In **Service**, click **AgentControllerService**.
3. For **Authorization Service Address**:
   a. Select the **Override Default** check box.
   b. In **Effective Value**, enter the IP address or FQDN of the cluster that hosts AuthorizationService.
4. Click **Commit**.

Setting the Authorization Service address to enable authorized access to Oceana transcripts

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In **Clusters**, click Avaya Oceana® Cluster 1.
   b. In **Service**, click **OCPDataServices**.
3. For **Authorization Service Address**:
   a. Select the **Override Default** check box.
   b. In **Effective Value**, enter the IP address or FQDN of the cluster that hosts AuthorizationService.
4. For **Enable Tokenless Access**:
   a. Select the **Override Default** check box.
   b. In **Effective Value**, select **false**.
5. Click **Commit**.
6. Restart Avaya Oceana® Cluster 3.

Chapter 34: Verify Chat contacts

Verify Chat contacts using Avaya Workspaces

This section describes how to use Avaya Workspaces to verify that the Avaya Oceana® is correctly configured to process Chat contacts.

Deploying Avaya Workspaces

Procedure

1. Install and commission Avaya Workspaces.

   For information about how to install and commission Avaya Workspaces, see the following documents:

   - *Using Avaya Workspaces for Avaya Oceana®*
   - *Administering Avaya Oceana®*
2. Identify the login details of an agent configured to handle Chat contacts.

Logging in to Avaya Workspaces

About this task

Use this procedure to log in to Avaya Workspaces to verify access details and agent status.

Procedure

1. Enter one of the following URLs in your web browser:
   - For an Avaya Oceana® deployment that supports up to 100 active agents, enter `https://<AvayaOceanaCluster1_FQDN>/services/UnifiedAgentController/workspaces/#/login`.
   - For an Avaya Oceana® deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, enter `https://<AvayaOceanaCluster2_FQDN>/services/UnifiedAgentController/workspaces/#/login`.
2. On the Agent Login screen, perform the following steps:
   a. In the **Username** field, enter the LDAP username of the agent as configured on the Users page on Avaya Control Manager.

Note:

- Ensure that the agent is configured through Avaya Control Manager to process Chat contacts.
- Ensure that the agent has appropriate attributes for this test contact.
- To simplify initial verification, ensure that no other agent with Chat capabilities is logged in. It ensures that the initial Chat messages are all routed to this agent.

b. In the **Password** field, enter the password of the agent.

c. Click **SIGN IN**.

3. On the Activate Agent screen, click **ACTIVATE**.
4. On the Avaya Workspaces agent interface, in the bottom right corner, verify that the agent state is `CONNECTED`.

Starting work in Avaya Workspaces

About this task

Use this procedure to configure the agent to accept incoming Chat contacts.

Procedure

1. On the Avaya Workspaces agent interface, from the agent status drop-down list, select **StartWork**.
2. In the bottom right corner, verify that the agent state changes to `READY`.

Note:

On the Avaya Workspaces agent interface, when an agent is in the `READY` state, the agent remains available for receiving interactions until the agent is occupied on all channels for which the agent is configured.

Avaya Oceana® provides the following agent states:

- `CONNECTED`: The state of agents when they log in and activate themselves in the Avaya Workspaces or when they click the **Finish Work** button. In this state, agents do not remain available for receiving interactions.
- `Ready`: The state of agents when they click the **Start Work** or **Go Ready** button. In this state, agents remain available for receiving interactions.
- `Not Ready`: The state of agents when they click the **Additional Work** or **Go Not Ready** button. In this state, agents do not remain available for receiving interactions.

If multiplicity configuration of an agent allows receiving multiple interactions on a channel, the agent remains available for receiving interactions on that channel until the maximum multiplicity is achieved.

Making a test Chat contact

About this task

Use the sample Chat client to generate a test contact.

Procedure

1. In your web browser, enter the following URL to open the sample Chat client:

   `<Apache HTTP Server IP Address>:8080/WebUI/home.html`.

2. On the upper-right area of the page, click **Show configuration panel**.
3. On the Configuration dialog box, perform the following steps:
   a. Click the **Click here to configure attributes** option.
   b. In the text box before the **Add** button, type the attribute that you want to add.

      For example, Language.English.

   c. Click **Add**.

      The system adds the attribute in the list in the Click here to configure attributes section.

   d. Click **Save Configuration**.
4. On the sample Chat client page, click **Live Chat**, enter test customer details, and click **Chat Now**.

   Note:

   If not using Bot, proceed to step 5.

   For solutions using Bot and the BotConnector service, the **Chat** section in Avaya Workspaces shows which portions of the chat are automated and which are with a real agent.

   For example, initially the BotConnector service handles the chat until the customer escalates the chat. Thereafter a real agent handles the chat session.

5. Configure the escalation phrases in Bot.

   These phrases allow a customer to request a real person instead of the BotConnector service. For example, you can configure a phrase like “Give me a real person” or “I want to escalate”.

6. When the system presents the Chat, continue to verify Chat configuration in your solution.
7. After the verification, click **Close** on the sample Chat client or close the chat using the contact card in Avaya Workspaces.
8. On the sample Chat client, ensure that the chat status is `Connection closed, chat has ended`.

Making a test Chat contact using Avaya Co-Browsing Snap-in

About this task

If your solution uses Co-Browsing Snap-in, you can verify the solution configuration by making a test Chat contact that includes a Co-Browsing session. This test uses the sample Chat client to generate a test contact and verify the Co-Browsing configuration.

Procedure

1. In your web browser, enter the following URL to open the sample Chat client:

   `<Apache HTTP Server IP Address>:8080/WebUI/home.html`.

2. On the upper-right area of the page, click **Show configuration panel**.
3. On the Configuration dialog box, perform the following steps:
   a. Click the **Click here to configure attributes** option.
   b. In the text box before the **Add** button, type the attribute that you want to add.

      For example, Language.English.

   c. Click **Add**.

      The system adds the attribute in the list in the Click here to configure attributes section.

   d. Click **Save Configuration**.
4. On the sample Chat client page, click **Live Chat**, enter test customer details, and click **Chat Now**.

   After some time, the system presents the Chat to an agent.
5. Answer the Chat.
6. To initiate a Co-Browsing session, click **Co-Browse**.

   The system displays the following options to the agent:

   - Co-Browse URL
   - Generate Co-Browse Key
7. Click one of the options to initiate the Co-Browsing session with the customer.

   The system displays the `Co-browsing session initiated` message at the customer end.

   Note:

   The system must display the same webpage to the agent.
8. To stop the Co-Browsing session, click **Stop** on the Connected to Co-Browse Session message box.

   The system displays the `Co-Browsing session finished` message.

   The Chat session continues after the Co-Browsing session is complete.

9. Continue to verify Chat contact configuration in your solution.

Chapter 35: Configure Email

Configure Email overview

This section describes how to initially configure Avaya Oceana® to support Email contacts. The chapter includes the procedures required to route Email contacts, for more information about optional tasks or how to change default configuration, see *Administering Avaya Oceana®*.

Important:

You must install and actively manage a SPAM filter to remove SPAM messages from all contact center mailboxes. If you do not filter unsolicited bulk SPAM messages in Avaya Oceana®, they can impact the performance or can cause damage to your contact center solution. Do not use the Avaya Oceana® Email Service as a SPAM filtering tool.

Avaya Oceana® Email Service does not support Email Source Routes. (RFC2821 Section C) This email format is deprecated. Configure your Email Servers to treat Source Route emails as SPAM. Do not relay Source Route emails to mailboxes monitored by the Avaya Oceana® Email Service.

Avaya Oceana® does not support incoming emails greater than 30MB in size. Ensure that the emails greater than 30MB in size are removed from your email system before Avaya Oceana® downloads the email.

Configuring an Email provider

About this task

Use this procedure to create a new Email provider through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. On the Avaya Oceana Server List page, do one of the following:
   - Double-click the administered Avaya Oceana® server.
   - Select the administered Avaya Oceana® server and click **Edit**.
4. Select the **Providers** tab.

5. Click **Add**.
6. From **Type**, select `Email`.
7. In **Name**, keep the value `OCP Email`.
8. In **Address**, enter `email`.
9. Click **Save**.
10. Restart the clusters to make the new provider available to Avaya Workspaces agents.

Configuring an Email Route Point

About this task

Use this procedure to create a new Email Route Point for Email contacts through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Route Points**.
2. On the Route Points List page, click **Add**.
3. To add the Email Route Point, perform the following steps:
   a. In the **Name** field, enter a Route Point name.
   b. Click **Save**.

Configuring Email server certificates

About this task

You must configure email server certificates because EmailServers requires certs to authenticate access applicable to TLS email connections. You can configure certificates for both on-premise and Microsoft Office 365 servers.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select the check box for one of the nodes of Avaya Oceana® Cluster 3, and click **More Actions** > **Manage Trusted Certificates**.
3. On the Manage Trusted Certificates page, click **Add**.
4. On the Add Trusted Certificate page, perform the following steps:
   a. Click **Import using TLS**.
   b. In **IP Address**, enter the IP address of your Email server.

c. In **Port**, enter the secure port number `443`.

d. Click **Retrieve Certificate**.

e. Click **Commit**.

5. Repeat Step 2 to Step 4 for the other node of Avaya Oceana® Cluster 3.
6. Click **Done**.

Configuring an Email server and mailboxes

About this task

Use this procedure to configure an Email server and mailboxes for Avaya Oceana®.

Avaya Oceana® supports the following authentication methods for IMAP and SMTP:

- PLAIN
- LOGIN

Both methods require Base64 encoding.

Procedure

1. Refer to Microsoft Exchange or other third-party Email server documentation for details.

   Important:

   - Ensure that IMAP/POP3/SMTP ports are open.
   - Ensure that you use the default Email domain since the non-default Email domains are not supported.

2. Configure an Email client that you can use to generate test Email messages.

Configuring the maximum number of days to retain active email contacts

About this task

Configure the maximum number of days that Engagement Designer (ED) and Work Assignment can retain active email contacts.

The default ED timeout value is 3 days. The default Work Assignment timeout value is 604800000 milliseconds, equivalent to 7 days. You can configure both of these values to retain active email contacts for a longer period. Avaya recommends configuring these timeout values to the same number of days. The maximum value for both is 24 days.

Snap-in	Attribute	Default value	Maximum value	Comment
EngagementDesigner	Number of days the user wants to retain active instances	3	24	Default value

Table continues…

Snap-in	Attribute	Default value	Maximum value	Comment
WorkAssignmentManagerService	IMPU WorkItem Queued state for Email timeout (value)	604800000 (7 days)	2073600000 (24 days) if in milliseconds, 100 if in days	2073600000 = (24 days) = (24 * 24 * 60 * 60 * 1000 * 1 ms)
WorkAssignmentManagerService	IMPU WorkItem Queued state for Email timeout time unit	Milliseconds	N/A	Select milliseconds or days from the drop-down list

Note:

The maximum number of queued email contacts that Avaya Oceana® supports is a fixed limit. If you extend the maximum number of days that ED and Work Assignment can retain active email contacts, the maximum number of queued emails limit can be reached before the increased retention time expires. For more information about the supported maximum number of queued email contacts, see Capacity specifications on page 46.

Procedure

1. Log on to the System Manager web console.
2. Click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
3. On the Service Clusters tab, from the **Cluster** list, select Avaya Oceana® Cluster 1.
4. From the **Service** list, select **EngagementDesigner**.
5. From the list of DEFAULT_GROUP attributes, select the **Number of days the user want to retain active instances** attribute.
6. Select **Override Default**.
7. Type the maximum number of days to retain active ED workflow instances.

   The maximum is 24 days.
8. Click **Commit**.
9. On the Service Clusters tab, from the **Cluster** list, select Avaya Oceana® Cluster 1.
10. From the **Service** list, select **WorkAssignmentManagerService**.
11. From the list of IMPU Configuration attributes, select the **IMPU WorkItem Queued state for Email timeout time unit** attribute.
12. Select **Override Default**.
13. From the list, select the time unit (milliseconds or days) in which to set the maximum timeout to retain active Work Assignment Email WorkItems.
14. From the list of IMPU Configuration attributes, select the **IMPU WorkItem Queued state for Email timeout (value)** attribute.
15. Select **Override Default**.

16. Type the maximum number of time units to retain active Work Assignment Email WorkItems.

    The maximum time is 2073600000 (24 days) if you use milliseconds or 100 if you use days.

    For more information about the attributes, see WorkAssignmentManagerService attributes on page 711.
17. Click **Commit**.
18. Reboot Avaya Oceana® Cluster 1.

Configuring an Outbound SMTP server

About this task

The Outbound SMTP server delivers the Email messages sent from the contact center.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **General Administration**.
3. Click **Server Settings**.
4. Click **New**.
5. From the list, select **Outbound SMTP Server**.
6. Enter the details of your Outbound Email server.
7. Click **Save**.

Configuring an Inbound Mail server

About this task

Add an Email server for your contact center to poll multiple Email servers for the Email messages to route to agents. The Inbound Mail server handles Email messages coming into the contact center.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **General Administration**.
3. Click **Server Settings**.
4. Click **New**.
5. From the list, select **Inbound Mail Server**.
6. Enter the details of your Inbound Email server.
7. Click **Save**.

Configuring keyword groups

About this task

You must assign at least one keyword to a keyword group before you can save the keyword group. The keyword search in an email message is not case sensitive. For example, if you add the word `John`, the Email Manager also matches `JOHN` and `john`. The **Keyword** field supports the Unicode UTF-8 character set.

You can specify a spelling accuracy in the keyword group. Keyword groups support only asterisks (*) and question marks (?) as wildcard characters. The asterisk (*) represents multiple characters. For example, t* specifies a list of all the words that start with t. The question mark (?) represents a single character. For example, p?t specifies all three letter words that start with p and end with t.

A keyword does not support the following characters: +-!(){}[]^"~:\&&||#$@€/><,.‘;=%£&¬|`‟. If you use any of these characters in your keywords, you receive an error message stating that the keyword contains invalid characters.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **Keyword Groups**.
4. Perform one of the following steps:
   - Click **New**.
   - Select an existing keyword group and click **Edit**.
5. In the Keyword Group section, perform the following steps:
   a. In the **Group Name** field, enter a unique name for the keyword group.
   b. In the **Keyword** field, enter a word or a group of words related to the keyword group.
   c. Select the **Allow spelling inaccuracies** check box to allow close misspellings of the word.

   The system displays the following levels of accuracy:
   - Low (greater than 70% accuracy)
   - Medium (greater than 80% accuracy)
   - High (greater than 90% accuracy)
6. Select the required level of accuracy.
7. Click **>**.

   The system moves the keyword or expression to the Keywords in Group section.
8. Click **Save**.

Configuring an automatic response

About this task

Use this procedure to create automatic responses. You can also add images for auto-responses.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **Prepared Responses**.
4. Perform the following steps:
    a. Click **New Response**.
    b. In **Name**, enter a name for the response.
    c. In **Type**, select **Auto-Response - Regular** or **Auto-Response - Out of Hours**.
    d. In **Subject**, enter the appropriate subject.
    e. In **Body**, enter the appropriate text.
    f. To add an image for auto-response, click the **Image** ( ) icon and select the required image.
    g. Click **Save**.

Configuring an automatic suggestion response

About this task

Use this procedure to configure an automatic suggestion response.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **Prepared Responses**.
4. Perform the following steps:
    a. Click **New Response**.
    b. In the **Name** field, enter a name for the response.
    c. In the **Type** field, select **Auto-Suggest**.
    d. In the **Subject** field, enter the appropriate subject.
    e. In the **Body** field, enter the appropriate text.
    f. Click **Save**.

Configuring Email inboxes

About this task

Create a recipient Email box to ensure that at least one Email inbox is configured for your Contact Center. You must configure one recipient to commission the server.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **Recipient Addresses**.
4. Click **New**.
5. In the **Mailbox Type** field, select from:
   - `Mail Store` - Select this option to configure the following:
     - A distribution group address for the **From** header of each email that goes out from the Avaya Oceana® mailbox.
     - A specific percentage of outbound reply emails.
     - Outgoing emails to be approved prior to being sent out.

     For details on configuring the Mail Store, see Mail Store field descriptions on page 559.
   - `Alias` - Select this option to create another name for the recipient email box. For details on configuring Alias, see Alias field descriptions on page 561.
   - `Distribution group` - Select this option to create a new email distribution list. For details on configuring Distribution group, see Distribution group field descriptions on page 562.
6. Enter the required information.
7. Click **Save**.

Mail Store field descriptions

Use the Mail Store option to:

- Configure a distribution group address for the **From** header of each email that goes out from the Avaya Oceana® mailbox. All outgoing emails from the agents are configured with the email address of the distribution group, instead of the actual mailbox from which the emails are sent.
- Configure the outgoing emails to be approved prior to being sent out to a customer.
- Configure a specific percentage of outbound reply emails from agents to go through an approval process.

Name	Description
Mailbox	Local-part (username) of mailbox email address.

Table continues…

Name	Description
Domain	Domain name of the mailbox email address.
Display Name	The name that appear in the Email From address.
Inbound Server	The host name of configured Inbound Server along with the respective security protocol.
Inbound Mail Threshold	The maximum number of Email messages to be retrieved from the mailbox every scan interval. You can enter a different value for this variable for each mailbox.
Outbound (SMTP) Server	The host name of configured Outbound Server.
% of mail to send to approval	The specific percentage of outbound reply emails from agents can be set to go through an approval process.
Approval for Fowards	To enable email approval process for email forwards, that is, if incoming emails are targeted for approval for individual mail box.
Credentials	Credentials to be used to access chosen mail servers.
Rule Group	The name of the Rule Group to be applied on the email messages received from the current Mail Store.
Agent Initiated Email	Sets the mailbox to allow an agent to initiate an Ad-Hoc email (emails that are initiated by agents without an incoming email from customer). **Note:** When the **Agent Initiated Email** option is selected for a mailbox, any email-enabled Avaya Oceana® agent can send out an email from that mailbox. The outbound email comes from that mailbox, and not from the agent.
Allow Multireply	To enable the multireply feature for individual mail boxes.

Table continues…

Name	Description
Send as group	Sets the distribution group address for each outgoing email sent from the current mailbox. The text box next to the check box displays the email address of the distribution group that is used for outgoing emails. All the outbound emails sent from this Mail Store have a group address as the sender address. **Note:** The **Send as group** option is available for authorized SMTP access and when the mailbox is a member of the Avaya Oceana® distribution group.
Shared	Select this option if the mailbox on the mail server is configured as shared. . **Note:** If a mail server is configured as a shared server, all the configuration is done on mail server side, you must only provide access information (shared username in addition to mailbox info).
Username	The shared user name of the account used to connect to the mailbox.

Alias field descriptions

Use Alias option to create another name for the recipient email box.

For example, the mailbox general@magscripts.com can have the aliases carz@magsubscriptions.com and planez@magsubscriptions.com. Email messages addressed to either alias are forwarded to the general@magscripts.com mailbox. The Email Service routes the email messages according to the rules from the Rule Group assigned to the alias.

Field Name	Description
Mailbox	Local-part (username) of mailbox email address.
Domain	Domain name of the mailbox email address.
Display Name	The name that appear in the Email From address.
Rule Group	The name of the Rule Group to be applied on the email messages received from the current Mail Store.
Outbound (SMTP) Server	The host name of configured Outbound Server.
Username	The user name used to access the mailbox on mail server.

Table continues…

Field Name	Description
Password	The password for the mailbox. **Important:** When you change a password on the Email server, you must update the password in this field.
Confirm Password	Confirmation of the password entered for the mailbox in **Password** field.
Agent Initiated Email	Sets the mailbox to allow an agent to initiate an Ad-Hoc email (emails that are initiated by agents without an incoming email from customer). **Note:** When the **Agent Initiated Email** option is selected for a mailbox, any email-enabled Avaya Oceana® agent can send out an email from that mailbox. The outbound email comes from that mailbox, and not from the agent.
Credentials	The credential used to access the mailbox on the MS Graph mail server. **Note:** OAuth2.0 credentials are available for the MS Graph SMTP server only and cannot be used with other SMTP servers.

Distribution group field descriptions

Use the Distribution group option to create a new email distribution list.

Name	Description
Mailbox	The group email address.
Available	Displays the list of members available.
Configured	Enables you to assign members to the distribution group by selecting from the Available list to the Configured list. **Note:** The Distribution group type is used only if you want to use Send as group feature.

Handling email contact with Send as Group option enabled

With the **Send as group** option enabled, administrators can configure distribution group address. This address is set to the **From** header of each email that goes out from the Avaya Oceana® mailbox. All outgoing emails from the agents are configured with the email address of the distribution group, instead of the actual mailbox from which the emails are sent.

The EmailService sends emails from an actual mailbox configured. However, EmailService checks if the **Send as group** option is configured for that mailbox. If the **Send as group** option is enabled, the distribution group address is set as the From address for the email.

This is applicable for all the outgoing email, including Ad-hoc emails, forwarded emails, and auto-replies sent from the mailbox for which the **Send as group** is configured.

Note:

The **Send as group** feature is supported only for Microsoft Office365 email provider.

Example

- A customer sends a new email from customer@mydomain.com to OceanaGroup@avaya.com, which is an email distribution group.

  Distribution group address is configured in the mail server and Avaya Oceana® as Distribution group mailbox type.
- Email server receives a new email and places in each mailbox in the distribution group.
- Avaya Oceana® polls a new email from OceanaMailbox@avaya.com mailbox and passes it to the agent.

  OceanaMailbox@avaya.com mailbox is configured in Avaya Oceana® for email polling.
- Agent writes a response to customer@mydomain.com.
- Avaya Oceana® EmailService receives a new outbound email to process, checks database configuration for mailbox OceanaMailbox@avaya.com, and sets an appropriate sender address, OceanaGroup@avaya.com, for a new email message.
- The customer receives a new email from OceanaGroup@avaya.com email address.

Configuring in Microsoft Office 365 administration portal

About this task

You must use Microsoft Office 365 administration portal to add Avaya Oceana® mailbox as a member with the permission to send as a group. Avaya Oceana® uses the mailbox configured to poll new emails.

Procedure

1. Go to admin.microsoft.com.
2. Log on to the Office 365 Administration portal with tenant administrator credentials.
3. Go to **Users**.
4. In the **Active users** tab, create a new Office365 mailbox.

   Avaya Oceana® uses the Office 365 mailbox to poll new emails.
5. Go to **Groups** > **Groups**.
6. Click **Add a group** to create a new distribution list.
7. Click the newly created distribution list.
8. Go to **Members** and add the Office 365 mailbox that was created in step 4 to the distribution list.

You can also add mailbox from Exchange admin center. Do the following:

a. Go to **Admin centers** > **Exchange**.
b. Go to **Recipients** > **Groups** and select the newly created distribution list.
c. Click **Edit**.
d. Go to **Group delegation** and add the mailbox in **Send As** section to give a permission to send as a group.

9. Click **Save** to save the changes.

Configuring rule groups

About this task

Use this procedure to create or change a rule to route your email contacts.

You can create a rule with one or more of the following routing options:

- Determine when the email was received (Office Hours)
- Determine who sent the email (Sender Groups)
- Determine the specific characters, words, or phrases in the email (Keyword Groups)

Rules can send an automatic response to a customer. Therefore no agent interaction is required.

A rule group contains a default rule for routing an email contact to a specific route point with a priority.

Before you begin

Configure an automatic response and an automatic suggestion response.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **Rule Groups**.
4. Perform one of the following steps:
   - Click **New**.
   - Select an existing Rule Group and click **Edit**.
5. In the Rules section, perform one of the following steps:
   - Click the plus sign **(+)** button.
   - Select an existing rule.
6. In the Current Search Criteria section, click **New**.
7. To add search criteria based on the keyword match, perform the following steps:
   a. In the Add New Criterion section, select **Keyword Match** and click **Go**.

b. In the Keyword Groups section, select the first keyword group and click **>** in the first row.

c. In the Keyword Groups section, select the second keyword group and click **>** in the second row.

d. Select the **AND** or **AND NOT** options to associate the second keyword group with the first keyword group.

e. In the Keyword Groups section, select the third keyword group and click **>** in the third row.

f. Select the **AND** or **AND NOT** options to associate the third keyword group with the first and second keyword groups.

g. Click **OK**.

Note:

The total keyword match weightage must add up to 100 percent.

8. To add search criteria based on the sender group, perform the following steps:

a. In the Add New Criterion section, select **Sender Group** and click **Go**.

b. In the Sender Groups section, select the required sender group and click **>**.

c. Click **OK**.

Note:

The total keyword match weightage must add up to 100 percent.

9. In the Current Search Criteria Summary section, click the rule name to view the details of each criteria that you configure.
10. Click **Next**.
11. In the Available Auto-Responses section, select a configured automatic response for the rule and click **>**.
12. In the Available Auto-Suggests section, select a configured automatic suggestion for the rule and click **>**.

    To remove an automatic suggestion for the rule, click **<**.
13. Click **Next**.
14. Perform the following steps based on your requirement:

- Select the **Will use Office Hours** check box to apply the Office Hours to the email message.
- Select the **Respond to original email** check box and select the appropriate recipient Email inbox.
- Select the **Will Close Contact** check box to close the contact.
- Select the **Call Open Interface web service** check box and select the Web service associated with the rule.

15. Keep the **WorkFlow** field blank.
16. **(Optional)** To configure different Engagement Designer workflows to meet your specific requirements, perform the following steps:
    a. In the Engagement Designer Admin Console, select the Event Catalog tab.
    b. Select the required workflow and click **Edit**.
    c. In the Event Catalog dialog box, click **Rules Editor**.
    d. In the Edit Rule dialog box, set the criteria for the required workflow based on the WorkflowType value.

    Note:

    You must also create a default rule to handle all cases that do not meet the criteria.
17. Click **Next**.
18. In the General Settings section, perform the following steps:
    a. In the **Name** field, enter a name for the rule.
    b. In the **Priority** field, select the priority to assign to the contact.
    c. In the **Routepoint** field, select the Route Point name to apply for the rule. You must select the Email Route Point that you configured using Avaya Control Manager.

    Important:

    You must configure a Route Point when creating rule groups.
    d. In the **CS Lease Time** field, enter the appropriate value.
    e. In the **Disclaimer** field, enter the appropriate text.
    f. In the **Profanity Profile** field, select the required profanity profile.

    Note:

    The profanity validation is not applicable if no profile is set. You can also unset profanity profile from Rule by choosing the empty option in the drop-down list of profanity profiles.
19. In the content pane, select the attributes.

    For example, Language.English.
20. In the Approval Settings section, perform the following steps:
    a. In the **Priority** field, select the priority to assign to the contact.
    b. In the **% of mail to send to approval:** field, set the value for the percentage of emails to be sent through the approval process.
21. In the content pane, select the Approval attributes for this rule.

If the approval ratio, that is, the percentage of emails to be marked for approval is greater than zero, you must select at least one approval attribute from the Approval category to be saved on the rule.

For example, Approval.Email.

22. Click **Save**.

    The configured inbox approval ratio may not directly correspond to the percentage of the email being sent through the approval process as the approval ratio converges to the percentage set based on sufficient traffic through the system.

    An email approval ratio is also set on the Inbox in the **Recipient Addresses** configuration section. If the rule approval ratio and the inbox approval ratio differ, the higher value between the two is the effective value. For more information about email approval ratios, see Email approval ratios on page 578.

Configuring system default rule

About this task

Administrators can configure default behavior if the contacts do not match any rules. When you create a recipient mailbox, the system default rule is copied as the last regular rule into the list of rules for the recipient mailbox.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **System Rules**.
4. In the System Default Rule section, in the **Routepoint** field, select the route point name to apply for the rule.

   You must select the Email Route Point that you configured using Avaya Control Manager.
5. To change the automatic response settings, in the **Auto-Responses** list, select the required response.

   An automatic response is a message sent to a customer without an agent's interaction.
6. In the **Priority** list, select the priority for the contact.
7. In the right pane, select the attributes.

   For example, Language.English.

   If you cannot close an email, you can route it to the agent attribute set that is configured in the **Edit Attributes** section.
8. Click **Save**.

Configuring system delivery failure rule

About this task

You can configure system delivery failure rule to ensure that any email message that contains particular phrases such as undeliverable, returned mail, unknown recipient, delivery failure, or delivery report is deleted and not assigned to an agent. When you create a recipient mailbox, the system delivery failure rule is copied as the first regular rule into the list of rules for the recipient mailbox.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **System Rules**.
4. In **System Delivery Failure Rule** section, in the **Routepoint** field, select a route point name to apply for the rule.

   You must select the Email Route Point that you configured using Avaya Control Manager.
5. To change the keyword group, in the **Keyword Group** list, select the keyword that you can search in an email message.
6. In the **Priority** list, select the priority for the contact.
7. In the right pane, select the attributes.

   For example, Language.English.

   If you cannot close an email, you can route it to agent attribute set that is configured in the **Edit Attributes** section.
8. Select the **Will close contact** check box to have the rule to close the contact.
9. Click **Save**.

Configuring email settings

About this task

You can configure email settings for email messages entering your mailboxes for:

- how frequently you scan the email server for new messages.
- the location in which attachments are stored.
- automatic numbering of email messages.
- text search result for the keywords used for rules.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **General Settings**.

4. In the **Message Properties** section, do the following:
   - In the **AutoNumber outgoing E-mail** field, select the **Customer ID** check box or **Contact ID** check box or both.

     Select the check box to number the email message automatically with either the customer ID, the contact ID, or both. The number appears in the subject of the message for identification. You can optionally add customer ID or contact ID, or both to the outgoing emails. This helps customers to track emails.
   - Select the **Include E-mail body in keyword search** check box to enable a keyword search in the body of the email message.
   - In the **Search first characters** field, type the number of characters in the content of the body of the email message that you search for keywords.
5. In the **Attachment** section, in the **Maximum outbound attachment size** field, type the size of the email. This indicates the maximum size of outbound email allowed in Avaya Oceana®, including the email attachments.
6. In the **Mailbox** section, do the following:
   a. In the **Scan Interval** field, type the time in minutes. This indicates the interval at which the mailbox scans for new incoming email messages from the email servers.
   b. In the **Max active Emails** field, type the number of active emails.

      Active emails are the maximum number of emails in the mailbox that are not closed. After the mailbox reaches this limit, you cannot read any email messages from the mail servers until the current number of emails drop below this limit. Avaya Oceana® supports up to 25000 active emails.

      Important:

      - To support 25000 emails in queue, you must increase the **Platform Space Container Heap Size (MB)** attribute value on the Common Cluster to `600`.
      - To support a maximum of 25000 active emails, you must also configure specific ContextStoreManager attributes.

      For more information on queued emails, see the note on Queued emails in the *Capacity specifications* topic of *Deploying Avaya Oceana®*.
7. Click **Save**.

Configuring Email Templates

Email Templates are predefined responses that Avaya Workspaces agents or supervisors can use when replying to customer emails.

For information about how to configure Email Templates, see *Using Avaya Control Manager to Administer Avaya Products*.

Blacklisting email addresses and domains

About this task

Use this procedure to blacklist the email addresses and domains from which the system must not receive emails.

Important:

For filtering of Inbound emails for potential risks, you must use a third-party software.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail** > **Sender Groups**.
3. Click **New**.
4. In the Sender Group section, perform the following steps:
   a. In the **Name** field, enter a name.

      For example, `Blacklist Group`.

   b. In the **E-mail Address** field, enter the email address or domain that you want to blacklist and click **Add Freeform**.

      You can repeat this step to add more email addresses or domains that you want to blacklist.

      Note:

      Sender groups support asterisks (*) as wildcard characters when they are placed in the email address.

   c. Click **Save**.
5. In the navigation pane, click **Rule Groups**.
6. Select an existing Rule Group and click **Edit**.
7. In Rules section, click the plus sign (**+**) button.
8. In New Rule section, click **New**.
9. In the **Add New Criterion** field, select **Sender Group** and click **Go**.
10. In the Sender Groups section, select the Sender Group that you created and click **>**.
11. Click **OK**.
12. Click **Next**.
13. Click **Next**.
14. Select the **Will Close Contact** check box.
15. Click **Next**.
16. Click **Save**.

Note:

You can also blacklist emails based on keywords in the subject and body of the emails by creating a keyword group and assigning the keyword group to a rule.

Deploying the sample Email workflow

About this task

Avaya provides a sample workflow for the Email channel. With this procedure, you can deploy the sample Email workflow and configure the workflow attributes.

Before you begin

- Download the latest version of the sample workflow from PLDS.
- In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Designer Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. In the Import Workflow dialog box, click **Choose File**.
4. Browse to the folder containing the sample workflow, select the workflow, and click **Import**.
5. Click **Save Workflow**.
6. In the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaEmailAssistedService`.

      You can provide any name for the workflow.

   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.
8. Repeat Steps 2 to 7 for `OceanaEmailResumeService`.
9. In the Deployment Details dialog box, click **OK**.
10. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

    `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

11. On the Workflows tab, verify that the OceanaEmailAssistedService and the OceanaEmailResumeService workflows are available in the list of deployed workflows.

12. On the Workflows tab, select the check box for the OceanaEmailAssistedService workflow and click **Attributes**.
13. In the Workflow Attributes dialog box, do the following:
    a. In the **LastAgentEnabled** field, enter the value `True` to enable the last agent routing for the Email channel.

       By default, the last agent routing is disabled.
    b. Click **Close**.

Deploying the sample Transfer to Service workflow for Email

About this task

Avaya provides a sample Transfer to Service workflow for the Email channel. With this procedure, you can deploy the sample Transfer to Service workflow.

Before you begin

- Download the latest version of the sample workflow from PLDS.
- In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Designer Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`
2. Click **Import**.
3. In the Import Workflow dialog box, click **Choose File**.
4. Browse to the folder containing the sample workflow, select the workflow, and click **Import**.
5. Click **Save Workflow**.
6. In the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaEmailTransfer`.

      You can provide any name for the workflow.
   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.
8. In the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

`https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

10. On the Workflows tab, verify that the OceanaEmailTransfer workflow is available in the list of deployed workflows.

Configuring the sample Transfer to Service workflow for Email

Before you begin

In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

2. On the Workflows tab, verify that the OceanaEmailTransfer workflow is available in the list of deployed workflows.
3. Click the **Routing** tab.
4. Click **Create**.
5. In the **Select event** field, click **ROUTE_CONTACT_TRANSFER**.
6. In the **Select workflows** field, select the OceanaEmailTransfer workflow.

   Note:

   Ensure that you click the workflow ending with the term `Latest`. For example, OceanaEmailTransfer:Latest.

7. In the **Enter rule name** field, type `EmailTransfer`.
8. Click **Add Rule**.
9. In the **Select schema attribute** field, click **RouteContactTransfer.ChannelType:string**.
10. In the **Select function** field, click **is equal to**.
11. In the **Enter value** field, type `Email`.
12. Click **Save**.

    The system displays the newly created rule in the list of rules.

Resume email flow

There are three different email flows in Avaya Oceana®:

- *OceanaEmailAssistedService.xml*

- *OceanaEmailResumeService.xml*
- *OceanaEmailTransfer.xml*

The *OceanaEmailResumeService.xml* controls the resumption of the contacts that have been deferred by agents. So when the deferred timer expires or the agents initiates retrieval of the contact, this ED flow operates and controls the flow of the retrieved email contact.

Creating a user to handle Email contacts

About this task

Use this procedure to create an agent to handle Email contacts from customers.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.

   Users are listed by Location. Select the location for your Avaya Oceana®.
3. Perform one of the following steps:
   - Click **Add**.
   - Select an existing user and click **Edit**.
4. Enter appropriate value in each of the following fields:
   a. In the **First Name (English)** field, enter the first name of the user in English.
   b. In the **Surname (English)** field, enter the surname of the user in English.
   c. In the Available applications section, select the **Avaya Oceana** check box.
   d. In the **LDAP Username** field, enter the LDAP user name of the user.

      The LDAP user name must be in the username@domain.com format. This user name is used to log on to Avaya Workspaces.
   e. In the **Username** field, enter a user name.

      In this release, the user name is the internal handle.
   f. In the **Password** field, enter a password.

      This password is used to log on to Avaya Control Manager.
   g. In the **Confirm Password** field, re-enter the password.
   h. In the **Extension** field, enter the station associated with this agent.

      This is used when logging on to Avaya Workspaces.
   i. In the **AVAYA Login** field, enter the Elite agent login ID only if the agent also supports Voice contacts. Otherwise, leave this field blank.

j. Click **Save**.

5. Scroll to the right and select the **Avaya Oceana** tab.
6. Select the **Email** check box.

   Important:

   To change the channel of an agent while the agent is live, the agent must be logged out and logged in again.

7. From the **Multiplicity** drop-down list, select the maximum of concurrent Email contacts.

   The ability of an agent to handle multiple concurrent multimedia contacts is called Multiplicity.

8. Select the **Attributes** tab.
9. Move the attributes from the **Available Attributes** list to the **Agent Attributes** list.

   Important:

   You must move the same attributes that you configured in the Omnichannel Administration Utility for the Email to be routed to your agent.

10. Click **Save**.

Configuring Email for Transfer to Service

Configuring a Transfer to Service Route Point for Email

About this task

Use this procedure to create a new Transfer to Service Route Point for Email through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Route Points**.
2. On the Route Points List page, click **Add**.
3. To add the Transfer to Service Route Point, perform the following steps:
   a. In the **Type** field, select `Route Point`.
   b. In the **Sub Type** field, select `Transfer to Service`.
   c. In the **Name** field, enter a name for the Route Point.
   d. Click **Save**.

Creating a Transfer Target service for Email

About this task

Use this procedure to create a Transfer Target service for Email through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™** > **Work Assignment**.
2. Select the **Services** tab.
3. On the Services tab, click **Add**.
4. To add a Transfer Target service, perform the following steps:
   a. In the **Service Name** field, enter the name of the service.
   b. Select the **Available for Transfer** check box.

      The system automatically selects the **Agent Display** check box.
   c. Move the required attributes from the **Available Attributes** list to the **Included Attributes** list.
   d. In the Transfer Routepoints section, in the **Email** field, select the Route Point that you created for Email.
   e. Click **Save**.

Outbound email approval

Use the following process flow to understand and configure the outbound email approval process.

No.	Tasks	Description	✔
1	Outbound email approval process overview.	See Outbound email approval process on page 577.	
2	Configure rejection codes.	See Configuring rejection codes on page 577.	
3	Configure approval attributes.	See Illustration of the approval attribute configuration for outbound emails on page 577.	
4	Configure inbound rule for assigning the approval attributes.	See Configuring rule groups on page 564.	
5	Configure percentage of mails routed for approval.	See Configuring percentage of mails going for approval on page 578.	
6	Email approval ratios.	See Email approval ratios on page 578	

Table continues…

No.	Tasks	Description	✔
7	Approval process of an outgoing email reply from the agent to the customer.	See “Approving outbound emails from agents to the customer” in the *Using Avaya Workspaces for Avaya Oceana®* document.	

Outbound email approval process

In Avaya Oceana®, you can configure emails for approval before sending them to a customer. For example, an individual or a group of designated approvers can approve emails. Approving emails is part of quality assurance to ensure the agents respond appropriately to customer queries.

Agents can send approved emails to the customer, which appear in the customer journey. Unapproved emails do not show up in the customer journey, and administrators can use the audit trail to see these emails.

You can use Avaya Analytics™ to view real-time and historical reporting on approving or rejecting outbound emails.

Configuring rejection codes

About this task

When an approver rejects emails, mandatory rejection reason codes must be assigned to the contacts. Administrators can create rejection reason codes.

Procedure

1. Log on to Avaya Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana** > **Reason Codes**.
3. Click the **Rejection Codes** tab.
4. Click **Add**.
5. In the **Name** field, enter a name for the rejection reason code.
6. In the **Number** field, enter a unique number for the rejection reason code.
7. In the **Contact Type** field, **Email** is selected by default.
8. Click **Save**.

Illustration of the approval attribute configuration for outbound emails

This section describes an example approval attribute configuration for a service.

Consider the following Work Assignment service **EnglishSalesEmail**.

Service Name	Service Attributes
EnglishSalesEmail	*Language.English* *Department.Sales* *Channel.Email*

To send an email associated with this service through the approval service, there is flexibility to configure the system. One approach is to create a new approval attribute, to represent the service.

In Avaya Control Manager, you must create a new Approval attribute for this service with a descriptive name, *Approval.EnglishSalesApproval*. Assign *Approval.EnglishSalesApproval* as the only approval attribute in OCP Administration. See Configuring rule groups on page 564.

Assign *Approval.EnglishSalesApproval* attribute to the agents or supervisors to be assigned as approvers, for the emails routed through this service.

Configuring percentage of mails going for approval

About this task

A specific percentage of outbound reply emails from agents can be set to go through an approval process. You can configure the approval percentage at a mailbox level or at a rule group level.

Use the following procedure to enable outbound reply emails approval for a mailbox, and set a percentage of mails to be sent for approval.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **Recipient Addresses**.
4. Click the mailbox for enabling approval.
5. In the **% of mail to send to approval:** field, set the value for percentage of mails to be marked for approval.
6. Click **Save**.

Important:

The configured inbox approval ratio may not directly correspond to the percentage of email being sent through the approval process as the approval ratio converge to the percentage set based on sufficient traffic through the system. All the email rules applied to email for the inbox must also be configured with the approval attributes, else some emails do not get sent for approval. See Configuring rule groups on page 564.

An email approval ratio is also set on inbound email rules, and if the rule approval ratio and the inbox approval ratio differ, then the higher value between the two values is the effective value. For more information on email approval ratios, see Email approval ratios on page 578.

Email approval ratios

An email approval ratio can be set on both the mail inbox and the mail's inbound mail rules. This introduces possible ambiguity on which approval ratio is the effective one. The higher of the two values is always taken as the effective approval ratio. For example, if a mail arrives through a mailbox where the approval ratio is 50%, and on a rule where the approval ratio is 0%, then the

effective email approval ratio for that mail is 50%. That is 50% of mail arriving through that mailbox and rule is marked for approval.

Examples:

Email arriving on Inbox	Inbox approval ratio	Rule approval ratio	Effective approval ratio
A	100%	0%	100% 100% of such email are subject to approval.
B	10%	50%	50%
C	0%	90%	90%

Configuring AgentControllerService to access UnifiedAgentController

About this task

Starting from Avaya Oceana® Release 3.8.0.0, UnifiedAgentController requires all the requests to its internal endpoints to be authenticated using the AuthorizationService token. Use this procedure to configure AgentControllerService to access UnifiedAgentController.

You can also configure AgentControllerService using the OceanaConfiguration service. For more information about the OceanaConfiguration service, see Setting OceanaConfiguration attributes on page 117.

Note:

This procedure is mandatory for Avaya Oceana® to handle contacts properly.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In **Clusters**, click Avaya Oceana® Cluster 3.
   b. In **Service**, click **AgentControllerService**.
3. For **Authorization Service Address**:
   a. Select the **Override Default** check box.
   b. In **Effective Value**, enter the IP address or FQDN of the cluster that hosts AuthorizationService.
4. Click **Commit**.

Creating or editing Authorization grants for the UnifiedAgentController service

About this task

Use this procedure to create or edit Authorization grants for the UnifiedAgentController service whenever you set the **Enable Tokenless Access** attribute in OCPDataServices set to `false`.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Authorization**.
2. On the Authorization Configuration page, on the Clients tab, do the following:
   a. Select **UnifiedAgentController**.
   b. Click **Edit Grants**.
3. To edit an existing OCPDataServices resource, do the following:
   a. On the Edit Grants for Authorization Client page, select **OCPDataServices** and click **Edit Values**.
   b. On the Edit Grant Values of Authorization Client page, select the **read** and **write** check boxes.
4. To create a new OCPDataServices resource, do the following:
   a. On the Edit Grants for Authorization Client page, click **New**.
   b. In the **Resource Name** field, select **OCPDataServices**.
   c. In the **Resource Cluster** field, select the cluster that hosts OCPDataServices.
   d. In the **Feature** field, select **access**.
   e. In the **Values** field, select the **read** and **write** check boxes.
5. Click **Commit**.

Setting the Authorization Service address to enable authorized access to Oceana transcripts

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In **Clusters**, click Avaya Oceana® Cluster 1.
   b. In **Service**, click **OCPDataServices**.
3. For **Authorization Service Address**:
   a. Select the **Override Default** check box.

b. In **Effective Value**, enter the IP address or FQDN of the cluster that hosts AuthorizationService.

4. For **Enable Tokenless Access**:
   a. Select the **Override Default** check box.
   b. In **Effective Value**, select **false**.
5. Click **Commit**.
6. Restart Avaya Oceana® Cluster 3.

Conversation Transcripts through Email

Avaya Oceana® introduces sending Conversation Transcripts through Email feature that allows web messenger users to get the transcript of the conversation through email after the session.

Configuration

For the conversation transcripts to be sent, the *oceana_intrinsic_send_transcript_email* attribute must be set to `true` and the *oceana_intrinsic_email* attribute must be configured with the correct email address.

Operation

The transcript is sent to the email address of the contact if it is specified and adheres to the email address format. The transcript is sent through the Oceana Email Service. You must specify the sender address and subject. Files shared during the conversation are sent in the transcript to the users. However rich media such as locations and carousels have only the alternate text included.

Scenario	Operation
Flag to send transcript is set to `true`	The value is passed to the Avaya Oceana® Adapter service. This sets the flag to `true` in the Messaging Channel API connectAsyncSession method. For all other cases, including non web messenger originated contacts, the flag is set to `false`.
Flag is not set	It is assumed that the transcript is not required and the Avaya Oceana® Adapter service sets the connectAsyncSession transcript flag value to `false`.
Flag is set to `true` but email address provided is invalid	Where the email address is invalid, the Avaya Oceana® Adapter service sets the connectAsyncSession transcript flag to `false`.

Limitations

The feature is applicable for web messenger conversations only. Transcripts from social messaging, for example, Facebook Messenger, WhatsApp are not sent. Rich media is sent in the transcript as the alternate text. Actual carousels are not sent in the transcript.

Chapter 36: Verify Email contacts

Verify Email contacts using Avaya Workspaces

This section describes how to use Avaya Workspaces to verify that the Avaya Oceana® is correctly configured to process Email contacts.

Deploying Avaya Workspaces

Procedure

1. Install and commission Avaya Workspaces.

   For information about how to install and commission Avaya Workspaces, see the following documents:

   - *Using Avaya Workspaces for Avaya Oceana®*
   - *Administering Avaya Oceana®*
2. Identify the login details of an agent configured to handle Email contacts.

Logging in to Avaya Workspaces

About this task

Use this procedure to log in to Avaya Workspaces to verify access details and agent status.

Procedure

1. Enter one of the following URLs in your web browser:
   - For an Avaya Oceana® deployment that supports up to 100 active agents, enter `https://<AvayaOceanaCluster1_FQDN>/services/UnifiedAgentController/workspaces/#/login`.
   - For an Avaya Oceana® deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, enter `https://<AvayaOceanaCluster2_FQDN>/services/UnifiedAgentController/workspaces/#/login`.
2. On the Agent Login screen, perform the following steps:
   a. In the **Username** field, enter the LDAP username of the agent as configured on the Users page on Avaya Control Manager.

Note:

- Ensure that the agent is configured through Avaya Control Manager to process Email contacts.
- Ensure that the agent has appropriate attributes for this test contact.
- To simplify initial verification, ensure that no other agent with Email capabilities is logged in. It ensures that the initial Email messages are all routed to this agent.
- If the **Enable Tokenless Access** attribute in OCPDataServices is set to false, ensure that you create or edit Authorization grants for the UnifiedAgentController service.

b. In the **Password** field, enter the password of the agent.

c. Click **SIGN IN**.

3. On the Activate Agent screen, click **ACTIVATE**.
4. On the Avaya Workspaces agent interface, in the bottom right corner, verify that the agent state is `CONNECTED`.

Starting work in Avaya Workspaces

About this task

Use this procedure to configure the agent to accept incoming customer email messages.

Procedure

1. On the Avaya Workspaces agent interface, from the agent status drop-down list, select **StartWork**.
2. In the bottom right corner, verify that the agent state changes to `READY`.

Note:

On the Avaya Workspaces agent interface, when an agent is in the `READY` state, the agent remains available for receiving interactions until the agent is occupied on all channels for which the agent is configured.

Avaya Oceana® provides the following agent states:

- `CONNECTED`: The state of agents when they log in and activate themselves in the Avaya Workspaces or when they click the **Finish Work** button. In this state, agents do not remain available for receiving interactions.
- `Ready`: The state of agents when they click the **Start Work** or **Go Ready** button. In this state, agents remain available for receiving interactions.
- `Not Ready`: The state of agents when they click the **Additional Work** or **Go Not Ready** button. In this state, agents do not remain available for receiving interactions.

If multiplicity configuration of an agent allows receiving multiple interactions on a channel, the agent remains available for receiving interactions on that channel until the maximum multiplicity is achieved.

Verifying Email contact routing to agents

About this task

Use this procedure to verify that the email contacts are routed to available agents.

Procedure

1. Create a rest email using an Email application.
2. In the **Subject** field, enter one of the keywords configured in the Omnichannel Administration Utility.

   For example, `sales`.

   In the Omnichannel Administration Utility, keywords are configured in the **E-mail** > **Keyword Groups** section.
3. In the **To** field, enter one of the email addresses configured in the Omnichannel Administration Utility.

   In the Omnichannel Administration Utility, email addresses are configured in the **E-mail** > **Recipient Addresses** section.
4. In Email Body, type a test message.
5. Click **Send**.
6. After some time, the system presents the email to a ready agent.
7. Answer the email message.
8. Verify that the message details are correct.
9. Reply to the message.
10. Continue to verify Email contact configuration in your solution.

Chapter 37: Configure SMS

Configure SMS overview

This section describes how to initially configure Avaya Oceana® to support Short Message Service (SMS) contacts. The chapter includes the procedures required to route SMS contacts, for more information about optional tasks or how to change default configuration, see *Administering Avaya Oceana®*.

Avaya provides the following two options:

- ZangSmsConnector Snap-in: To support Inbound and Outbound messaging through Avaya Oceana®.
- SMSVendorSnapin: To test SMS functionality without having to use a physical handset. SMSVendorSnapin uses the same REST messages that any third-party uses. It does not use live SMS traffic. It simulates sending new messages in to the Contact Center and logs the responses instead of sending them to customer numbers.

Prerequisites for ZangSmsConnector Snap-in

Prerequisite	Description
An account with **SMS portal**.	For information about how to create an account, go to For information about how to create a Zang account, see https://zang.io/products/cloud/messaging. For information about how to create a CPaaS account, see https://www.avaya.com/en/products/cpaas/.
An SMS capable number in the required region.	Purchase an SMS capable number from the **SMS Portal** account, and configure the number in the OCP administration tool and set it as a default sender number.

Using CPaaS portal

About this task

To receive incoming messages using ZangSMSConnector, you must include the SMS Request Url for your phone number on the **SMS Portal** dashboard.

Procedure

1. Log on to **CPaaS SMS** Portal.
   a. For CPaaS US Portal:https://us.cpaas.avayacloud.com

b. For CPaaS EU Portal: https://eu.cpaas.avayacloud.com

2. Click **Numbers** > **My Numbers**.
3. Click the **SMS** configuration.
4. In the **SMS Request Url** field, enter the sms request url for your phone number.

   This URL must be in the following format:

   a. For CPaaS US Portal: https://pubsub-us.cpaas.avayacloud.com/<AccountSID>/SMS/Incoming

   b. For CPaaS EU Portal: https://pubsub-eu.cpaas.avayacloud.com/<AccountSID>/SMS/Incoming

   Where <Account SID> is the Account SID displayed for the SMS account on the CPaaS Portal Dashboard.

   Note:

   It is applicable for Avaya CPaaS and Zang SMS services only and not applicable for any other 3rd party SMS services

Using Zang portal

Procedure

1. Log on to https://cloud.zang.io or zang.io (old zang portal).
2. Click **Numbers** > **My Numbers**.If you are using old zang portal then **Click** > **Manage Numbers**.
3. Click the **SMS** configuration.If you are using old zang portal then Click **SMS** tab.
4. In the **SMS Request Url** field, enter the sms request url for your phone number.

   This URL must be in the following format:

   https://pubsub.zang.io /<AccountSID>/SMS/Incoming.Where <Account SID> is the Account SID displayed for the SMS account on the Zang SMS Portal Dashboard.

   Note:

   It is applicable for Avaya CPaaS and Zang SMS services only and not applicable for any other 3rd party SMS services.

Configuring an SMS provider

About this task

Use this procedure to create a new SMS provider through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. On the Avaya Oceana Server List page, do one of the following:
   - Double-click the administered Avaya Oceana® server.
   - Select the administered Avaya Oceana® server and click **Edit**.
4. Select the **Providers** tab.
5. Click **Add**.
6. In the **Type** field, select **SMS**.
7. In the **Name** field, keep the value `OCP ShortMessageService`.
8. In the **Address** field, enter `sms`.
9. In the **Auto Answer Timer (sec)** field, enter the time in seconds after which the interaction must be answered automatically.
10. Click **Save**.
11. Restart the clusters to make the new provider available to Avaya Workspaces agents.

Configuring SMS Gateway

About this task

This gateway ties accounts to a snap-in. The snap-in also uses this gateway when querying for account details.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **SMS/Social**.
3. Click **SMS Configuration**.
4. Click **Create**.
5. On the Account tab, perform the following steps:
   a. In the Create Snapin section, in the **Name** field, enter the same name that you configured for SMS in the **Messaging Snapin Key** attribute of MessagingService or **Snap-in Key** attribute of the OceanaConfiguration service.
   b. Click **Create**.
   c. In the **Snapin** field, select the snap-in that you created.
   d. Enter appropriate values in the remaining fields.

      The following table provides a description of each field:

Field	Description
Name	An account name - Sent back to third-party snap-in when they request their gateways.
API ID	An API ID - Sent back to third-party snap-in when they request their gateways.
API URL	An API URL - Sent back to third-party snap-in when they request their gateways.
API Password	An API Password - Sent back to third-party snap-in when they request their gateways.
Extra1	An extra field - Sent back to third-party snap-in when they request their gateways.
Extra2	An extra field - Sent back to third-party snap-in when they request their gateways.
Snapin	The name of the third-party snap-in you want to link it to. Enter the name created in earlier steps.

6. Click **Save**.
7. Select the **Details** tab.
8. Create an entry for the gateway that you just added.
9. Enter appropriate values in the remaining fields.

   The following table provides a description of each field:

Field	Description
Phone Number	A unique telephone number - Sent back to third-party snap-in when they request their gateways. The phone number is used later when sending a SMS through the sample vendor application.
Tag	A TAG to send messages with - Currently not used - One Off SMS Scenario.
Workflow	An Engagement Designer workflow - If none is supplied, the default flow is used. Used for routing SMS chats. Keep this field blank. To meet your specific requirements, you can configure a specific Engagement Designer workflow through the Event Catalog tab in the Engagement Designer Admin Console, and specify the name of the workflow in this field. If you configure a specific workflow by defining the workflow type and creating suitable Engagement Designer rules, you must also create a default rule to handle all cases that do not meet the criteria.
Description	A description of what to use the number for - Currently not used - One Off SMS Scenario.
Extra1	An extra field - Sent back to third-party snap-in when they request their gateways.
Gateway Account	The gateway account to link the telephone to.

Table continues…

Field	Description
Routepoint	Select a Route Point that you configured using Avaya Control Manager. Route Points are used to route SMS chats. **Important:** You must select a Route Point when configuring the SMS Gateway.
Priority	The priority from 1 to 100.
Attributes	Routing attributes of the telephone number. Used for routing SMS chats.

10. Review your configuration details.
11. In the Edit Attributes section, select the attributes which you want the incoming SMS messages to be routed.

    For example, select `Language.English`.
12. Click **Save**.

Loading and installing the ZangSmsConnector or SMSVendorSnapin SVAR

About this task

Use this procedure to load the ZangSmsConnector or SMSVendorSnapin SVAR in System Manager and install it to Avaya Oceana® Cluster 3.

When you load ZangSmsConnector Snap-in in System Manager for the first time, System Manager displays a message related to a certificate installation and system restart. You must ignore the message and proceed with the installation.

Important:

The SMSVendorSnapin service is only for testing purposes. Therefore, do not use this service in your production environment.

Before you begin

- Remove the older version of the SVAR.
- Download the latest version of the SVAR from PLDS.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. On the Services page, click **Load**.
3. In the Load Service dialog box, perform the following steps:
   a. Click **Browse**.
   b. Select the SVAR and click **Open**.

c. Click **Load**.

4. In the Accept End User License Agreement dialog box, click **Accept**.
5. On the Services page, verify that the state of the SVAR is `Loaded`.
6. On the Services page, select the check box for the SVAR and click **Install**.
7. In the Confirm install service: ZangSmsConnector or SMSVendorSnapin dialog box, select the check box for Avaya Oceana® Cluster 3 and click **Commit**.
8. On the Services page, verify that the state of the SVAR is `Installing`.

   The state changes to `Installed` when the installation is complete.
9. Set ZangSmsConnector Snap-in or SMSVendorSnapin attributes.

Installation of Certificate on SMGR for SMS Portals

Use the following procedure to retrieve and install the snap-in certificates if the certificates are not installed automatically or are cleared by some other process.

Note:

While installing ZangSMSConnector, snap-in certificates for HTTPS connections to SMS portals are automatically installed.

You must configure or install trusted certificates for your outgoing HTTPS proxy on the enterprise network.

Downloading certificates for CPaaS SMS Portal

Procedure

1. Log on to **CPaaS SMS** Portal.
   a. For CPaaS US Portal:https://us.cpaas.avayacloud.com
   b. For CPaaS EU Portal: https://eu.cpaas.avayacloud.com
2. Download the **GlobalSign Root CA** certificate from the portal.

   Note:

   Currently, US and EU require the same certificate, which can change for the upcoming release.

Downloading certificates for Zang SMS Portal

Procedure

1. Log on to https://cloud.zang.io or zang.io (old zang portal).
2. Download the **Baltimore CyberTrust Root** certificate from the portal.

Installing certificates on System Manager

Procedure

1. On System Manager, click **Elements** > Avaya Breeze® platform > **Cluster Administration**.

2. Select the cluster where the ZangSMSConnector Snap-in is installed.
3. Click **Certificate Management** > **Install Trust Certificate** (All Avaya Breeze® platform instances).
4. From the **Select Store Type to install trusted certificate** menu, select **WebSphere**.
5. Click **Browse** and navigate to the location of your certificate.
6. Click **Retrieve Certificate** and review the details of the Trusted Certificate.
7. Click **Commit**.
8. Repeat the above steps to retrieve and commit all trusted certificates one by one.

Setting ZangSmsConnector Snap-in or SMSVendorSnapin attributes

About this task

Use this procedure to configure the attributes of the ZangSmsConnector snap-in or SMSVendorSnapin service to simulate and test SMS contacts.

Important:

The SMSVendorSnapin service is only for testing purposes. Therefore, do not use this service in your production environment.

Before you begin

Install the ZangSmsConnector or SMSVendorSnapin SVAR on Avaya Oceana® Cluster 3.

Important:

For more than 100-Agent deployments, install the ZangSmsConnector on Avaya Oceana® Cluster 5.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In the **Cluster** field, select Avaya Oceana® Cluster 3.
   b. In the **Service** field, select either **ZangSmsConnector** or **SMSVendorSnapin**.
3. Set ZangSmsConnector or SMSVendorSnapin attributes.
4. Click **Commit**.
5. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
6. Select the `ZangSmsConnector` service check box.
7. Click **Stop** to stop the service.

8. Click **Start** to start the service.

SMSVendorSnapin attributes

Name	Description
Oceana Messaging Service IP or FQDN	The FQDN or IP address of the cluster that hosts MessagingService.
Oceana Messaging Service key	The name of the snap-in that you provide while configuring the SMS gateway. The same name is configured for SMS in the **Messaging Snapin Key** attribute of MessagingService or **Snap-in Key** attribute of the OceanaConfiguration service.
Oceana Messaging Service name	The name of the MessagingService snap-in. **Note:** This is not an account gateway name.
Message expiration timer	The time, in minutes, for which a message exists in SMSVendorSnapin. After the specified time, the message is automatically removed. This time is applicable for inbound and outbound messages. The value of this attribute must be a between 0 and 500. To permanently store the messages in SMSVendorSnapin, set the value of this attribute to 0.

Verifying the SMSVendorSnapin deployment

About this task

Use this procedure to verify the deployment of the SMSVendorSnapin service.

Important:

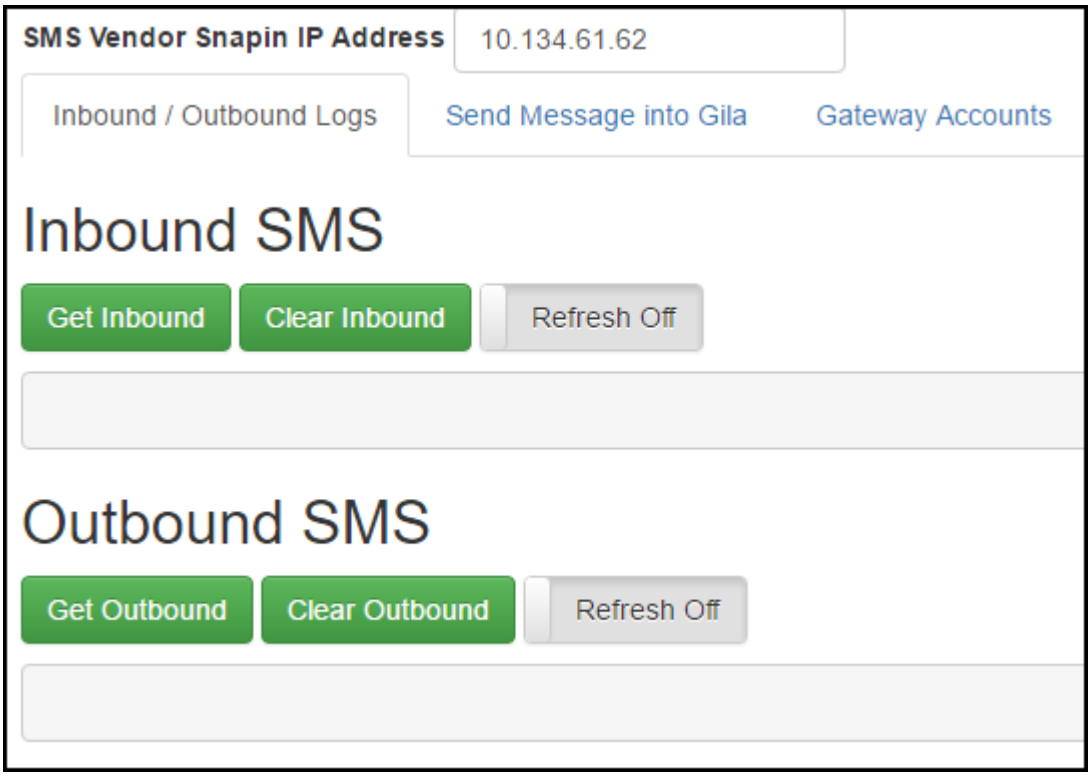
The SMSVendorSnapin service is only for testing purposes. Therefore, do not use this service in your production environment.

Procedure

1. In your web browser, enter the following URL:

   `https://<AvayaOceanaCluster3_FQDN>/services/SMSVendorSnapin/SMSTest.html`

2. Verify that the system displays the following screen:



Verifying the ZangSmsConnector Snap-in

About this task

Use this procedure to verify the deployment of the ZangSmsConnector Snap-in.

Procedure

In your web browser, enter the following URL:

`https://<AvayaOceanaCluster3_FQDN>/services/ZangSmsConnector/api/health`

The browser displays the following message:

```
{"msg": "ZangSMSConnector is running and Active" }
```

Deploying the sample SMS workflow

About this task

Avaya provides a sample workflow for the SMS channel. With this procedure, you can deploy the sample SMS workflow and configure the workflow attributes.

Before you begin

- Download the latest version of the sample workflow from PLDS.

- In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Designer Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. In the Import Workflow dialog box, click **Choose File**.
4. Browse to the folder containing the sample workflow, select the workflow, and click **Import**.
5. Click **Save Workflow**.
6. In the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaSMSAssistedService`.

      You can provide any name for the workflow.

   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.
8. In the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

10. On the Workflows tab, verify that the OceanaSMSAssistedService workflow is available in the list of deployed workflows.
11. On the Workflows tab, select the check box for the OceanaSMSAssistedService workflow and click **Attributes**.
12. In the Workflow Attributes dialog box, do the following:
    a. In the **BotEnabled** field, keep the default value `True`.

       The `True` value specifies that the workflow always attempts to get the Bot. If your solution does not have a BotConnector or you want to skip the Bot, you must manually set this value to `False`.

    b. In the **LastAgentEnabled** field, enter the value `True` to enable the last agent routing for the SMS channel.

       By default, the last agent routing is disabled.

c. Click **Close**.

Deploying the sample Transfer to Service workflow for SMS

About this task

Avaya provides a sample Transfer to Service workflow for the SMS channel. With this procedure, you can deploy the sample Transfer to Service workflow and configure the workflow attributes.

Before you begin

- Download the latest version of the sample workflow from PLDS.
- In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Designer Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. In the Import Workflow dialog box, click **Choose File**.
4. Browse to the folder containing the sample workflow, select the workflow, and click **Import**.
5. Click **Save Workflow**.
6. In the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaSMSTransfer`.

      You can provide any name for the workflow.

   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.
8. In the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

10. On the Workflows tab, verify that the OceanaSMSTransfer workflow is available in the list of deployed workflows.
11. On the Workflows tab, select the check box for the OceanaSMSTransfer workflow and click **Attributes**.

12. **(Optional)** In the Workflow Attributes dialog box, do the following:
    a. In the **BotEnabled** field, replace the default value `False` with the value `True` to enable Bot after Transfer to Service.

       The default value `False` specifies that the workflow always tries to skip the Bot.

    b. Click **Close**.

Configuring the sample Transfer to Service workflow for SMS

Before you begin

In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`
2. On the Workflows tab, verify that the OceanaSMSTransfer workflow is available in the list of deployed workflows.
3. Click the **Routing** tab.
4. Click **Create**.
5. In the **Select event** field, click **ROUTE_CONTACT_TRANSFER**.
6. In the **Select workflows** field, select the OceanaSMSTransfer workflow.

   Note:

   Ensure that you click the workflow ending with the term `Latest`. For example, OceanaSMSTransfer:Latest.
7. In the **Enter rule name** field, type `SMSTransfer`.
8. Click **Add Rule**.
9. In the **Select schema attribute** field, click **RouteContactTransfer.ChannelType:string**.
10. In the **Select function** field, click **is equal to**.
11. In the **Enter value** field, type `ShortMessageService`.
12. Click **Save**.

    The system displays the newly created rule in the list of rules.

Configuring the maximum number of days to retain active SMS contacts

About this task

Configure the maximum number of days that Engagement Designer (ED) and Work Assignment can retain active SMS contacts.

The default ED timeout value is 3 days. The default Work Assignment timeout value is 604800000 milliseconds, equivalent to 7 days. You can configure both of these values to retain active SMS contacts for a longer period. Avaya recommends configuring these timeout values to the same number of days. The maximum value for both is 24 days.

Snap-in	Attribute	Default value	Maximum value	Comment
EngagementDesigner	Number of days the user want to retain active instances	3	24	Default value
WorkAssignmentManagerService	IMPU WorkItem Queued state for SMS timeout in milliseconds	604800000 (7 days)	2073600000 (24 days)	2073600000 = (24 days) = (24 * 24 * 60 * 60 * 1000 * 1 ms)

Note:

The maximum number of queued SMS contacts supported by Avaya Oceana® is a fixed limit. If you extend the maximum number of days that ED and Work Assignment can retain active SMS contacts, the maximum number of queued SMS limit can be reached before the increased retention time expires. For more information about the supported maximum number of queued SMS contacts, see Capacity specifications on page 46.

Procedure

1. Log on to the System Manager web console.
2. Click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
3. On the Service Clusters tab, from the **Cluster** list, select Avaya Oceana® Cluster 1.
4. From the **Service** list, select **EngagementDesigner**.
5. From the list of DEFAULT_GROUP attributes, navigate to the to the **Number of days the user want to retain active instances** attribute.
6. Select **Override Default**.
7. Type the maximum number of days to retain active ED workflow instances. The maximum time is 24 days.
8. Click **Commit**.
9. On the Service Clusters tab, from the **Cluster** list, select Avaya Oceana® Cluster 1.
10. From the **Service** list, select **WorkAssignmentManagerService**.

11. From the list of IMPU Configuration attributes, navigate to the **IMPU WorkItem Queued state for SMS timeout in milliseconds** attribute.
12. Select **Override Default**.
13. Type the maximum number of milliseconds to retain active SMS contacts. The maximum time is 2073600000 ms (24 days).

    For more information, see WorkAssignmentManagerService attributes on page 711.
14. Click **Commit**.
15. Reboot Avaya Oceana® Cluster 1.

Creating a user to handle SMS contacts

About this task

Use this procedure to create an agent to handle SMS contacts from customers.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.
3. Select the location for your Avaya Oceana®.
4. Perform one of the following steps:
   - Click **Add**.
   - Select an existing user and click **Edit**.
5. Enter appropriate value in each of the following fields:
   a. In the **First Name (English)** field, enter the first name of the user in English.
   b. In the **Surname (English)** field, enter the surname of the user in English.
   c. In the Available applications section, select the **Avaya Oceana** check box.
   d. In the **LDAP Username** field, enter the LDAP user name of the user.

      The LDAP user name must be in the username@domain.com format. This user name is used to log on to Avaya Workspaces.
   e. In the **Username** field, enter a user name.

      In this release, the user name is the internal handle.
   f. In the **Password** field, enter a password.

      This password is used to log on to Avaya Control Manager.
   g. In the **Confirm Password** field, re-enter the password.

h. In the **Extension** field, enter the station associated with this agent.

This is used when logging on to Avaya Workspaces.

i. In the **AVAYA Login** field, enter the Elite agent login ID only if the agent also supports Voice contacts. Otherwise, leave this field blank.

j. Click **Save**.

6. Scroll to the right and select the **Avaya Oceana** tab.
7. Select the **SMS** check box.

Important:

To change the channel of an agent while the agent is live, the agent must be logged out and logged in again.

8. From the **Multiplicity** drop-down list, select the maximum of concurrent SMS contacts.

The ability of an agent to handle multiple concurrent multimedia contacts is called Multiplicity.

9. Select the **Attributes** tab.
10. Move the attributes from the **Available Attributes** list to the **Agent Attributes** list.

Important:

You must move the same attributes that you configured in the Omnichannel Administration Utility for the SMS to be routed to your agent.

11. Click **Save**.

Configuring SMS for Transfer to Service

Configuring a Transfer to Service Route Point for SMS

About this task

Use this procedure to create a new Transfer to Service Route Point for SMS through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Route Points**.
2. On the Route Points List page, click **Add**.
3. To add the Transfer to Service Route Point, perform the following steps:
   a. In the **Type** field, select `Route Point`.
   b. In the **Sub Type** field, select `Transfer to Service`.

c. In the **Name** field, enter a name for the Route Point.

d. Click **Save**.

Creating a Transfer Target service for SMS

About this task

Use this procedure to create a Transfer Target service for SMS through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™** > **Work Assignment**.
2. Select the **Services** tab.
3. On the Services tab, click **Add**.
4. To add a Transfer Target service, perform the following steps:
   a. In the **Service Name** field, enter the name of the service.
   b. Select the **Available for Transfer** check box.

      The system automatically selects the **Agent Display** check box.
   c. Move the required attributes from the **Available Attributes** list to the **Included Attributes** list.
   d. In the Transfer Routepoints section, in the **SMS** field, select the Route Point that you created for SMS.
   e. Click **Save**.

SMS limits

For SMS, the length of coaching messages, which are sent between the agent and supervisor, must be in the range of 1-2500 characters.

Configuring AgentControllerService to access UnifiedAgentController

About this task

Starting from Avaya Oceana® Release 3.8.0.0, UnifiedAgentController requires all the requests to its internal endpoints to be authenticated using the AuthorizationService token. Use this procedure to configure AgentControllerService to access UnifiedAgentController.

You can also configure AgentControllerService using the OceanaConfiguration service. For more information about the OceanaConfiguration service, see Setting OceanaConfiguration attributes on page 117.

Note:

This procedure is mandatory for Avaya Oceana® to handle contacts properly.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In **Clusters**, click Avaya Oceana® Cluster 3.
   b. In **Service**, click **AgentControllerService**.
3. For **Authorization Service Address**:
   a. Select the **Override Default** check box.
   b. In **Effective Value**, enter the IP address or FQDN of the cluster that hosts AuthorizationService.
4. Click **Commit**.

Setting the Authorization Service address to enable authorized access to Oceana transcripts

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In **Clusters**, click Avaya Oceana® Cluster 1.
   b. In **Service**, click **OCPDataServices**.
3. For **Authorization Service Address**:
   a. Select the **Override Default** check box.
   b. In **Effective Value**, enter the IP address or FQDN of the cluster that hosts AuthorizationService.
4. For **Enable Tokenless Access**:
   a. Select the **Override Default** check box.
   b. In **Effective Value**, select **false**.
5. Click **Commit**.
6. Restart Avaya Oceana® Cluster 3.

Chapter 38: Verify SMS contacts

Verify SMS contacts using Avaya Workspaces

This section describes how to use Avaya Workspaces to verify that the Avaya Oceana® is correctly configured to process SMS contacts.

Deploying Avaya Workspaces

Procedure

1. Install and commission Avaya Workspaces.

   For information about how to install and commission Avaya Workspaces, see the following documents:

   - *Using Avaya Workspaces for Avaya Oceana®*
   - *Administering Avaya Oceana®*
2. Identify the login details of an agent configured to handle SMS contacts.

Logging in to Avaya Workspaces

About this task

Use this procedure to log in to Avaya Workspaces to verify access details and agent status.

Procedure

1. Enter one of the following URLs in your web browser:
   - For an Avaya Oceana® deployment that supports up to 100 active agents, enter `https://<AvayaOceanaCluster1_FQDN>/services/UnifiedAgentController/workspaces/#/login`.
   - For an Avaya Oceana® deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, enter `https://<AvayaOceanaCluster2_FQDN>/services/UnifiedAgentController/workspaces/#/login`.
2. On the Agent Login screen, perform the following steps:
   a. In the **Username** field, enter the LDAP username of the agent as configured on the Users page on Avaya Control Manager.

Note:

- Ensure that the agent is configured through Avaya Control Manager to process SMS contacts.
- Ensure that the agent has appropriate attributes for this test contact.
- To simplify initial verification, ensure that no other agent with SMS capabilities is logged in. It ensures that the initial test messages are all routed to this agent.

b. In the **Password** field, enter the password of the agent.

c. Click **SIGN IN**.

3. On the Activate Agent screen, click **ACTIVATE**.
4. On the Avaya Workspaces agent interface, in the bottom right corner, verify that the agent state is `CONNECTED`.

Starting work in Avaya Workspaces

About this task

Use this procedure to configure the agent to accept incoming customer SMS messages.

Procedure

1. On the Avaya Workspaces agent interface, from the agent status drop-down list, select **StartWork**.
2. In the bottom right corner, verify that the agent state changes to `READY`.

Note:

On the Avaya Workspaces agent interface, when an agent is in the `READY` state, the agent remains available for receiving interactions until the agent is occupied on all channels for which the agent is configured.

Avaya Oceana® provides the following agent states:

- `CONNECTED`: The state of agents when they log in and activate themselves in the Avaya Workspaces or when they click the **Finish Work** button. In this state, agents do not remain available for receiving interactions.
- `Ready`: The state of agents when they click the **Start Work** or **Go Ready** button. In this state, agents remain available for receiving interactions.
- `Not Ready`: The state of agents when they click the **Additional Work** or **Go Not Ready** button. In this state, agents do not remain available for receiving interactions.

If multiplicity configuration of an agent allows receiving multiple interactions on a channel, the agent remains available for receiving interactions on that channel until the maximum multiplicity is achieved.

Verifying SMS contact routing to agents

About this task

Use this procedure to verify that the SMS messages are routed to agents.

Important:

The SMSVendorSnapin service is only for testing purposes. Therefore, do not use this service in your production environment.

Procedure

1. In your web browser, enter the following URL:

   `https://<AvayaOceanaCluster3_FQDN>/services/SMSVendorSnapin/SMSTest.html`

2. Select the **Send New SMS Message** tab.
3. On the Send New Message page, do the following:
   a. In the **To** field, enter the phone number to which you want to send the message.

      Ensure that the phone number is configured in the Omnichannel Administration Utility.

      In the Omnichannel Administration Utility, you can configure the phone numbers by clicking **SMS/Social** > **SMS Configuration** > **Details** > **Phone Number** section.

   b. In the **From** field, the phone number on which you want the agent to respond.
   c. In the **Message Text** field, type the message text.
   d. Click **Send Message**.
4. In Avaya Workspaces, verify that a ready agent received the message.
5. Answer the SMS contact.
6. Verify that the message details and number are correct.
7. Continue to verify SMS contact configuration in your solution.

Chapter 39: Configure Social Media

Configure Social Media overview

This section describes how to initially configure Avaya Oceana® to support Social Media contacts. The chapter includes the procedures required to route Social Media contacts, for more information about optional tasks or how to change default configuration, see *Administering Avaya Oceana®*.

Configuring a Social Media provider

About this task

Use this procedure to create a new Social Media provider through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. On the Avaya Oceana Server List page, do one of the following:
   - Double-click the administered Avaya Oceana® server.
   - Select the administered Avaya Oceana® server and click **Edit**.
4. Select the **Providers** tab.
5. Click **Add**.
6. In the **Type** field, select **Social**.
7. In the **Name** field, keep the value `OCP Social`.
8. In the **Address** field, enter `OCP Social`.
9. Click **Save**.
10. Restart the clusters to make the new provider available to Avaya Workspaces agents.

Configuring Social Media for third-party gateways

Procedure

1. Start Omnichannel Administration Utility.

2. In the navigation pane, click **SMS/Social**.
3. Click **Social Configuration**.
4. Click **Create**.
5. On the Account tab, perform the following steps:
    a. In the **Create Snapin** section, in the **Name** field, enter a name for the new snap-in and click **Create**.
    b. In the **Snapin** field, select the snap-in that you created.
    c. In the **Name** field, enter the name of the gateway for the snap-in.

       Social Media Snap-in can support maximum five incoming social gateway channels.
    d. In the **Gateway Name** field, enter the name of the gateway.

       You can enter up to 50 characters.
    e. In the **Social Type** field, type `Devconnect`.
    f. In the **Header Access Key** field, enter the unique access key for this channel.

       You can enter up to 50 characters.
    g. In the **Callback URL** field, enter the URL hosted by the third-party gateway.

       You can enter up to 100 characters.
6. Click **Save**.
7. Select the **Details** tab.
8. On the Details tab, perform the following steps:
    a. Click **Create**.
    b. In the **Social Handle** field, enter the social handle.
    c. Keep the **Workflow** field blank.

       To meet your specific requirements, you can configure a specific Engagement Designer workflow through the Event Catalog tab in the Engagement Designer Admin Console, and specify the name of the workflow in this field.

       If you configure a specific workflow by defining the workflow type and creating suitable Engagement Designer rules, you must also create a default rule to handle all cases that do not meet the criteria.
    d. In the **Gateway Account** field, select the account that you created in Step 5.
    e. In the **Edit Attributes** section, select the attributes based on which the incoming Social Media messages must be routed.
    f. In the **Routepoint** field, select a routepoint from the list.
    g. Click **Save**.

Configuring secure communication to third-party gateways

Procedure

1. In your web browser, open the callback URL that you specified in the **Callback URL** field while configuring Social Media for third-party gateways.
2. From your web browser, download the relevant certificate.
3. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
4. On the Cluster Administration page, do the following:
   a. Select the check box for the cluster containing SocialConnector Snap-in.
   b. Click **Certificate Management** > **Install Trusted Certificate**.
5. On the Install Trusted Certificate page, do the following:
   a. Browse and locate the certificate.
   b. Click **Retrieve Certificate**.
   c. Click **Commit**.
6. Restart the Avaya Breeze® platform nodes that are added to the cluster containing SocialConnector Snap-in.

Deploying the sample Social Media workflow

About this task

Avaya provides a sample workflow for the Social Media channel. With this procedure, you can deploy the sample Social Media workflow and configure the workflow attributes.

Before you begin

- Download the latest version of the sample workflow from PLDS.
- In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Designer Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. In the Import Workflow dialog box, click **Choose File**.
4. Browse to the folder containing the sample workflow, select the workflow, and click **Import**.
5. Click **Save Workflow**.

6. In the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaSocialAssistedService`.

      You can provide any name for the workflow.

   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.
8. In the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`
10. On the Workflows tab, verify that the OceanaSocialAssistedService workflow is available in the list of deployed workflows.
11. On the Workflows tab, select the check box for the OceanaSocialAssistedService workflow and click **Attributes**.
12. In the Workflow Attributes dialog box, do the following:
    a. In the **BotEnabled** field, keep the default value `True`.

       The `True` value specifies that the workflow always attempts to get the Bot. If your solution does not have a BotConnector or you want to skip the Bot, you must manually set this value to `False`.

    b. In the **LastAgentEnabled** field, enter the value `True` to enable the last agent routing for the Social Media channel.

       By default, the last agent routing is disabled.

    c. Click **Close**.

Deploying the sample Transfer to Service workflow for Social Media

About this task

Avaya provides a sample Transfer to Service workflow for the Social Media channel. With this procedure, you can deploy the sample Transfer to Service workflow and configure the workflow attributes.

Before you begin

- Download the latest version of the sample workflow from PLDS.
- In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Designer Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. In the Import Workflow dialog box, click **Choose File**.
4. Browse to the folder containing the sample workflow, select the workflow, and click **Import**.
5. Click **Save Workflow**.
6. In the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaSocialTransfer`.

      You can provide any name for the workflow.

   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.
8. In the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

10. On the Workflows tab, verify that the OceanaSocialTransfer workflow is available in the list of deployed workflows.
11. On the Workflows tab, select the check box for the OceanaSocialTransfer workflow and click **Attributes**.
12. **(Optional)** In the Workflow Attributes dialog box, do the following:
    a. In the **BotEnabled** field, replace the default value `False` with the value `True` to enable Bot after Transfer to Service.

       The default value `False` specifies that the workflow always tries to skip the Bot.

    b. Click **Close**.

Configuring the sample Transfer to Service workflow for Social Media

Before you begin

In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

2. On the Workflows tab, verify that the OceanaSocialTransfer workflow is available in the list of deployed workflows.
3. Click the **Routing** tab.
4. Click **Create**.
5. In the **Select event** field, click **ROUTE_CONTACT_TRANSFER**.
6. In the **Select workflows** field, select the OceanaSocialTransfer workflow.

   Note:

   Ensure that you click the workflow ending with the term `Latest`. For example, OceanaSocialTransfer:Latest.

7. In the **Enter rule name** field, type `SocialTransfer`.
8. Click **Add Rule**.
9. In the **Select schema attribute** field, click **RouteContactTransfer.ChannelType:string**.
10. In the **Select function** field, click **is equal to**.
11. In the **Enter value** field, type `Social`.
12. Click **Save**.

    The system displays the newly created rule in the list of rules.

Configuring the maximum number of days to retain active social media contacts

About this task

Configure the maximum number of days that Engagement Designer (ED) and Work Assignment can retain active social media contacts.

The default ED timeout value is 3 days. The default Work Assignment timeout value is 604800000 milliseconds, equivalent to 7 days. You can configure both of these values to retain active social media contacts for a longer period. Avaya recommends configuring these timeout values to the same number of days. The maximum value for both is 24 days.

Snap-in	Attribute	Default value	Maximum value	Comment
EngagementDesigner	Number of days the user want to retain active instances	3	24	Default value

Table continues…

Snap-in	Attribute	Default value	Maximum value	Comment
WorkAssignmentManagerService	IMPU WorkItem Queued state for Social timeout in milliseconds	604800000 (7 days)	2073600000 (24 days)	2073600000 = (24 days) = (24 * 24 * 60 * 60 * 1000 * 1 ms)

Note:

The maximum number of queued social media contacts supported by Avaya Oceana® is a fixed limit. If you extend the maximum number of days that ED and Work Assignment can retain active social media contacts, the maximum number of queued social media limit can be reached before the increased retention time expires. For more information about the supported maximum number of queued social media contacts, see Capacity specifications on page 46.

Procedure

1. Log on to the System Manager web console.
2. Click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
3. On the Service Clusters tab, from the **Cluster** list, select Avaya Oceana® Cluster 1.
4. From the **Service** list, select **EngagementDesigner**.
5. From the list of DEFAULT_GROUP attributes, navigate to the to the **Number of days the user want to retain active instances** attribute.
6. Select **Override Default**.
7. Type the maximum number of days to retain active ED workflow instances. The maximum time is 24 days.
8. Click **Commit**.
9. On the Service Clusters tab, from the **Cluster** list, select Avaya Oceana® Cluster 1.
10. From the **Service** list, select **WorkAssignmentManagerService**.
11. From the list of IMPU Configuration attributes, navigate to the to the **IMPU WorkItem Queued state for Social timeout in milliseconds** attribute.
12. Select **Override Default**.
13. Type the maximum number of milliseconds to retain active social media contacts. The maximum time is 2073600000 ms (24 days).

    For more information, see WorkAssignmentManagerService attributes on page 711.
14. Click **Commit**.
15. Reboot Avaya Oceana® Cluster 1.

Creating a user to handle Social Media contacts

About this task

Use this procedure to create an agent to handle Social Media contacts from customers.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.
3. Select the location for your Avaya Oceana®.
4. Perform one of the following steps:
   - Click **Add**.
   - Select an existing user and click **Edit**.
5. Enter appropriate value in each of the following fields:
   a. In the **First Name (English)** field, enter the first name of the user in English.
   b. In the **Surname (English)** field, enter the surname of the user in English.
   c. In the Available applications section, select the **Avaya Oceana** check box.
   d. In the **LDAP Username** field, enter the LDAP user name of the user.

      The LDAP user name must be in the username@domain.com format. This user name is used to log on to Avaya Workspaces.
   e. In the **Username** field, enter a user name.

      In this release, the user name is the internal handle.
   f. In the **Password** field, enter a password.

      This password is used to log on to Avaya Control Manager.
   g. In the **Confirm Password** field, re-enter the password.
   h. In the **Extension** field, enter the station associated with this agent.

      This is used when logging on to Avaya Workspaces.
   i. In the **AVAYA Login** field, enter the Elite agent login ID only if the agent also supports Voice contacts. Otherwise, leave this field blank.
   j. Click **Save**.
6. Scroll to the right and select the **Avaya Oceana** tab.
7. Select the **Social** check box.

Important:

To change the channel of an agent while the agent is live, the agent must be logged out and logged in again.

8. From the **Multiplicity** drop-down list, select the maximum of concurrent Social Media contacts.

   The ability of an agent to handle multiple concurrent multimedia contacts is called Multiplicity.

9. Select the **Attributes** tab.
10. Move the attributes from the **Available Attributes** list to the **Agent Attributes** list.

    Important:

    You must move the same attributes that you configured in the Omnichannel Administration Utility for the Social Media to be routed to your agent.

11. Click **Save**.

Configuring Social Media for Transfer to Service

Configuring a Transfer to Service Route Point for Social Media

About this task

Use this procedure to create a new Transfer to Service Route Point for Social Media through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Route Points**.
2. On the Route Points List page, click **Add**.
3. To add the Transfer to Service Route Point, perform the following steps:
   a. In the **Type** field, select `Route Point`.
   b. In the **Sub Type** field, select `Transfer to Service`.
   c. In the **Name** field, enter a name for the Route Point.
   d. Click **Save**.

Creating a Transfer Target service for Social Media

About this task

Use this procedure to create a Transfer Target service for Social Media through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™** > **Work Assignment**.
2. Select the **Services** tab.
3. On the Services tab, click **Add**.
4. To add a Transfer Target service, perform the following steps:
   a. In the **Service Name** field, enter the name of the service.
   b. Select the **Available for Transfer** check box.

      The system automatically selects the **Agent Display** check box.
   c. Move the required attributes from the **Available Attributes** list to the **Included Attributes** list.
   d. In the Transfer Routepoints section, in the **Social** field, select the Route Point that you created for Social Media.
   e. Click **Save**.

Deployment process for the Asynchronous Connector

Important:

For production environments, you must deploy the Async Messaging Connector in a High Availability environment.

For laboratory deployments, High Availability is not required. You may select laboratory deployments in the Excel deployment spreadsheet to do this.

Note:

The compute resources allocated to asynchronous components are unchanged.

No.	Task	Description	✔
1	Configure your Digital Connection account and note the application ID, provider key, and security key.	See *Administering Avaya OneCloud™ CCaaS*.	

Table continues…

No.	Task	Description	✔
2	Deploy Avaya Oceana® and note the FQDN of the Avaya Oceana® Omnichannel Provider (OCP) cluster.	See “Configuring the Avaya Analytics™ deployment spreadsheet for Messaging” in *Deploying Avaya Analytics for Avaya Oceana*.	
3	Create a new Avaya Oceana® user, required for securing file transfers.	See *Deploying Avaya Oceana®*.	
4 a	Deploy Avaya Analytics™ and Asynchronous Connector using the application ID, provider key, and security key provided from the Digital Connection account and the Avaya Oceana® OCP cluster FQDN. Specify the Avaya Oceana® user created for the file transfers.	See “Post-installation configuration for Messaging” in *Deploying Avaya Analytics for Avaya Oceana*.	
4 b	Ensure the post-installation steps are performed. Install Avaya Aura® System Manager CA certificate CSP. You may also require to install your corporate proxy certificate if one exists in your organization, for example, Zscaler. You may also require to install the Amazon Root CA; that is, the Digital Connection cloud service deployed in AWS. Usually, servers have trusted Amazon CA. In the unlikely event that it is not already trusted, deploy and install this certificate.		

5	After the deployment completes successfully, you must ensure the Digital Connection Cloud provider can access the Digital Connection component and Asynchronous Messaging Connector on CSP. Ensure your external load balancer is publicly accessible and is configured to point to the FQDN of the newly installed Asynchronous product. The mapping setup depends on your hardware infrastructure.
	For example:
	If you are using a reverse proxy, you may have to specify a port depending on the setup.
	`https://your.external.loadbalancer.fqdn/async/messaging/v1/health-check HTTP GET`
	`https://csp.cluster.fqdn/async/messaging/v1/health-check HTTP GET`
	Expected response:
	`{alive:true}`
	Proceed to the next step.		

Table continues…

No.	Task	Description	✔
6	Register the webhook created by the Asynchronous Connector deployment in your Digital Connection account. Provide the FQDN for inbound traffic into the CSP cluster to your Digital Connection account administrator. You must complete this step before messages are routed.		
7	Optional: After your Digital Connection account administrator successfully registers webhook, you are provided with a secret for your webhook. This is an API Key sent with each REST request from the Digital Connection provider. If your organization uses a network edge security device, you can configure validation of the secret by checking the following value from the REST header: `X-API-Key: secret`		
8	Identify the integrations you must support in your environment, such as iOS, Android, or Web SDKs for custom messaging-enabled applications, WhatsApp, Facebook Messenger, and Twitter DM Social Messaging applications. Your Digital Connection account administration must configure this after providing them with the account details for each channel and any security credentials for the chosen channels.		
9	Ensure the Engagement Designer Messaging workflow in Avaya Oceana® is deployed, target agents are assigned the Messaging channel, and the assigned attributes match the attributes specified in the Excel workbook.	See *Deploying Avaya Oceana®*.	
10	If you are using Android, iOS or Web SDK integrations, download the latest sample clients and SDK from DevConnect `Avaya_In-app-Messaging_SDKs_Oceana_R.zip`. Follow the `Readme` guide to setup the sample clients, ensuring they are configured correctly for your Digital Connection account.		
11	If you are using WhatsApp, Facebook Messenger, or Twitter DM, you can send messages directly to the business number or profile if these are configured integrations in your Digital Connection account (Step 8).		
12	Route the inbound messaging interactions to your logged-in agents.		

Configuring AgentControllerService to access UnifiedAgentController

About this task

Starting from Avaya Oceana® Release 3.8.0.0, UnifiedAgentController requires all the requests to its internal endpoints to be authenticated using the AuthorizationService token. Use this procedure to configure AgentControllerService to access UnifiedAgentController.

You can also configure AgentControllerService using the OceanaConfiguration service. For more information about the OceanaConfiguration service, see Setting OceanaConfiguration attributes on page 117.

Note:

This procedure is mandatory for Avaya Oceana® to handle contacts properly.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In **Clusters**, click Avaya Oceana® Cluster 3.
   b. In **Service**, click **AgentControllerService**.
3. For **Authorization Service Address**:
   a. Select the **Override Default** check box.
   b. In **Effective Value**, enter the IP address or FQDN of the cluster that hosts AuthorizationService.
4. Click **Commit**.

Setting the Authorization Service address to enable authorized access to Oceana transcripts

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In **Clusters**, click Avaya Oceana® Cluster 1.
   b. In **Service**, click **OCPDataServices**.
3. For **Authorization Service Address**:
   a. Select the **Override Default** check box.
   b. In **Effective Value**, enter the IP address or FQDN of the cluster that hosts AuthorizationService.
4. For **Enable Tokenless Access**:
   a. Select the **Override Default** check box.
   b. In **Effective Value**, select **false**.
5. Click **Commit**.
6. Restart Avaya Oceana® Cluster 3.

Chapter 40: Verify Social Media contacts

Verify Social Media contacts using Avaya Workspaces

This section describes how to use Avaya Workspaces to verify that the Avaya Oceana® is correctly configured to process Social Media contacts.

Deploying Avaya Workspaces

Procedure

1. Install and commission Avaya Workspaces.

   For information about how to install and commission Avaya Workspaces, see the following documents:

   - *Using Avaya Workspaces for Avaya Oceana®*
   - *Administering Avaya Oceana®*
2. Identify the login details of an agent configured to handle Social Media contacts.

Logging in to Avaya Workspaces

About this task

Use this procedure to log in to Avaya Workspaces to verify access details and agent status.

Procedure

1. Enter one of the following URLs in your web browser:
   - For an Avaya Oceana® deployment that supports up to 100 active agents, enter `https://<AvayaOceanaCluster1_FQDN>/services/UnifiedAgentController/workspaces/#/login`.
   - For an Avaya Oceana® deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, enter `https://<AvayaOceanaCluster2_FQDN>/services/UnifiedAgentController/workspaces/#/login`.
2. On the Agent Login screen, perform the following steps:
   a. In the **Username** field, enter the LDAP username of the agent as configured on the Users page on Avaya Control Manager.

Note:

- Ensure that the agent is configured through Avaya Control Manager to process Social Media contacts.
- Ensure that the agent has appropriate attributes for this test contact.
- To simplify initial verification, ensure that no other agent with Social Media capabilities is logged in. It ensures that the initial test messages are all routed to this agent.

b. In the **Password** field, enter the password of the agent.

c. Click **SIGN IN**.

3. On the Activate Agent screen, click **ACTIVATE**.
4. On the Avaya Workspaces agent interface, in the bottom right corner, verify that the agent state is `CONNECTED`.

Starting work in Avaya Workspaces

About this task

Use this procedure to configure the agent to accept incoming customer Social Media messages.

Procedure

1. On the Avaya Workspaces agent interface, from the agent status drop-down list, select **StartWork**.
2. In the bottom right corner, verify that the agent state changes to `READY`.

Note:

On the Avaya Workspaces agent interface, when an agent is in the `READY` state, the agent remains available for receiving interactions until the agent is occupied on all channels for which the agent is configured.

Avaya Oceana® provides the following agent states:

- `CONNECTED`: The state of agents when they log in and activate themselves in the Avaya Workspaces or when they click the **Finish Work** button. In this state, agents do not remain available for receiving interactions.
- `Ready`: The state of agents when they click the **Start Work** or **Go Ready** button. In this state, agents remain available for receiving interactions.
- `Not Ready`: The state of agents when they click the **Additional Work** or **Go Not Ready** button. In this state, agents do not remain available for receiving interactions.

If multiplicity configuration of an agent allows receiving multiple interactions on a channel, the agent remains available for receiving interactions on that channel until the maximum multiplicity is achieved.

Verifying Social Media contact routing to agents

About this task

You can verify to ensure that the social media contacts are routed to agents by using the SMSVendorSnapin service.

Important:

The SMSVendorSnapin service is only for testing purposes. Do not use this service in your production environment.

Before you begin

- Ensure that the Social Media Snap-in is available in Omni Channel Administration.
- Ensure that the Social agent is available in Avaya Control Manager.
- Get the snapin keys or the gateway identifiers that is available in Omni Channel Administration Social Gateway Details panel.

Procedure

1. On your web browser, enter the following URL:

   `https://<AvayaOceanaCluster3_FQDN>/services/SMSVendorSnapin/SMSTest.html`.

2. To obtain the identifier or the gatewayID for the agent, click **Gateway Accounts**.

   The SMSVendorSnapin service displays the **Get Gateway Accounts** page.

3. In the **Key** field, enter the snapin key for example, `snapinSMS` and click **Get Gateways**.

   The Response section on the right displays the identifiers.

4. Note the identifier or the gateway ID that you require for future routing.
5. Click **Send Social Message into Gila**.
6. On the Send New Social Message page, do the following:
   a. In the **From Name** field, enter the name of the sender that you want the work card to display in Avaya Workspaces.
   b. In the **From Account** field, enter the user ID of the sender.
   c. In the **To** field, enter the identifier or the gateway ID that you noted earlier.
   d. In the **Message Text** field, type the sample message text.
   e. In the **Messaging Service** field, type the name of the service that you are using to deliver the message. For example, twittermessage, twitterdm, facebook
   f. In the **Message Type** field, type the type of message for example, `TEXT_PUBLIC` or `TEXT_PRIVATE`.
7. Click **Send Social Message**.
8. In Avaya Workspaces, verify that a ready agent received the message.

9. Answer the Social contact.
10. Verify that the message details and number are correct.
11. Continue to verify Social contact configuration in your solution.

Chapter 41: Configure Messaging

Configure Messaging overview

Avaya Oceana® supports the Messaging channel. With this channel, a customer can use a Chat-like interface to engage with a contact center agent over an extended period. The communication between the customer and agent does not require live availability of either of them.

Organizations can enable Messaging in their applications for a customer to submit queries. After submitting the queries, the customer can close the application. The customer does not have to wait for an immediate response. When an agent responds, the device notification alerts the customer. When the customer opens the application, the application shows the conversation and enables the conversation to continue seamlessly. Conversation through the Messaging channel contain many engagements over an extended period. The full conversation remains visible to all participants. Messaging conversations are currently supported through In-App Messaging, WhatsApp, Facebook Messenger, and Twitter Direct Messaging.

For information about how to deploy Messaging, see *Deploying Avaya Analytics*™.

For information on social messaging platforms, see *Using Avaya Workspaces for Avaya Oceana*®.

The following table provides information about the administrative tasks for the Messaging channel:

Component	Tasks
Avaya Control Manager	Administrative tasks are: • Configuring a Messaging provider • Assigning the Messaging channel to an agent and assigning a multiplicity value • Configuring the Messaging channel for Transfer to Service • Configuring screen pops for Messaging
Omnichannel Administration Utility	Administrative tasks are: • Creating automatic phrases for Messaging • Creating a welcome message to send to the customer when an agent joins the interaction

Table continues…

Component	Tasks
Avaya Engagement Designer	Administrative tasks are: • Deploying the sample Messaging workflow • Deploying the sample Transfer to Service workflow for Messaging • Configuring the sample Transfer to Service workflow for Messaging Avaya Oceana® provides a sample Engagement Designer workflow for Messaging. Messaging interactions are assigned routing attributes and are routed through the sample workflow. Each engagement from the customer is routed as a separate interaction. The workflow encapsulates the last agent routing logic to maintain the conversations by showing the past engagement messages in the active conversation window.

The following table provides information about the rich media content that the Messaging channel supports:

Feature	Description
Text and Emojis	Supports plain text messages and Unicode Emojis.
Images, GIFs*, and Stickers	Supports images, GIFs, and stickers.
Links	Displays web links as buttons and transforms links into clear calls to action.
Location	Supports sending and receiving geographical location messages.
Postback	Supports sending buttons to trigger events on your server. Based on the selection, the server acts and posts messages back to the customer.
Reply	Suggests a few answers to reply to a message.
Location Request	Supports requesting the current location of the customer.
Compound Message	Supports sending a text, image, and multiple buttons in a single message.
Typing Status	Displays a typing indicator.
Carousel	Supports sending a horizontally scrollable set of cards containing text, image, and action buttons. Carousels support a maximum of 10 message items. Each message item must include a title and at least one supported action.

Table continues…

Feature	Description
Badge for unread messages	Displays a badge containing the count of unread messages in the header of the web messenger.
Push Notification	Sends push notifications to let the customer know when an agent replies to the customer query.
*Animated GIF displays first frame only in Android devices. Otherwise, GIFs are rendered as MPEG files.	

Deploying the sample Messaging workflow

About this task

Avaya provides a sample workflow for the Messaging channel. With this procedure, you can deploy the sample Messaging workflow and configure the workflow attributes. This workflow is also applicable for WhatsApp messaging.

Before you begin

- Download the latest version of the sample workflow from PLDS.
- In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Designer Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. In the Import Workflow dialog box, click **Choose File**.
4. Browse to the folder containing the sample workflow, select the workflow, and click **Import**.
5. Click **Save Workflow**.
6. In the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaMessagingAssistedService`.

      You can provide any name for the workflow.

   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.
8. In the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

`https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

10. On the Workflows tab, verify that the OceanaMessagingAssistedService workflow is available in the list of deployed workflows.

    If the workflow is not available in the list, you must redeploy the workflow.

11. On the Workflows tab, select the check box for the OceanaMessagingAssistedService workflow and click **Attributes**.

12. In the Workflow Attributes dialog box, do the following:

    a. In the **BotEnabled** field, keep the default value `True`.

       The `True` value specifies that the workflow always attempts to get the Bot. If your solution does not have a BotConnector, or you want to skip the Bot, you must manually set this value to `False`.

    b. In the **LastAgentEnabled** field, enter the value `True` to enable the last agent routing for the Messaging channel.

       By default, the last agent routing is disabled.

    c. In the **OngoingThreadTime** field, set the time in seconds.

       For the Messaging High Availability (HA) in Avaya Oceana®, you must enable this attribute with a reasonable value, such as several minutes, hours, or a day. You must also ensure that you enter the value only after converting it to seconds. This attribute is used in the Omnichannel Provider logic to identify whether a saved contact enters an interaction with Auto Bot, when contact is restored after cluster reboot. The default value of this attribute is `86400` secs.

    d. Click **Close**.

Deploying the sample Transfer to Service workflow for Messaging

About this task

Avaya provides a sample Transfer to Service workflow for the Messaging channel. With this procedure, you can deploy the sample Transfer to Service workflow and configure the workflow attributes.

Before you begin

- Download the latest version of the sample workflow from PLDS.
- In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Designer Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/index.html`

2. Click **Import**.
3. In the Import Workflow dialog box, click **Choose File**.
4. Browse to the folder containing the sample workflow, select the workflow, and click **Import**.
5. Click **Save Workflow**.
6. In the Save Workflow dialog box, do the following:
   a. In the **Workflow** field, type `OceanaMessagingTransfer`.

      You can provide any name for the workflow.

   b. Select the folder where you want to save the workflow.
   c. Click **Save**.
7. Click **Deploy Workflow**.
8. In the Deployment Details dialog box, click **OK**.
9. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

10. On the Workflows tab, verify that the OceanaMessagingTransfer workflow is available in the list of deployed workflows.

    If the workflow is not available in the list, you must redeploy the workflow.

11. On the Workflows tab, select the check box for the OceanaMessagingTransfer workflow and click **Attributes**.
12. **(Optional)** In the Workflow Attributes dialog box, do the following:
    a. In the **BotEnabled** field, replace the default value `False` with the value `True`.

       When you replace the default value, the workflow enables the Bot after the contact is transferred to a service. The default value `False` specifies that the workflow always attempts to skip the Bot.

    b. Click **Close**.

Configuring the sample Transfer to Service workflow for Messaging

About this task

Use this procedure to configure the sample Transfer to Service workflow for Messaging.

Before you begin

In the Windows hosts file, add an entry containing the cluster IP address and FQDN of Avaya Oceana® Cluster 1. The FQDN in the entry must be different from the FQDNs of Avaya Oceana® Cluster 1 nodes.

Procedure

1. In your web browser, enter the following URL to open the Admin Console of Engagement Designer:

   `https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html`

2. On the Workflows tab, verify that the OceanaMessagingTransfer workflow is available in the list of deployed workflows.
3. Click the **Routing** tab.
4. Click **Create**.
5. In the **Select event** field, click **ROUTE_CONTACT_TRANSFER**.
6. In the **Select workflows** field, select the OceanaMessagingTransfer workflow.

   Note:

   To select the latest workflow, ensure that you click the workflow ending with the term `Latest`. For example, OceanaMessagingTransfer:Latest.

7. In the **Enter rule name** field, type `MessagingTransfer`.
8. Click **Add Rule**.
9. In the **Select schema attribute** field, click **RouteContactTransfer.ChannelType:string**.
10. In the **Select function** field, click **is equal to**.
11. In the **Enter value** field, type `Messaging`.
12. Click **Save**.

    Engagement Designer displays the newly created rule in the list of rules.

Configuring a Messaging provider

About this task

Use this procedure to create a new Messaging provider through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. On the Avaya Oceana Server List page, do one of the following:
   - Double-click the administered Avaya Oceana® UCA server.
   - Select the administered Avaya Oceana® UCA server and click **Edit**.
4. Select the **Providers** tab.
5. Click **Add**.
6. In the **Type** field, select **Messaging**.
7. In the **Name** field, keep the value `OCP Messaging`.
8. In the **Address** field, enter `OCP Messaging`.
9. Click **Save**.
10. Restart the clusters to make the new provider available to Avaya Workspaces agents.

Configuring the maximum number of days to retain active messaging contacts

About this task

Configure the maximum number of days that Engagement Designer (ED) and Work Assignment can retain active messaging contacts.

The default ED timeout value is 3 days. The default Work Assignment timeout value is 604800000 milliseconds, equivalent to 7 days. You can configure both of these values to retain active messaging contacts for a longer period. Avaya recommends configuring these timeout values to the same number of days. The maximum value for both is 24 days.

Snap-in	Attribute	Default value	Maximum value	Comment
EngagementDesigner	Number of days the user want to retain active instances	3	24	Default value
WorkAssignmentManagerService	IMPU WorkItem Queued state for Messaging timeout in milliseconds	604800000 (7 days)	2073600000 (24 days)	2073600000 = (24 days) = (24 * 24 * 60 * 60 * 1000 * 1 ms)

Note:

The maximum number of queued messaging contacts supported by Avaya Oceana® is a fixed limit. If you extend the maximum number of days that ED and Work Assignment can retain active messaging contacts, the maximum number of queued messaging limit can be reached before the increased retention time expires. For more information about the supported maximum number of queued messaging contacts, see Capacity specifications on page 46.

Procedure

1. Log on to the System Manager web console.
2. Click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
3. On the Service Clusters tab, from the **Cluster** list, select Avaya Oceana® Cluster 1.
4. From the **Service** list, select **EngagementDesigner**.
5. From the list of DEFAULT_GROUP attributes, navigate to the to the **Number of days the user want to retain active instances** attribute.
6. Select **Override Default**.
7. Type the maximum number of days to retain active ED workflow instances. The maximum time is 24 days.
8. Click **Commit**.
9. On the Service Clusters tab, from the **Cluster** list, select Avaya Oceana® Cluster 1.
10. From the **Service** list, select **WorkAssignmentManagerService**.
11. From the list of IMPU Configuration attributes, navigate to the to the **IMPU WorkItem Queued state for Messaging timeout in milliseconds** attribute.
12. Select **Override Default**.
13. Type the maximum number of milliseconds to retain active messaging contacts. The maximum time is 2073600000 ms (24 days).

    For more information, see WorkAssignmentManagerService attributes on page 711.
14. Click **Commit**.
15. Reboot Avaya Oceana® Cluster 1.

Creating a user to handle Messaging contacts

About this task

Use this procedure to create a user to handle Messaging contacts from customers.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.
3. Select the location for your Avaya Oceana®.
4. Perform one of the following steps:
   - Click **Add**.
   - Select an existing user and click **Edit**.
5. Enter the appropriate value in each of the following fields:
   a. In the **First Name (English)** field, enter the first name of the user in English.
   b. In the **Surname (English)** field, enter the last name of the user in English.
   c. In the Available applications section, select the **Avaya Oceana** check box.
   d. In the **LDAP Username** field, enter the LDAP user name of the user.

      The LDAP user name must be in the username@domain.com format. The LDAP user name is used for logging on to Avaya Workspaces.
   e. In the **Username** field, enter a user name.

      In this release, the user name is the internal handle.
   f. In the **Password** field, enter a password.

      This password is used for logging on to Avaya Control Manager.
   g. In the **Confirm Password** field, re-enter the password.
   h. In the **Extension** field, enter the station associated with this agent.

      This station is used when logging on to Avaya Workspaces.
   i. In the **AVAYA Login** field, enter the Elite agent login ID only if the agent also supports Voice contacts. Otherwise, leave this field blank.
   j. Click **Save**.
6. Scroll right and select the **Avaya Oceana** tab.
7. Select the **Messaging** check box.

Important:

The agent must log out and log in again to change the channel while the agent is live.

8. From the **Multiplicity** drop-down list, select the maximum of concurrent Messaging contacts.

   The ability of an agent to handle multiple concurrent multimedia contacts is called Multiplicity.

9. Select the **Attributes** tab.
10. Move the attributes from the **Available Attributes** list to the **Agent Attributes** list.
11. Click **Save**.

Configuring Messaging for Transfer to Service

Configuring a Transfer to Service Route Point for Messaging

About this task

Use this procedure to create a new Transfer to Service Route Point for Messaging through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Route Points**.
2. On the Route Points List page, click **Add**.
3. To add the Transfer to Service Route Point, perform the following steps:
   a. In the **Type** field, select `Route Point`.
   b. In the **Sub Type** field, select `Transfer to Service`.
   c. In the **Name** field, enter a name for the Route Point.
   d. Click **Save**.

Creating a Transfer Target service for Messaging

About this task

Use this procedure to create a Transfer Target service for Messaging through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™** > **Work Assignment**.
2. Select the **Services** tab.
3. On the Services tab, click **Add**.
4. To add a Transfer Target service, do the following:
    a. In the **Service Name** field, enter the name of the service.
    b. Select the **Available for Transfer** check box.

       Avaya Control Manager automatically selects the **Agent Display** check box.
    c. Move the required attributes from the **Available Attributes** list to the **Included Attributes** list.
    d. In the Transfer Routepoints section, in the **Messaging** field, select the Route Point that you created for Messaging.
    e. Click **Save**.

Configuring screen pops for Messaging

About this task

Use this procedure to configure screen pops for Avaya Workspaces agents to view information about contacts.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **ScreenPOP Configuration**.
3. **(Optional)** Select the **Screen Pop Filters** tab and do the following:
    a. Click **Add**.
    b. In the **Name** field, type the name of the filter.
    c. In the **Provider** field, select the service provider.
    d. **(Optional)** If any service is assigned for the client, in the **Service Name** field, click the assigned service name.

       If you specify a service name here, only the contacts with a matching service name receive a screen pop that has this filter applied.

e. Click **Save**.

4. Select the **Screen Pop Applications** tab and do the following:
   a. Click **Add**.
   b. In the **Name** field, type the name of the application.
   c. In the **URL** field, type the URL of the screen pop application.

      You can add pairs of curly braces {} to represent additional parameters collected from the contact. For example, an account number entered in a voice response interaction. Put a plus sign between each set of curly braces.

      For example, `http://www.google.com?search={}+{}`.

   d. Click **Save**.
5. Select the **Screen Pops** tab and do the following:
   a. Click **Add**.
   b. In the **Name** field, type a name for the screen pop.

      Avaya Workspaces displays this name on the screen pop tab.

   c. In the **Provider** field, select `OCP Messaging`.
   d. In the **Application Name** field, select the application that you created on the **Screen Pop Application** tab.
   e. **(Optional)** In the **Filter Name** field, click the filter name that you created on the **Screen Pop Filters** tab.

      If you do not assign a filter, the system displays the screen pop for all interactions of the Messaging provider.

   f. In the **Event** field, select `ACTIVE`.

      This value specifies that the screen pop is displayed for the interaction when the interaction is in the active state.

   g. In the **Event Direction** field, select `INCOMING` or `OUTGOING`.

      This value specifies whether the screen pop is displayed for incoming or outgoing interactions.

   h. In the **Auto Close** field, select `Yes` or `No`.

      If you select `Yes`, the screen pop closes when you close the interaction card. If you select `No`, the screen pop remains open even after the interaction is closed. You must manually close the screen pop.

   i. In the **Launch Internal** field, select `Yes` or `No`.

      To display the screen pop in the Avaya Workspaces client, select `Yes`. To display the screen pop in a new window, select `No`.

   j. In the **Priority** field, type the screen pop display order.

Do not duplicate the priority because two screen pops cannot have the same priority. Avaya Workspaces displays five screen pops. A screen pop with a lower priority number gets the preference over the screen pop with a higher priority number.

You can configure a maximum of five screen pops for a single interaction. The value in the **Priority** field determines which screen pops to display if more than five screen pops match the criteria of the contact. The priority value must be unique to avoid overriding screen pops.

The **URL** field displays the URL created on the **Screen Pop Applications** tab that is associated with the **Application Name** you select.

k. **(Optional)** In the **Screen Pop Parameters** section, in the **Intrinsics** column, click a parameter.

The **Parameter Position** field displays the number corresponding to the order in which the parameter is added to the URL. The number of parameters depends on the number of curly braces at the end of the URL.

To add the originating address as the first parameter for the URL, click the **Originating Address** parameter in the **Intrinsics** column in row 1.

l. Click **Save**.

Messaging limits

For Messaging:

- The length of a text message must be between 1-4000 characters.
- The whole length of CustomData size must be between 1-7500 characters.
- The length of coaching messages, which are sent between the agent and supervisor, must be between 1-4000 characters.

Incoming messages limit

The following table shows incoming messages limits depending on the Messaging Service Deployment Type attribute:

Deployment type	Rate Limit (messages per second)
OCEANA_LAB	3
OCEANA_SMALL	3
OCEANA_MEDIUM	33

Table continues…

Deployment type	Rate Limit (messages per second)
OCEANA_LARGE	33
OCEANA_XLARGE	33
OCEANA_3XLARGE	66
OCEANA_4XLARGE	66

If the rate limit exceeds, Avaya Oceana® does not process the incoming message and displays the following message: `Messages rate <rate> exceeded. Reject the message <message parameters>.`

Configuring Message Connector parameters in Omnichannel Administration Utility

About this task

For Messaging, configure a new message connector address and secure mode in the Omnichannel Administration Utility.

Note:

To apply the new address, you must restart the OCP cluster.

Procedure

1. Start the Omnichannel Administration Utility.
2. In the navigation pane, click **General Administration**.
3. Click the **Server Settings**.
4. Click **New**.
5. From the drop-down list, select **Messaging Connector Server**.
6. In the **New Messaging Connector Server** section, in the **IP/FQDN** field, enter the IP address or FQDN of the Async server.
7. In the **Port** field, enter the port number as `443`.
8. Select the **Enable secure mode (HTTPS)** check box for a secure communication.
9. Click **Save**.

Installing Certificate Authority and Identity Certificate for Messaging HA

About this task

For communication with the Messaging Connector deployed on the Avaya Common Services (CSP) cluster, you must install the Certificate Authority and Identity Certificate.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, do the following:
   a. Select the check box for the Messaging cluster.
   b. Click **Certificate Management** > **Install Trusted Certificate**.
3. On the Install Trusted Certificate page, do the following:
   a. Browse and locate the certificate.
   b. Click **Retrieve Certificate**.
   c. Click **Commit**.
4. Click **Done**.

Viewing contact status in Oceana Data Viewer for Messaging HA

About this task

The Messaging page of the Oceana Data Viewer provides an option to save Messaging contacts before reboot. Thus, the MessagingConnector enables or disables incoming contacts.

Important:

If the administrator wants to restart the cluster and there are Messaging contacts that are not in a closed state, they must select a **Save Contacts** option in the Oceana Data Viewer that saves the contents of the contacts. When you restart Avaya Oceana®, the contacts are re-routed to the available agents. Saving incoming contacts is a mandatory step before any planned reboot to allow contact data preservation.

Procedure

1. In your web browser, enter the following URL to view the Oceana Data Viewer page:

   `https://<Cluster IP>/services/OceanaDataViewer/ocp/home.html`

2. On the authentication screen, do the following:
   a. In the **Username** field, enter the LDAP username of the Administrator agent as configured on the Users page on Avaya Control Manager.
   b. In the **Password** field, enter the password of the agent.
   c. Click **SIGN IN**.
3. On the Oceana Data Viewer page, click **Messaging**.
4. Click **Save Contacts**.

   The background color of the **Save Contacts** button reflects the current status of incoming contacts:

   - Green: Accept incoming contacts.

- Red: Do not accept incoming contacts.

If incoming contacts are enabled, and you click **Save Contacts**, then:

- The database saves all Messaging contact transcripts.
- The MessagingConnector closes incoming contacts.

If incoming contacts are disabled, and you click **Save Contacts**, the MessagingConnector allows incoming contacts.

Configuring AgentControllerService to access UnifiedAgentController

About this task

Starting from Avaya Oceana® Release 3.8.0.0, UnifiedAgentController requires all the requests to its internal endpoints to be authenticated using the AuthorizationService token. Use this procedure to configure AgentControllerService to access UnifiedAgentController.

You can also configure AgentControllerService using the OceanaConfiguration service. For more information about the OceanaConfiguration service, see Setting OceanaConfiguration attributes on page 117.

Note:

This procedure is mandatory for Avaya Oceana® to handle contacts properly.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In **Clusters**, click Avaya Oceana® Cluster 3.
   b. In **Service**, click **AgentControllerService**.
3. For **Authorization Service Address**:
   a. Select the **Override Default** check box.
   b. In **Effective Value**, enter the IP address or FQDN of the cluster that hosts AuthorizationService.
4. Click **Commit**.

Setting the Authorization Service address to enable authorized access to Oceana transcripts

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In **Clusters**, click Avaya Oceana® Cluster 1.
   b. In **Service**, click **OCPDataServices**.
3. For **Authorization Service Address**:
   a. Select the **Override Default** check box.
   b. In **Effective Value**, enter the IP address or FQDN of the cluster that hosts AuthorizationService.
4. For **Enable Tokenless Access**:
   a. Select the **Override Default** check box.
   b. In **Effective Value**, select **false**.
5. Click **Commit**.
6. Restart Avaya Oceana® Cluster 3.

Delivery Failure Notification

Avaya Oceana® may undergo outages or maintenance windows longer than 15 minutes. The users who message the contact center during an outage period may be unaware that the message has not been delivered to the Contact Center.

The Delivery Failure Notification feature provides automatic configurable notification to the users that the message has not been processed and to retry again later. The system notifies the users with a message similar to the following:

```
Unfortunately the system is unavailable at the moment. Please try your
message again later.
```

You can modify the notification in the deployment excel file.

The users are also notified that the messages sent to the Contact Center are not processed if Avaya Oceana® has reached the maximum capacity. In this scenario, the system notifies the users with a message similar to the following:

```
Unfortunately the system is busy at the moment. Please try your message
again later.
```

You can modify the notification in the deployment excel file.

Important:

This feature does not need any configuration. Defaulted messages are in place for both the system busy and system unavailable scenarios. You can modify the default messages in the deployment excel file.

Operation

The Messaging Connector specifies if it is currently receiving messages `UP` or not `Down`. When the status is `UP`, normal message processing continues. If the status is `DOWN`, a configurable notification is sent to the users notifying them that the message has not been processed and to retry again later.

Scenario	Operation
Avaya Oceana® planned or unplanned reboot - Messaging Connector not impacted	The Messaging Connector monitors the status of Avaya Oceana®. The endpoint is notified to set the application in a `DOWN` state. New messages beyond that time, receive the configured delivery failure message. Upon Avaya Oceana® recovery, the Messaging Connector sets the application to an `UP` state using the endpoint. Further messages after this point do not receive the delivery failure notification.
Avaya Oceana® planned or unplanned reboot - Messaging Connector rebooted	A timing issue may occur. If the Messaging Connector is rebooted first OR both Avaya Oceana® and the Messaging Connector are rebooted at the same time, the status of the application cannot be updated to `DOWN`, therefore delivery failure messages are not sent.
Disaster recovery failover - Avaya Oceana® and Messaging Connector	Not Supported.
Network Outages	If a network failure occurs between the Messaging Connector and Avaya Oceana®, the Messaging Connector detects this outage and updates the application status to `DOWN` which resets on recovery. Where the network outage isolates the Messaging Connector from being able to communicate with Avaya Oceana®, the status cannot be set to `DOWN` and therefore no delivery failure message is sent to the user.
System Busy	When Avaya Oceana® reaches maximum capacity and new messages arrive, one of the following can occur: • The new message is part of an existing conversation that is in queue or open with an agent. The message is processed as no new chatroom needs to be created. • The new message does not have an existing conversation open or in queue. A new chatroom is necessary but Avaya Oceana® does not have the capacity to create this. Therefore, a system busy message is sent to the user notifying them to retry later.

Limitations

- The user message is retried by the application for up to 15 minutes. Therefore, if the system recovers and the Messaging Connector is in an `UP` status within 15 minutes of the user sending the message, the retried message may be received even though the user has received a delivery failure notification.

- The user continues to see the failed message in their transcript history on the social messaging application. However, the failed message is not visible to the agent.
- During complete outage of the messaging component, for example, power outage, it is not possible to set the status to `DOWN`, therefore users do not receive the delivery failure notification message.

Credit Card Redaction

Avaya Oceana® introduces the Credit Card Redaction feature which allows credit card patterns sent by the user in a message to be redacted, and not shared with the agent, or stored in the transcript.

The feature is enabled at an application level and applied to all user messages received on any platform. Only the user messages having the credit card details redacted, the agent messages are not checked. The feature scans for common credit card patterns, such as 16-digit numbers, including combinations of credit card numbers separated by dot, space, or dash. For example, 4242 4242 4242 4242.

Configuration

The Avaya New Product Introduction (NPI) team configures this feature on behalf of the customer.

Operation

The credit card masking function is enabled at application level. The Avaya NPI team administers the operation on behalf of the customer.

Scenario	Operation
Mask Credit Card Numbers Enabled	When a user sends a message that contains any combination of a credit card pattern, the card number is redacted.
Masked Credit Card Numbers Disabled	Messages must pass through without masking the credit card numbers.

Limitations

PIN numbers, expiry dates, or CVV codes are not redacted by this feature. Also, if the credit card pattern is different from the pattern mentioned above, it may not be filtered.

For example, if a user replaces a zero with the letter 'O' - the examples may be missed by the filter.

Enabling this feature only impacts future messages. The existing credit card numbers in conversations, already in queue, or already in historical transcripts are not redacted.

Routing enhancement - contact priority

Avaya Oceana® introduces custom routing attribute using which Contact Priority (1-100) can be set for the web messenger.

Configuration

You can configure contact priority in the deployment excel file during the deployment. This value is used for Social messaging platforms. Priority value ranges from 1 to 100, with 1 being the highest priority. If priority is set to a value out of this range, the value 5 is used.

Operation

The feature enables contact priority to be set in the following ways:

- Web front-end - a web developer can specify the priority programmatically.
- System default priority: If the priority has not been set from the web front-end, or when using other channels, a default priority can be set in the deployment excel file.

Scenario	Operation
Priority set from web messenger	The priority value set as a metadata value in the `index.html` is passed as the contact priority intrinsic to the Engagement Deployment Workflow. *oceana_intrinsic_contact_priority* attribute is added with value in range from 1 to 100.
Priority not set or invalid value from the web messenger	If the web developer does not specify a value or specifies an invalid value, the system default priority set at installation time from the deployment excel file is used.
Other Social Channels	The system default priority value set during installation from the deployment excel file is applied to all other channels. For example, WhatsApp, Facebook Messenger.

Limitations

- You cannot specify separate priority values to contacts originating from multiple social channels. For example, the same system default priority applies to contacts originating from WhatsApp, as from the Facebook Messenger.
- The feature does not allow parsing messages from social channels and applying separate priorities.

Chapter 42: Configure the sample Messaging clients

Configure sample Messaging clients

Avaya Oceana® supports the development of :

- Sample Messaging clients
- WhatsApp
- Facebook Messenger
- Twitter Direct Messaging

Note:

Ensure that WhatsApp, Facebook Messenger, and Twitter Direct Messaging are configured on your cloud messaging provider account.

The sample messaging clients, WhatsApp, Facebook Messenger, and Twitter Direct Messaging can be accessed on Web browser, Android, and iOS platforms.

Web browser

For detailed information about how to integrate messaging and conversational capabilities a web messenger, see *Avaya Web Messenger - Development Guide* available on the Avaya DevConnect portal at http://www.avaya.com/devconnect.

Android

For detailed information about how to build In-app messaging applications on android platform, see *Avaya In-App Messaging android SDK - Development Guide* available on the Avaya DevConnect portal at http://www.avaya.com/devconnect.

iOS

For detailed information about how to integrate the In-app messaging iOS SDK to any iOS application, see *Avaya In-App Messaging iOS SDK - Development Guide* available on the Avaya DevConnect portal at http://www.avaya.com/devconnect.

Chapter 43: Verify Messaging contacts

Verify Messaging contacts using Avaya Workspaces

This section describes how to use Avaya Workspaces to verify that the Avaya Oceana® is correctly configured to process Messaging contacts.

Deploying Avaya Workspaces

Procedure

1. Install and commission Avaya Workspaces.

   For information about how to install and commission Avaya Workspaces, see the following documents:

   - *Using Avaya Workspaces for Avaya Oceana®*
   - *Administering Avaya Oceana®*
2. Identify the login details of an agent configured to handle Messaging contacts.

Logging in to Avaya Workspaces

About this task

Use this procedure to log in to Avaya Workspaces to verify access details and agent status.

Procedure

1. Enter one of the following URLs in your web browser:
   - For an Avaya Oceana® deployment that supports up to 100 active agents, enter `https://<AvayaOceanaCluster1_FQDN>/services/UnifiedAgentController/workspaces/#/login`.
   - For an Avaya Oceana® deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, enter `https://<AvayaOceanaCluster2_FQDN>/services/UnifiedAgentController/workspaces/#/login`.
2. On the Agent Login screen, perform the following steps:
   a. In the **Username** field, enter the LDAP username of the agent as configured on the Users page on Avaya Control Manager.

Note:

- Ensure that the agent is configured through Avaya Control Manager to process Messaging contacts.
- Ensure that the agent has appropriate attributes for this test contact.
- To simplify initial verification, ensure that no other agent with Messaging capabilities is logged in. It ensures that the initial test messages are all routed to this agent.

b. In the **Password** field, enter the password of the agent.

c. Click **SIGN IN**.

3. On the Activate Agent screen, click **ACTIVATE**.
4. On the Avaya Workspaces agent interface, in the bottom right corner, verify that the agent state is `CONNECTED`.

Starting work in Avaya Workspaces

About this task

Use this procedure to configure the agent to accept incoming customer Async messages.

Procedure

1. On the Avaya Workspaces agent interface, from the agent status drop-down list, select **StartWork**.
2. In the bottom right corner, verify that the agent state changes to `READY`.

Note:

On the Avaya Workspaces agent interface, when an agent is in the `READY` state, the agent remains available for receiving interactions until the agent is occupied on all channels for which the agent is configured.

Avaya Oceana® provides the following agent states:

- `CONNECTED`: The state of agents when they log in and activate themselves in the Avaya Workspaces or when they click the **Finish Work** button. In this state, agents do not remain available for receiving interactions.
- `Ready`: The state of agents when they click the **Start Work** or **Go Ready** button. In this state, agents remain available for receiving interactions.
- `Not Ready`: The state of agents when they click the **Additional Work** or **Go Not Ready** button. In this state, agents do not remain available for receiving interactions.

If the multiplicity configuration of an agent allows receiving multiple interactions on a channel, the agent remains available for receiving interactions on that channel until the maximum multiplicity is achieved.

Verifying Messaging contact routing to agents

About this task

Use this procedure to verify that the Messaging messages are routed to agents.

Procedure

1. Access the Messaging application using a Messaging account.
2. Send a test message through the application.

   After some time, the system presents the test message to a ready agent.
3. Answer the Messaging contact.

Chapter 44: Configure Outbound

Configure Outbound overview

This section describes how to enable the Outbound voice capability in Avaya Oceana® by integrating Avaya Proactive Outreach Manager (POM) with Avaya Oceana®.

Install and configure POM

To integrate POM with Avaya Oceana®, you must install and configure POM in Oceana mode. For more information, see:

- *Implementing Avaya Proactive Outreach Manager*
- *Avaya Proactive Outreach Manager Integration*

Configuring and exchanging certificates for Proactive Outreach Manager

About this task

You can use this procedure to configure and exchange certificate for Proactive Outreach Manager.

Procedure

1. Log on to the Avaya Experience Portal web console with the Administrator user role.
2. To fetch axis2 certificate at Proactive Outreach Manager, do the following:
   a. In the navigation pane, click **POM** > **POM Home**.
   b. Click **Configurations** > **POM Trusted Certificates**.
   c. Click **Fetch**.
   d. In the **Name** field, type the name of the certificate. For example, axis2.
   e. In the **Location** field, type `https://IPAddress/axis2`.
   f. Click **Continue**.
   g. Click **Save**.
3. To fetch axis2 certificate at AppServer, do the following:
   a. Log on to the AppServer using the `https:/IPAddress:PortNumber/runtimeconfig/` link.

b. In the navigation pane, click **Certificate**.
c. Click **Change**.
d. In the **Keystore path** field, type `/opt/AppServer/Tomcat/tomcat/conf/myTrustStore`.
e. In the **Password** field, type the password.
f. Click **Fetch** to fetch axis2 certificate.
g. In the **Name** field, type the name of the certificate. For example, axis2.
h. In the **Location** field, type `https://IPAddress/axis2`.

4. To generate Experience Portal certificate, do the following:
   a. On the AppServer Home page, click **Certificate**.
   b. On the **Root Certificates** tab, click **Generate** and generate the certificate.
   c. Click **Export** and export the Experience Portal certificate.
5. To generate Proactive Outreach Manager certificate, do the following:
   a. In the navigation pane, click **POM** > **POM Home** .
   b. Click **Configurations** > **POM Servers**.
   c. To add the POM server, click **Add**.
   d. Type the POM server name and IP address.
   e. Click **Continue**.
   f. Select the **Trust this certificate** check box.
   g. Click **Save**.
   h. Click **Export** and export the Proactive Outreach Manager certificate.
6. To generate AppServer certificate, do the following:
   a. Click **Generate**.
   b. In the **Alias** field, type `AppServer`.
   c. In the **Common Name** field, type `AppServer`.
   d. In the **Organization Unit** field, type `OrganizationName`.
   e. In the **Organization** field, type `OrganizationName`.
   f. In the **City** field, type the name of the city.
   g. In the **State** field, type the name of the state.
   h. In the **Country** field, type the name of the country.
   i. In the **SAN** field, type `IP:IPAddress or DNS:HOSTNAME`.
   j. Select SHA256 with RSA, key size 2048 OR SHA1 with RSA, key size 1024.

k. Click **Continue**.
l. Click **Export**.
m. Click **Save**.

7. To add Proactive Outreach Manager certificate to Experience Portal, do the following:
   a. In the navigation pane, click **Certificates**.
   b. On the **Trusted Certificates** tab, click **Upload**.
   c. In the **Name** field, type `POMName`.
   d. In the **Type** field, select **application**.
   e. Browse to the location of the POM certificate and select the file.
   f. Click **Continue**.
   g. Click **Save**.
8. To add AppServer certificate to Experience Portal, do the following:
   a. In the navigation pane, click **Certificates**.
   b. In the **Trusted Certificates** tab, click **Upload**.
   c. In the **Name** field, type `AppServer`.
   d. In the **Type** field, select **application**.
   e. Browse to the location of the AppServer certificate and select the file.
   f. Click **Continue**.
   g. Click **Save**.
9. To add the Experience Portal certificate to Proactive Outreach Manager, do the following:
   a. In the navigation pane, click **POM** > **POM Home** .
   b. Click **Configurations** > **POM Trusted Certificates**.
   c. To import the certificate, click **Import**.
   d. In the **Name** field, type a unique certificate name.
   e. Click **Browse** and locate the Experience Portal file on the local system.
   f. Click **Continue**.
10. To add the AppServer certificate to Proactive Outreach Manager, do the following:
    a. In the navigation pane, click **POM** > **POM Home** .
    b. Click **Configurations** > **POM Trusted Certificates**.
    c. To import the certificate, click **Import**.
    d. In the **Name** field, type a unique certificate name.
    e. Click **Browse** and locate the AppServer certificate file on the local system.

f. Click **Continue**.

11. Add Experience Portal and Proactive Outreach Manager certificates to AppServer.
12. Restart Proactive Outreach Manager after exchanging certificates.

    If there is an issue with Appserver certificate, then restart the AppServer.

Configuring the POM server certificate for Avaya Oceana® Cluster 3

Before you begin

Log in to the POM server web interface and export POM server certificate. For more information, refer Configuring and exchanging certificates for Proactive Outreach Manager on page 646.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select the check box for one of the nodes of Avaya Oceana® Cluster 3, and click **More Actions** > **Manage Trusted Certificates**.
3. On the Manage Trusted Certificates page, click **Add**.
4. On the Add Trusted Certificate page, perform the following steps:
   a. Click **Import from file**.
   b. In the **Please select a file** field, click **Browse**.
   c. In the Choose File to Upload dialog box, browse to the POM server certificate, and then click **Open**.
   d. Click **Retrieve Certificate**.
   e. Click **Commit**.
5. Repeat Step 2 to Step 4 for the other node of Avaya Oceana® Cluster 3.
6. Click **Done**.

Configuring an Outbound provider

About this task

Use this procedure to create a new Outbound provider through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.

3. On the Avaya Oceana Server List page, do one of the following:
   - Double-click the administered Avaya Oceana® server.
   - Select the administered Avaya Oceana® server and click **Edit**.
4. Select the **Providers** tab.
5. Click **Add**.
6. In the **Type** field, select **Outbound**.
7. In the **Name** field, keep the value `POM`.
8. In the **Address** field, enter `POM`.
9. Click **Save**.
10. Restart the clusters to make the new provider available to Avaya Workspaces agents.

Adding Disposition Codes for Outbound contacts

About this task

Use this procedure to add Disposition Codes for Outbound contacts through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Reason Codes**.
2. Select the **Disposition Codes** tab.
3. Click **Add**.
4. Perform the following steps:
   a. In the **Name** and **Number** fields, enter the name and number of the Completion Code configured on the POM server.

      Important:

      - The complete list of Avaya Oceana® Outbound Disposition Codes must match the complete list of POM Completion Codes. It implies that both numeric codes and text must match.
      - A POM Completion Code is automatically generated. Therefore, Completion Codes must be added to the POM server before adding them to Avaya Oceana® through Avaya Control Manager.
      - When creating a POM campaign, the campaign must contain the complete list of all POM Completion Codes.

- In POM-Avaya Oceana® integration, Avaya Workspaces displays all Completion Codes that are configured in Avaya Control Manager.

b. In the **Contact Type** field, select the **Outbound** check box.

c. Click **Save**.

Creating a user to handle Outbound contacts

About this task

Use this procedure to create an agent to handle Outbound contacts.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.
3. Select the location for your Avaya Oceana®.
4. Perform one of the following steps:
   - Click **Add**.
   - Select an existing user and click **Edit**.
5. Enter appropriate value in each of the following fields:
   a. In the **First Name (English)** field, enter the first name of the user in English.
   b. In the **Surname (English)** field, enter the surname of the user in English.
   c. In the Available applications section, select the **Avaya Oceana** check box.
   d. In the **LDAP Username** field, enter the LDAP user name of the user.

      The LDAP user name must be in the username@domain.com format. This user name is used to log on to Avaya Workspaces.
   e. In the **Username** field, enter a user name.

      In this release, the user name is the internal handle.
   f. In the **Password** field, enter a password.

      This password is used to log on to Avaya Control Manager.
   g. In the **Confirm Password** field, re-enter the password.
   h. In the **Extension** field, enter the station associated with this agent.

      This is used when logging on to Avaya Workspaces.
   i. In the **AVAYA Login** field, enter the Elite agent login ID only if the agent also supports Voice contacts. Otherwise, leave this field blank.

j. Click **Save**.

6. Scroll to the right and select the **Avaya Oceana** tab.
7. Select the **Outbound** check box.

Important:

- Outbound users can have only Outbound account.
- Avaya Oceana® supports Hot Desking for Inbound Voice agents but does not support it for POM Outbound agents.
- To change the channel of an agent while the agent is live, the agent must be logged out and logged in again.

8. Select the **Attributes** tab.
9. Move the attributes from the **Available Attributes** list to the **Agent Attributes** list.

Important:

- Ensure that the attributes assigned to the agent match the attributes configured in POM.
- Do not assign a Work Assignment skill to the user.

10. Click **Save**.

Configuring After Contact Work time

About this task

Use this procedure to configure After Contact Work (ACW) time through Avaya Control Manager.

Important:

Enabling ACW time is a mandatory global setting that impacts all interaction types.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. Either double-click the administered Avaya Oceana® UCA server, or select the administered Avaya Oceana® UCA server and click **Edit**.
4. Select the **System Properties** tab.
5. Expand **After Contact Work**.
6. Select the **Enable After Contact Work** check box.
7. In the **After Contact Work Timer (Seconds)** field, enter the same time as the POM completion timer.

Note:

Avaya Oceana® supports **After Contact Work Timer** settings only up to version 3.8. From version 3.8.1, Avaya Oceana® supports **After Contact Work Timer for Voice (Seconds)** for POM.

8. Click **Save**.

Chapter 45: Verify Outbound contacts

Verify Outbound contacts using Avaya Workspaces

This section describes how to use Avaya Workspaces to verify that the Avaya Oceana® is correctly configured to process Outbound contacts.

Deploying Avaya Workspaces

Procedure

1. Install and commission Avaya Workspaces.

   For information about how to install and commission Avaya Workspaces, see the following documents:

   - *Using Avaya Workspaces for Avaya Oceana®*
   - *Administering Avaya Oceana®*
2. Identify the login details of an agent configured to handle Outbound contacts.

Logging in to Avaya Workspaces

About this task

Use this procedure to log in to Avaya Workspaces to verify access details and agent status.

Procedure

1. Enter one of the following URLs in your web browser:
   - For an Avaya Oceana® deployment that supports up to 100 active agents, enter `https://<AvayaOceanaCluster1_FQDN>/services/UnifiedAgentController/workspaces/#/login`.
   - For an Avaya Oceana® deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, enter `https://<AvayaOceanaCluster2_FQDN>/services/UnifiedAgentController/workspaces/#/login`.
2. On the Agent Login screen, perform the following steps:
   a. In the **Username** field, enter the LDAP username of the agent as configured on the Users page on Avaya Control Manager.

Note:

- Ensure that the agent is configured through Avaya Control Manager to process Outbound contacts.
- Ensure that the agent has appropriate attributes for this test contact.
- To simplify initial verification, ensure that no other agent with Outbound capabilities is logged in. It ensures that the initial test messages are all routed to this agent.

b. In the **Password** field, enter the password of the agent.

c. Click **SIGN IN**.

3. On the Activate Agent screen, click **ACTIVATE**.
4. On the Avaya Workspaces agent interface, in the bottom right corner, verify that the agent state is `CONNECTED`.

Starting work in Avaya Workspaces

About this task

Use this procedure to configure the agent to accept Outbound calls.

Procedure

1. On the Avaya Workspaces agent interface, from the agent status drop-down list, select **StartWork**.
2. In the bottom right corner, verify that the agent state changes to `READY`.

Note:

Avaya Oceana® provides the following agent states:

- `CONNECTED`: The state of agents when they log in and activate themselves in the Avaya Workspaces or when they click the **Finish Work** button. In this state, agents do not remain available for receiving interactions.
- `Ready`: The state of agents when they click the **Start Work** or **Go Ready** button. In this state, agents remain available for receiving interactions.
- `Not Ready`: The state of agents when they click the **Additional Work** or **Go Not Ready** button. In this state, agents do not remain available for receiving interactions.

Verifying Outbound contact routing to agents

About this task

Use this procedure to verify that the Outbound contacts are routed to agents.

Before you begin

1. Commission the POM server and configure it to connect to Avaya Oceana®.

2. Configure attributes in Avaya Oceana® and assign them to the Outbound agent.
3. Configure a campaign on the POM server and ensure that all Completion Codes are added.

   The campaign must contain skills that match the attributes for the Outbound agent. The campaign must be predictive or progressive.
4. Enable the Publish Attempt Data To Context Store flag under the Context Store option while creating a campaign.

Procedure

1. Log in to Avaya one-X® Agent or Avaya one-X® Communicator.
2. Log in an agent with Outbound channel to Avaya Workspaces and ensure that agent is ready to handle Outbound calls.
3. Log in to the POM server and start the POM campaign.
4. Answer the nail up call on the agent station.
5. Answer the customer call on the customer phone and ensure that the work card appears on the agent work space.
6. Release the Outbound contact, select a Disposition Code, and then complete the ACW timer.

Chapter 46: Avaya Workspaces for Avaya Oceana® logging

Logs

Each Avaya Breeze® platform node has a log file for all the SVARs deployed on a cluster. If a cluster has two nodes, examine the log files on both nodes.

Avaya Oceana® stores logs for Avaya Workspaces at `/var/log/Avaya/services/Service_Name` for the following services:

- AuthorizationService
- CallEventControl
- EventingConnector
- OceanaMonitorService
- UnifiedAgentContextService
- UnifiedAgentController

Downloading the Avaya Workspaces logs

Procedure

1. Log in to Avaya Workspaces.
2. In the navigation pane, click the ⚙ icon.

   The system displays the Settings widget.
3. Click the **LOGS** tab.
4. Select the duration to view the logs.
5. Click one of the following:
   - **DOWNLOAD**: Avaya Workspaces downloads a zip file of the log files to the Downloads folder on your client computer. You can then share or send an email with the logs to your Supervisor or support personnel.
   - **UPLOAD**: Avaya Workspaces automatically uploads a zip file of log files to a pre-configured central storage location that your administrator sets. Note the date and time

when you click **UPLOAD**. You must share the date and time of the upload with your Supervisor or support personnel so that they can identify and retrieve the logs.

Modifying the logging configuration

About this task

Use the Logging Configuration page to change the logging level of an installed server on Avaya Breeze® platform servers or a cluster. You can also clear the logs for an installed service.

The log level for a snap-in does not persist when you:

- Upgrade the Avaya Breeze® platform servers on which you install the snap-in.
- Reinstall the snap-in.

Procedure

1. On the System Manager web interface, click **Elements** > **Avaya Breeze®** > **Configuration** > **Logging**.
2. On the Logging Configuration page, do the following:
3. In the **Cluster** field, select the cluster to apply the log level.
4. In the **Server** field, select the server to apply the log level.
5. In the **Service** field, select the snap-in to change the logging level.
6. In the **Log Level** field, select the logging level of the snap-in that you selected.

   The system displays the clusters and instances where the snap-in is loaded.
7. Click **Set Log Level**.
8. To clear the logs of the selected snap-in, click **Clear Logs**.

Chapter 47: Deploy Avaya Oceana® for High Availability

Avaya Oceana® High Availability overview

Avaya Oceana® provides the Campus High Availability (HA) functionality. Using this functionality, Avaya Oceana® can automatically recover from a single point of failure.

Note:

In this chapter, the terms virtual machine and node refer to a virtual server that hosts the Avaya Breeze® platform.

This functionality provides mitigation for the following failure scenarios:

- A single Avaya Oceana® process outage at a time.
- A single virtual machine outage at a time.
- A single physical server outage at a time.
- A single network link outage at a time.

The following are the advantages and limitations of Avaya Oceana® HA:

- Avaya Oceana® successfully processes new contacts after the outage.
- Agents and supervisors successfully operate after the outage.
- Loss of active and queued contacts and sessions can occur during the outage.
- Avaya Analytics™ reports can contain incorrect or missing metrics after the outage.
- The outage period counts the time taken to detect the failure and the time taken to fail over to backup processes.

The following table lists the concepts used in Avaya Oceana® HA:

Concept	Description
Failure Event	Specifies one of the following single failure scenarios: • Failure of a single process. • Failure of a single virtual machine. • Failure of a single physical server. • Failure of both network links to a virtual machine. • Failure of all network links to a single physical server.
Network Failure	Specifies one of the following network failures: • Failure of all network links to a virtual machine. For example, the failure of a virtual network adaptor on a virtual machine isolates the virtual machine from the network. • Failure of all network links to a single physical server. For example, the failure of all network adaptors on a physical server isolates the physical server from the network. Avaya Oceana® does not detect the network latency directly. The Avaya Breeze® platform detects all severe network issues and triggers a failover of the virtual machine or process. When a network failure isolates a virtual machine or a physical server from the network, manual intervention is required before the virtual machine or physical server can reconnect to the network. When a network failure isolates a virtual machine or a physical server from the network, Avaya Oceana® identifies and shuts down WAS and GigaSpaces on the isolated virtual machine or physical server.
Process Failure	Specifies the failure of a single process in Avaya Oceana®. For example, the failure of the WebSphere Application Server process or a GigaSpaces PU instance.
Server Failure	Specifies the failure of a single virtual machine or a single physical server. This failure implies that all process instances within the virtual machine or the physical server are lost.

Avaya Oceana® only supports a single failure event. Therefore, if two simultaneous failure events occur, Avaya Oceana® components cannot operate in HA mode.

Avaya Oceana® supports HA in the following failure scenarios:

- Network failure on the physical server hosting the Avaya Oceana® Cluster 3 - Avaya Breeze® platform node (Active Load Balancer) and Active Omnichannel Database.
- Power failure on the physical server hosting the Avaya Oceana® Cluster 3 - Avaya Breeze® platform node (Active Load Balancer) and Active Omnichannel Database.
- Network failure on the physical server hosting the Avaya Oceana® Cluster 2 - Avaya Breeze® platform node (Active Load Balancer).
- Power failure on the physical server hosting the Avaya Oceana® Cluster 2 - Avaya Breeze® platform node (Active Load Balancer).

- Network failure on the physical server hosting the Avaya Oceana® Cluster 1 - Avaya Breeze® platform node (Active Load Balancer and Database), Active Application Enablement Services, and Active Communication Manager.
- Power failure on the physical server hosting the Avaya Oceana® Cluster 1 - Avaya Breeze® platform node (Active Load Balancer and Database), Active Application Enablement Services, and Active Communication Manager.

Recovery from failure scenarios

The following table lists the recovery mechanism for different failure types:

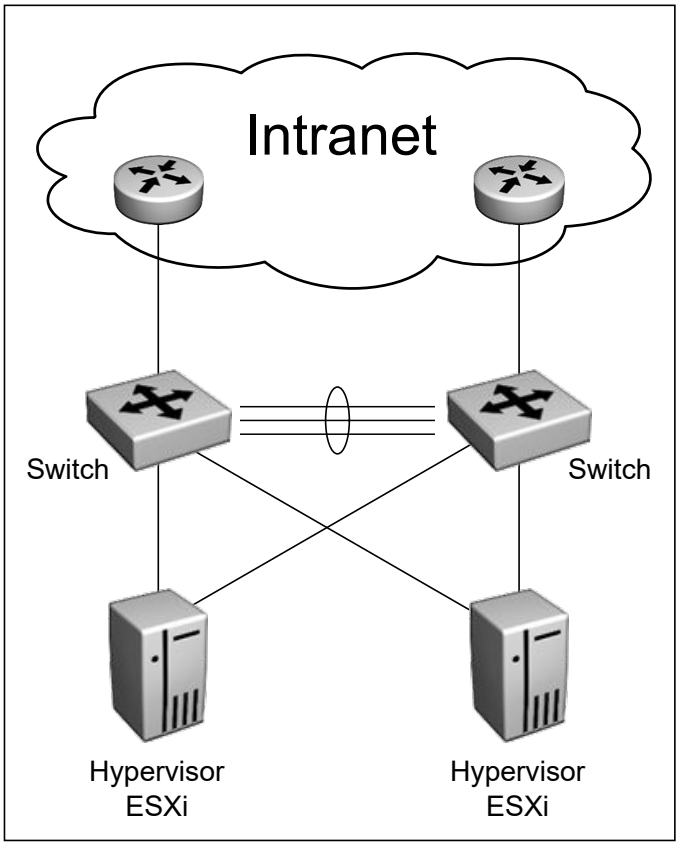
Failure type	Recovery mechanism	Notes
Process Failure For example GigaSpaces PU failure, WebSphere process failure, and Nginx process failure	Automatic	-
Virtual Machine Failure For example accidental shutdown	Manual	If an Avaya Breeze® platform node in an Avaya Oceana® cluster becomes faulty or is shut down for testing, you must reboot all nodes in the cluster after the recovery of the node. The reboot is mandatory to: • Reload SVARs on all nodes • Re-balance the SVAR Gigaspaces Processing Units (PUs) across all nodes Rebooting all nodes in the cluster causes an outage of Avaya Oceana®. Therefore, you must plan the reboot during a maintenance window.
Physical Server Failure For example power failure on a physical server.	Automatic	After you clear the fault and restart the physical server and virtual machines.
Network Failure For example accidental disconnection of all network cards of a physical server.	Manual	Recommission the physical server or the virtual machine. **Note:** • For agents with active interactions, you must reboot all clusters. • For an active agent and network failure on an active UAC node, you must reboot UAC cluster. • After recommission, the agents must refresh the page and re-login if required.

With the Avaya Oceana® Release 3.8, you do not need to restart all the Avaya Oceana® clusters if you have to restart an individual cluster. If you want to restart Unified Agent Controller (UAC) cluster, the agents must not have any contacts. If the agents are having contacts and you restart UAC cluster, then you must restart all the clusters in the following order:

1. Core cluster
2. UAC cluster
3. OCP cluster

In Avaya Oceana®, you must deploy virtual machines within a network configuration that does not have a single point of failure.

The following diagram depicts a network configuration of two physical servers hosting virtual machines:



In this configuration:

- Each physical server is configured with two Network Interface Cards (NICs).
- Each NIC on each physical server is connected to a separate switch.
- Each switch is connected to the company’s intranet through separate routers or switches.

In this configuration, a single failure of a cable, NIC, switch, or router does not impact the network connectivity of virtual machines.

Avaya Control Manager HA

Avaya Control Manager supports full HA. For more information, see *Application Notes for Installing and Configuring Avaya Control Manager Enterprise Edition in a High Availability mode*.

The Avaya Control Manager HA environment consists of two Avaya Control Manager application servers and two Avaya Control Manager MS-SQL Database servers that are deployed in an Active/Active mode.

Omnichannel Provider HA

To support Omnichannel Provider (OCP) HA, you must deploy Omnichannel Avaya Breeze® platform components on a cluster with two Avaya Breeze® platform nodes. OCP operates with a single node only if an outage occurs in one of the nodes.

Omnichannel Avaya Breeze® platform components support service continuity. Therefore:

- The system automatically recovers from any single failure.
- When an outage occurs, an agent cannot process work for maximum 90 seconds.
- On recovery, the agent can continue to process incoming interactions.
- Preservation of existing work depends on the type of the failure.
- If an agent loses control of an existing interaction, the agent can clear the existing interaction and process the next interaction.

Omnichannel Database HA

Omnichannel Database utilizes the Cache mirroring feature for Campus HA. A mirror can provide HA through automatic failover where a failure of the Cache instance causes the other instance to take over automatically.

All Omnichannel Database clients connect to the active mirror through a Virtual IP address, which is always bound to an interface on the currently active database.

When you configure Omnichannel Database, you can do data mirroring with one of the following:

- HA active and standby Omnichannel Database servers within one Avaya Oceana® site (Data Center 1) with automatic failover

  In this configuration, you do not have a geo-redundant backup.
- Active Omnichannel Database server in Data Center 1 and Geo backup Omnichannel Database server in the geo-redundant site (Data Center 2) with no automatic failover

  For information about this configuration, see *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.

- HA active and standby Omnichannel Database servers within Data Center 1 with automatic failover and Geo backup Omnichannel Database server in Data Center 2 with no automatic failover

  For information about this configuration, see *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.

In Omnichannel Database HA, Omnichannel Database:

- Records the transcripts of Chat, Email, Messaging, SMS, and Social sessions for Customer History at the end of the interaction.
- Requires its deployment in an active-standby configuration on separate physical servers in the same subnet with a Round Trip Time (RTT) less than 120ms.
- Automatically switches over to the standby server during outage of the active server or lack of communication from the active server. After the switchover, the standby server becomes the active server.

  Data on the standby server remains updated in real time.

Reinstate the Omnichannel Database HA after failure

If the Omnichannel server or the Cache application on one of the servers goes down, you must either startup or restart the server.

Omnichannel Database HA configuration checklist

Use the following checklist to configure Omnichannel Database HA:

No.	Task	Description	✔
1	Retrieve the certificate files.	See Retrieve certificate files on page 665.	
2	Export the Certificate Authority file	See Exporting the Certificate Authority file on page 665.	
2	Install the Arbiter service on the Avaya Control Manager application server.	See Installing the Arbiter service on page 665.	
3	Configure Cache Mirroring on the active Omnichannel Database server.	See Configuring Cache Mirroring on the active Omnichannel Database server on page 666.	
4	Configure Cache Mirroring on the standby Omnichannel Database server.	See Configuring Cache Mirroring on the standby Omnichannel Database server on page 668.	
5	Configure the **Omnichannel Database Address** attribute with the Virtual IP address of Omnichannel Database for the OCP services.	See Setting the Omnichannel Database Address attribute for HA on page 670.	

Table continues…

No.	Task	Description	✔
6	Configure the **Omni Channel Database Server** field with the Virtual IP address of Omnichannel Database in Avaya Control Manager.	See Configuring the Omnichannel Database address in Avaya Control Manager on page 671.	
7	Secure the Cache Mirror on the Omnichannel Database servers using TLS.	See Securing the Cache Mirror on the Omnichannel Database servers on page 671.	

Retrieve certificate files

To retrieve the certificate files, do the following:

- For information on generating CSR file and the private key file, see Creating a Certificate Signing Request on page 208.
- For information on generating X.509 certificate from the CSR file, see Creating a certificate from a CSR on page 209.

Exporting the Certificate Authority file

Procedure

1. Log into Avaya Aura® System Manager.
2. Navigate to **Services** > **Security** > **Certificates** > **Authority**.
3. On the left pane, click **Public Web**.
4. In the **Retrieve** area, click **Fetch CA Certificates**.
5. Click **Download as PEM**.
6. Save the Certificate Authority file.

Installing the Arbiter service

About this task

Omnichannel Provider (OCP) is deployed with active and standby Omnichannel Database servers. The standby server uses database mirroring to replicate the changes made on the active server. You must deploy the Arbiter service on the Avaya Control Manager application server with which active and standby servers communicate to provide context in a failover scenario.

The configuration of the Arbiter service involves minimal software installation and does not require the installation of Cache.

Important:

The Arbiter service, which is installed on the primary Avaya Control Manager application server, controls the Omnichannel Database failover. If the primary Avaya Control Manager application server is unreachable, the automatic Omnichannel Database failover does not occur until the primary Avaya Control Manager application server is recovered.

Procedure

1. Log in to the Avaya Control Manager server as an administrator.
2. Insert the Omnichannel Database DVD into the DVD drive.
3. Browse to the `<DVD_Drive>\ThirdPartySoftware\IntersystemsCache\ISCAgent` folder.
4. In the folder, double-click the `ISCAgent.msi` file.
5. On the Select Instance screen, keep the default option and click **OK**.
6. On the License Agreement screen, select **I accept the terms in the license agreement** and click **Next**.
7. On the Ready to Install the Program screen, click **Install**.
8. Click **Finish**.
9. Start the Windows Services application by doing the following:
    a. Click **Start** > **Run**.
    b. In the Run dialog box, type `services.msc`.
    c. Click **OK**.
10. In the Services window, do the following:
    a. Double-click the ISCAgent service.
    b. In the Properties dialog box, click **Start**.
    c. In **Startup type**, select **Automatic**.
    d. Click the **Recovery** tab.
    e. In the **First failure**, **Second failure**, and **Subsequent failures** fields, select the **Restart the Service** option.
    f. In the **Reset fail count after** field, type `120`.
    g. In the **Restart service after** field, type `0`.
    h. Click **Apply**.
    i. Click **OK**.

Configuring Cache Mirroring on the active Omnichannel Database server

About this task

Nominate one of the Omnichannel servers to be the active server. If your solution has only one Omnichannel server, then that server is considered as the active server. Take a Cache data backup on the active server and later restore the Cache data on the standby server.

Before you begin

Retrieve the necessary certificate files from Retrieve certificate files on page 665 section if using SSL.

Procedure

1. Start the Windows Services application by doing the following:
    a. Click **Start** > **Run**.
    b. In the Run dialog box, type `services.msc`.
    c. Click **OK**.
2. In the Services window, do the following:
    a. Right-click **ISCAgent service** and select **Start**.
    b. Double-click the **ISCAgent service**.
    c. Click the **General** tab.
    d. In the **Startup type** field, select `Automatic`.
    e. Click the **Recovery** tab.
    f. In the **First failure**, **Second failure**, and **Subsequent failures** fields, select the **Restart the Service** option.
    g. In the **Reset fail count after** field, type `120`.
    h. In the **Restart service after** field, type `0`.
    i. Click **Apply**.
    j. Click **OK**.
3. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
4. Right-click the `OceanaDataManagementTool.exe` file and click **Run as administrator**.
5. Navigate to **Configuration** > **Mirror Settings** > **Create Mirror**.
6. Enter the details for the attribute **Arbiter address**, **Virtual IP address**, **Network Interface** and **Subnet Mask**.
7. To setup **SSL** select the **Require SSL/TLS** checkbox.
    a. In the **File containing trusted Certificate Authority X.509 certificate** field, enter the location of your CA certificate.
    b. In the **File containing this configuration's X.509 certificate** field, browse and select the server certificate.
    c. In the **Private key type password** field, enter the new password.
    d. In the **Private key password** field, enter the new password..
8. Click **Save**.
9. In the Oceana Data Management utility, click **Backup And Restore**.

10. In the navigation pane, click **Backup And Restore**.
11. In the **Select/create file to backup to** field, click **Browse**.
12. On the Save As screen, do the following:
    a. Select the location where you want to save the backup file.

       Do not save the backup file to the software, journal, or multimedia drive.

    b. Specify a name for the backup file. When naming the file, use English or numeric characters only.
    c. Click **Save**.
13. Click **Backup Database**.

    The utility displays the `Backup complete!` message when the backup process is complete.
14. Verify that the backup file is created at the specified location.

Configuring Cache Mirroring on the standby Omnichannel Database server

About this task

Nominate one of the Omnichannel servers to be the standby server. Take a Cache data backup on the active server and later restore the Cache data on the standby server.

Before you begin

Retrieve the necessary certificate files from Retrieve certificate files on page 665 section if using SSL.

Procedure

1. Start the Windows Services application by performing the following steps:
    a. Click **Start** > **Run**.
    b. In the Run dialog box, type `services.msc`.
    c. Click **OK**.
2. In the Services window, do the following:
    a. Right-click **ISCAgent service** and select **Start**.
    b. Double-click the **ISCAgent service**.
    c. Click the **General** tab.
    d. In the **Startup type** field, select `Automatic`.
    e. Click the **Recovery** tab.
    f. In the **First failure**, **Second failure**, and **Subsequent failures** fields, select the **Restart the Service** option.

g. In the **Reset fail count after** field, type `120`.

h. In the **Restart service after** field, type `0`.

i. Click **Apply**.

j. Click **OK**.

3. Navigate to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
4. Right-click the `OceanaDataManagementTool.exe` file and click **Run as administrator**.
5. Navigate to **Configuration** > **Mirror Settings** > **Join Mirror**.
6. In the **Type** field select **Failover**.
7. Type the **Agent Address on Other System** and select the **Network Interface** and mirror **Type**.
8. If SSL is configured on Primary server select the **Require SSL/TLS** checkbox here.
   a. In the **File containing trusted Certificate Authority X.509 certificate** field, enter the location of your CA.
   b. In the **File containing this configuration's X.509 certificate** field, browse and select the server certificate.
   c. In the **File containing associated private key** field, browse and select the certificate key file.
   d. In the **Private key password** field, enter the new password.
9. Click **Save**.
10. In the Oceana Data Management utility, click **Backup And Restore**.
11. In the navigation pane, click **Backup And Restore**.
12. In the **Select file to restore from** field, click **Browse**.
13. On the Open dialog box, do the following:
    a. Browse to the location where you stored the backup file.
    b. Select the backup file.
    c. Click **Open**.
14. Click **Restore Database**.
15. Click **Restore**.

    Click **Yes** when the utility displays the message `Are you restoring a mirrored backup`.

    The utility displays the `Restore complete!` message after the restore process is completed.
16. To verify whether the restore was successful, do the following:
    a. On Cache Management Portal, click **System Operation** > **Mirror Monitor**.

b. Click **Details**.

Verify both Avaya Oceana® databases in the list.

Setting the Omnichannel Database Address attribute for HA

About this task

Use this procedure to configure the **Omnichannel Database Address** attribute with the virtual IP address of Omnichannel Database for the Omnichannel Provider (OCP) services. You can also configure the **Omnichannel Database Address** attribute for all OCP services by configuring this attribute in the OceanaConfiguration service.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In the **Cluster** field, click Avaya Oceana® Cluster 3.
   b. In the **Service** field, click **AgentControllerService**.
3. For **Omnichannel Database Address**:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, enter the FQDN or virtual IP address of the Omnichannel Database.
4. Click **Commit**.
5. Repeat Step 2 to Step 4 for the following services:
   - AutomationController
   - CustomerControllerService
   - EmailService
   - GenericChannelAPI
   - MessagingService
   - ORCRestService
   - OceanaDataViewer
   - CoBrowse
6. Restart all Avaya Breeze® platform nodes of Avaya Oceana® Cluster 3.
7. On the Service Clusters tab, do the following:
   a. In the **Cluster** field, click Avaya Oceana® Cluster 1.
   b. In the **Service** field, click **OCPDataServices**.

8. For **Omnichannel Database Address**:
    a. Select the **Override Default** check box.
    b. In the **Effective Value** field, enter the virtual IP address of Omnichannel Database.
9. Click **Commit**.
10. Restart all Avaya Breeze® platform nodes of Avaya Oceana® Cluster 1.

Configuring the Omnichannel Database address in Avaya Control Manager

Procedure

1. Log on to Avaya Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. Double-click the **UCAServer** instance, or click **Edit**.
4. Select the **System Properties** tab.
5. Expand **Omni Channel**.
6. In the Omni Channel Database section, perform the following steps:
    a. In the **Omni Channel Database Server** field, enter the Virtual IP address of Omnichannel Database.
    b. In the **Omni Channel Database Server Port Number** field, keep the default port number as 57772.
7. Click **Save**.

Securing the Cache Mirror on the Omnichannel Database servers

About this task

Use this procedure to secure the Cache Mirror on the active and standby Omnichannel Database servers using TLS.

Before you begin

- Configure Cache Mirroring on the active Omnichannel Database server.
- Ensure that the same CA signs the certificates for the active and standby servers.
- Ensure that the certificates for the active and standby servers are part of the Trusted Root Certificate Authorities.
- Do not specify the revocation list while entering certificates details because the revocation list is optional.

Procedure

1. On Primary server do the following:
    a. Navigate to the **OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement** folder.

b. Double-click the `OceanaDataManagementTool.exe` configuration file.

c. Go to **Configuration** > **Mirror Settings** > **Create Mirror**.

d. Select the **Require SSL/TLS** check box.

- In the **File containing trusted Certificate Authority X.509 certificate** field, enter the location of your CA.
- In the **File containing this configuration's X.509 certificate** field, browse and select the server certificate.
- In the **File containing associated private key** field, browse and select the key.
- In the **Private key password field**, enter the new password.

e. Click **Save** or **Update** button.

2. Go to standby sever and do the following:

a. Navigate to the **OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement** folder.

b. Double-click the `OceanaDataManagementTool.exe` configuration file.

c. Go to **Configuration** > **Mirror Settings** > **Create Mirror**.

d. Select the **Require SSL/TLS** check box.

- In the **File containing trusted Certificate Authority X.509 certificate** field, enter the location of your CA.
- In the **File containing this configuration's X.509 certificate** field, browse and select the server certificate.
- In the **File containing associated private key** field, browse and select the key.
- In the **Private key password field**, enter the new password.

e. Click **Save** or **Update** button.

3. Go back to Primary server:

a. In your web browser, enter the following URL to open Cache Management Portal:

http://<DC1OmnichannelServerIP>:57772/csp/sys/UtilHome.csp

<DC1OmnichannelServerIP> is the IP address of the active Omnichannel Database server

in Data Center 1.

b. On the Cache Management Portal login page, do the following:

- In the **User Name** field, type the user name.
- In the **Password** field, type the password.
- Click **Login**.

c. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Edit Mirror**.

d. On the Edit Mirror page, look for **Pending New Members** section.

e. Tick the async server and select **Authorize**.

f. . Select **Ok**.

Removing Cache Mirroring from the standby Omnichannel Database server

Procedure

1. In your web browser, enter the following URL to open Cache Management Portal:

   `http://<StandbyOmnichannelServerIP>:57772/csp/sys/UtilHome.csp`

   <StandbyOmnichannelServerIP> is the IP address of the server containing the standby Omnichannel Database.

2. On the Cache Management Portal login page, do the following:

   a. In the **User Name** field, type `_admin`.

   b. In the **Password** field, type `Oceana16`.

   c. Click **LOGIN**.

3. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Remove Mirror Configuration**.

4. Click **Remove**.

5. For **Remove mirror** attribute, select `Yes`.

6. Restart the Windows Omnichannel Database server.

7. Remove any Journal files beginning with MIRROR in `E:\AVAYA\OCEANA\DATABASES\JOURNAL` where E represents the Journal drive.

Removing Cache Mirroring from the active Omnichannel Database server

Procedure

1. In your web browser, enter the following URL to open Cache Management Portal:

   `http://<ActiveOmnichannelServerIP>:57772/csp/sys/UtilHome.csp`

   <ActiveOmnichannelServerIP> is the IP address of the server containing the active Omnichannel Database.

2. On the Cache Management Portal login page, do the following:

   a. In the **User Name** field, type `_admin`.

   b. In the **Password** field, type `Oceana16`.

   c. Click **LOGIN**.

3. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Edit Mirror** > **Remove Mirror Configuration**.
4. On the Remove Mirror Configuration page, click **Clear JoinMirror Flag**.
5. On the server, right-click the **Cache** icon on the toolbar and click **Stop Cache**.
6. Click **Restart**.
7. On Cache Management Portal, click **System Administration** > **Configuration** > **Mirror Settings** > **Edit Mirror** > **Remove Mirror Configuration**.
8. Remove any Journal files beginning with MIRROR in `E:\AVAYA\OCEANA\DATABASES\JOURNAL` where E represents the Journal drive.

Recommissioning physical servers or virtual machines after a network outage

About this task

If a network outage occurs for a single virtual machine or a single physical server, use the following procedure before reconnecting the virtual machine or physical server to the network.

Procedure

1. Connect a monitor, a keyboard, and a mouse to the physical server that is isolated from the network.
2. Log in to the ESXi console.

   You can press **F2** and enter the login credentials.
3. On the System Customization screen, scroll to **Troubleshooting Options** and press **Enter**.
4. **(Optional)** On the Troubleshooting Mode Options screen, scroll to **Enable ESXi Shell** and press **Enter**.

   You can skip this step if ESXi Shell is already enabled.
5. Keep pressing **Esc** until you return to the main direct console screen.
6. On the main direct console screen, press **Alt+F1** to open a local console window to the physical server.
7. Run the following command to list all virtual machines that are hosted on the physical server:

   ```
   vim-cmd vmsvc/getallvms
   ```
8. Identify the ID of the virtual machine that is affected because of the network outage.
9. Run the following command to restart the affected virtual machine:

`vim-cmd vmsvc/power.reboot <virtual_machine_ID>`

<virtual_machine_ID> is the ID of the affected virtual machine.

10. Type `exit` to log out of the console.

EU Data Center Deployments

Avaya Oceana® introduces EU Data Center deployments feature that allows the user to determine at installation time if the AWS instance used is US data center or EU Data Center. You can perform the selection in the deployment excel file. After deployment, you cannot make any changes between the data centers. The default selection is US data center. Avaya Oceana® and the Messaging Connector continue to remain on-premise. The overall system operation remains unchanged.

Configuration

The Avaya NPI Ops team must perform this task on behalf of a customer.

Operation

The URL used by the messaging connector is https://api.smooch.io OR https://api.eu-1.smooch.io depending on the system setting.

Scenario	Operation
User selects EU data center	The functionality is unchanged. All API calls are directed to the EU instance.

Limitations

You must select the data center during installation. After selection, you cannot change the data center.

Chapter 48: Configure Oceana Customer Management Tool and Omnichannel Administration Tool

Configuring access to Oceana Customer Management Tool

About this task

Use this procedure to configure access to Oceana Customer Management Tool so that you can open it by clicking the **Launch Customer Management Client** option in Avaya Control Manager.

Important:

This procedure is mandatory because it is the only supported method to open Oceana Customer Management Tool.

Note:

Skip this procedure if you have already configured access to Omnichannel Administration Utility.

Before you begin

Ensure that you install and commission Avaya Control Manager.

Procedure

1. Log on to Avaya Control Manager.
2. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Server Details**.
3. Double-click the **UCAServer** instance.
4. Select the **System Properties** tab.
5. Expand **Omni Channel**.
6. In the **Omni Channel Database Server** field, enter the FQDN of the Omnichannel Windows server.

7. In the **Omni Channel Database Server Port Number** field, enter 443.
8. Select the **Https** check box to have a secure communication between Avaya Control Manager and your Omnichannel Windows server.
9. Click **Save**.

Omnichannel Administration Utility access configuration

Use the following checklist to configure access to Omnichannel Administration Utility so that you can open it by clicking the **Launch OC Database Administration Client** option in Avaya Control Manager.

Important:

This procedure is mandatory because it is the only supported method to open Omnichannel Administration Utility.

No.	Tasks	Description	✔
1	For secure communication between Avaya Control Manager and Omnichannel Windows server	See Configuring access to Omnichannel Administration Utility on page 677.	
2	Generate a certificate `pfx` file	See Generating a certificate pfx file on page 680.	
3	Import the certificate `pfx` file	See Importing certificate pfx file to Omnichannel Database server on page 681.	
4	Export the Certificate Authority file	See Exporting the Certificate Authority file on page 682.	
5	Import the Certificate Authority as Trusted Root Certificate	See Importing the Certificate Authority as a Trusted Root Certificate Authority through the mmc application on page 682.	
6	For non-secure communication between Avaya Control Manager and Omnichannel Windows server	See Performing non-secure communication between Avaya Control Manager and Omnichannel Windows server on page 683.	

Configuring access to Omnichannel Administration Utility

Before you begin

Install and commission Avaya Control Manager.

For more information about how to install Avaya Control Manager, see “Installing Avaya Control Manager” document. For more information on commissioning Avaya Control Manager, see the earlier topics of this chapter.

Procedure

1. Log on to Avaya Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. On the Avaya Oceana Server List page, do one of the following:
   - Double-click the **UCAServer** instance.
   - Select the check box for the **UCAServer** instance and click **Edit**.
4. Click the **System Properties** tab.
5. Expand **Omni Channel**.
6. In the **Omni Channel Database Server** field, enter the FQDN of the Omnichannel Windows server or host name of the virtual IP if using Omni Channel Cache mirroring HA.
7. For a secure communication between Avaya Control Manager and your Omnichannel Windows server, do the following:
   a. In the **Omni Channel Database Server Port Number** field, enter the port number `443`.
   b. Select the **Https** check box.
   c. Click **Save**.

Creating end entities

About this task

End entities are users such as browsers, email clients, or servers. This section assumes that you want to add a server using the default INBOUND_OUTBOUND_TLS end entity profile. This profile is used for client and server authentication.

You must use this procedure if you use System Manager Certificate Authority (CA).

Procedure

1. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
2. In the navigation pane, in the RA Functions section, click **Add End Entity**.
3. In the **End Entity Profile** field, select `INBOUND_OUTBOUND_TLS`.
4. In the **Username** field, enter a user name.

Ensure that you make a note of the user name. This user name is required when creating a certificate for this server.

5. In the **Password (or Enrollment Code)** field, enter a password.

   Ensure that you make a note of the password. This password is required when creating a certificate for this server.

6. In the **Confirm Password** field, re-enter the password.
7. In the **CN, Common name** field, enter the FQDN of the Omnichannel Windows server.
8. In the **DNS Name** field, enter the server FQDN.
9. In the **IP Address** field, enter the server IP address.
10. In the **Main certificate data** section, do the following:
    a. In the **Certificate Profile** field, select the appropriate certificate profile.
    b. In the **CA** field, select the appropriate CA.
    c. In the **Token** field, select **User Generated**.
11. Click **Add**.

Creating a Certificate Signing Request

About this task

A Certificate Signing Request (CSR) is used by a server to apply for an SSL/TLS certificate. Use this procedure to create a CSR using OpenSSL.

Note:

This procedure is a worked example that describes how to create a CSR using OpenSSL. You can also create a CSR by using other options.

Before you begin

Install `openssl`. For more information about how to install `openssl`, see http://openssl.org.

Procedure

1. Log on to the Microsoft Windows Server 2019 (Desktop Experience) for Omnichannel Provider (OCP).
2. Download a Windows version of OpenSSL to this Microsoft Windows Server 2019 (Desktop Experience).
3. Generate a private key using the OpenSSL **`genpkey`** command.
4. Generate a CSR for this key using the OpenSSL **`req`** command.

Sample CSR generation:

```
# generate the private key. This creates a 2048-bit RSA key, which is encrypted
using AES-256.

# The -pass parameter passes in "testing" as the password - consult the OpenSSL
documentation for other ways of doing this.

openssl genpkey -algorithm RSA -out mmdev1.key -aes-256-cbc -pass pass:testing
-pkeyopt rsa_keygen_bits:2048

# generate the CSR.
# The value of the -passin parameter MUST match the password for the private key.
# This generates a CSR called mmdev1.csr.

openssl req -new -in mmdev1.key -key mmdev1.key -passin pass:testing -out
mmdev1.csr
```

Creating a certificate from a CSR

Procedure

1. Connect to Omnichannel Windows Server.
2. Open the CSR file in a text editor such as Notepad.
3. In your web browser, enter the following URL for the System Manager installation of EJBCA:

   `https://<SMGR FQDN>/ejbca`
4. In the navigation pane, in Enroll section, click **Create Certificate from CSR**.
5. In the **Username** field, enter the user name.
6. In the **Enrollment code** field, enter the password or enrollment code.
7. From the text editor, copy the content of the CSR file that is present between the `---BEGIN CERTIFICATE REQUEST---` and `---END CERTIFICATE REQUEST---` lines.
8. Paste the copied content into the list.
9. Click **OK**.

Generating a certificate pfx file

Procedure

1. Create an end entity in Avaya Aura® System Manager. See Creating end entities on page 678.
2. Create a Certificate Signing Request (CSR) file. See Creating a Certificate Signing Request on page 679.

3. Create a certificate from CSR. See Creating a certificate from a CSR on page 680. Download the certificate in PEM format.
4. Open windows command line from the downloaded certificate location.
5. Run the following command, replacing your certificate name with “certname” where appropriate, and also “cache” key with the key file you used in step 2.

   ```
   openssl pkcs12 -export -out certname.pfx -inkey cache.key -in certname.pem
   ```

Importing certificate pfx file to Omnichannel Database server

Procedure

1. Log on to the Omnichannel Database server.
2. Click **Start** > **Windows Administrative Tools** > **Internet Information Services (IIS) Manager**.
3. In the navigation pane, click the node for Omnichannel Database server.
4. In the content pane, in the IIS area, double-click **Server Certificates**.
5. In the **Actions** pane, click **Import**.

   The **Import Certificate** window opens.
6. In the **Certificate file (.pfx)** field, select the `pfx` file generated for the certificate file.
7. In the **Password** field, provide the password used for the private key.
8. Click **OK**.

Configuring admin certificates for HA

About this task

If you have a campus HA setup you must configure certificates on standby server in case of switchover. Skip this section if you do not have campus HA.

Procedure

1. Repeat Generating a certificate pfx file on page 680 using the standby server details when generating entity.
2. Repeat Importing certificate pfx file to Omnichannel Database server on page 681 where the database server is the standby server.

Exporting the Certificate Authority file

Procedure

1. Log into Avaya Aura® System Manager.
2. Navigate to **Services** > **Security** > **Certificates** > **Authority**.
3. On the left pane, click **Public Web**.
4. In the **Retrieve** area, click **Fetch CA Certificates**.
5. Click **Download as PEM**.
6. Save the Certificate Authority file.

Importing the Certificate Authority as a Trusted Root Certificate Authority through the mmc application

Procedure

1. Log on to Avaya Control Manager server.
2. Run the `mmc.exe` application.
3. Navigate to **File** > **Add/Remove Snap-in**.
4. From the **Available snap-ins:** list, select `Certificates` and click **Add>** to move the snap-ins to the **Selected snap-ins:** list.
5. On the Certificates snap-in page, select `My user account`.
6. Click **Finish**.
7. Click **OK**.
8. Expand **Certificates - Current User** and right-click **Trusted Root Certificate Authority**.
9. Navigate to **All Tasks** > **Import**.

   The **Certificate Import Wizard** opens.
10. Click **Next**.
11. Choose the required option on the **Certificate Import Wizard** and click **Next**.
12. For **File to Import**, in the **File name** field, browse and select the location for file import.
13. Click **Finish**.

Performing non-secure communication between Avaya Control Manager and Omnichannel Windows server

Procedure

1. Log on to Avaya Control Manager .
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. On the Avaya Oceana Server List page, do one of the following:
   - Double-click the **UCAServer** instance.
   - Select the check box for the **UCAServer** instance and click **Edit**.
4. Click the **System Properties** tab.
5. Expand **Omni Channel**.
6. In the **Omni Channel Database Server** field, enter the FQDN of the Omnichannel Windows server.
7. For a non-secure communication between Avaya Control Manager and your Omnichannel Windows server, do the following:
   a. In the **Omni Channel Database Server Port Number** field, enter the port number `80`.
   b. Clear the **Https** check box.
8. Click **Save**.

Enabling SSL for secure browser access

About this task

Secure Sockets Layer (SSL) protocols provide communications security over a computer network. Use the following procedure to enable an SSL secure communication on different web browsers.

Procedure

1. Log on to Windows as administrator.
2. Click **Start** > **Windows Administrative Tools** > **Internet Information Services (IIS) Manager**.
3. In the navigation pane, click the Omnichannel Database server node.
4. Expand the **Sites** folder and select **Default Web Site**.
5. Select **Bindings** from the **Actions** menu on the right side of the screen.

   The system displays the Site Bindings screen.
6. Click **Add**.

   The system displays the Add Site Binding screen.

7. Administer the following parameters:
   - Set **Type** to **https**.
   - Set **IP address** to **All Unassigned**.
   - Set **Port** to **443**.
   - Leave **Host name** blank.
   - In the **SSL certificate** field, click **Select** to browse to the signed certificate you requested from the CA.
8. Click **OK**.

   The system displays the Site Bindings screen showing the HTTPS type.
9. Click **Close**.
10. On the Default Web Site Home page, double-click the **SSL Settings** option.

    The system displays the SSL Settings screen.
11. Select the **Require SSL** option.
12. Select **Apply** from the **Actions** menu on the right side of the screen.
13. You can now exit from the IIS Manager tool.

Starting Oceana Customer Management Tool

About this task

Use this procedure to start Oceana Customer Management Tool from the Avaya Control Manager web interface. Oceana Customer Management Tool (OCMT) is a ClickOnce application. You must open the Oceana Customer Management Tool using the browser with which you downloaded the ClickOnce application.

Before you begin

Ensure that you have downloaded and installed the following:

- OmniDB server certificate in the trust store of the client's machine.
- Root CA certificate used to create the OmniDB certificate in the trust store of the client's machine.
- .Net framework that matches the .Net framework version of the OCMT client on the client's machine.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Omnichannel Administration**.
2. Click **Launch Customer Management Client**.

   The system starts Oceana Customer Management Tool.

Starting Omnichannel Administration Utility

About this task

Use this procedure to start Omnichannel Administration Utility from the Avaya Control Manager web interface.

Note:

If you are using Chrome or Firefox, then a ClickOnce plugin must be installed on the browser before the user launches the Oceana administration client or the OCMT.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Omnichannel Administration**.
2. Click **Launch OC Database Administration Client**.

   Avaya Control Manager starts Omnichannel Administration Utility.

Exporting customer details from Salesforce

About this task

Use this procedure to export customer details from Salesforce by using the Data Loader export wizard. You can export customer data into a CSV file and import the CSV file into Avaya Oceana® using the Oceana Customer Management Tool.

Before you begin

Ensure that you are using a cloud version of Salesforce and the user login has read access to the Salesforce data.

Procedure

1. On your web browser, enter the following URL:.

   `https://login.salesforce.com/`

   Note:

   If you are using a custom domain to log in to Salesforce, specify the domain name in the Salesforce data loader when you log in.
2. On the login screen, enter the user name and password of a user who has read access to the data.
3. In the top right corner, select **Setup** .
4. In the **Quick Find** field, type `Data Loader`.

5. Based on your operating system, click one of the following to download the relevant data loader:
   - Download Data Loader for Windows
   - Download Data Loader for MAC
6. To install the data loader, do the following:
   a. Double-click the downloaded file.
   b. Go through the prompts until the installation is complete.
7. Run the Data Loader.
8. Open the Data Loader and click one of the following:
   - **Export**
   - **Export All**
9. Enter the Salesforce user name and password and click **Log in**.
10. Click **Next** to choose an object.
11. Do one of the following:
    - Select the Account object
    - Click **Show all objects** to see a complete list of objects that you can access
12. Click **Browse** to select the CSV file to which you want to export the data.
13. Click **Next**.
14. Type the query, `SELECT Id,Account.Name, Salutation,FirstName,MiddleName,LastName,Suffix,Email,Phone, HomePhone, MobilePhone, Id, MailingStreet, MailingCity, MailingCountry, MailingState, MailingPostalCode,Languages__c from Contact` to export data from Salesforce.
15. Click **Finish** and then click **Yes** to confirm.
16. Click **View Extraction** to view the exported CSV file.

Customer data import template

The table below lists the customer data fields available as columns in the excel or text file template.

Fields	Description
Phone number	Phone number of the customer. For example, landline. You can enter up to 32 numeric values in this field. **Note:** Either the phone number or an email address is mandatory.
Intl Code	International code of the customer. You can enter up to 10 numeric values in this field.
Area Code	Area code of the customer. You can enter up to 10 numeric values in this field.
CRM ID	The ID of the customer from the primary CRM system. You can enter up to 255 characters in this field.
Social Platform	Social platform such as Facebook or Twitter account's are mapped to customer email address or phone number.
Social Handle	Social handle for a customer matching based on social details.
#2 Phone number	Phone number of the customer. For example, mobile. **Note:** Either the phone number or an email address is mandatory.
#2 Intl Code	International code of the second phone number. You can enter up to 10 numeric values in this field.
#2 Area Code	Area code of the second phone number. You can enter up to 10 numeric values in this field.
#2 CRM ID	The ID of the customer from the second alternative CRM system. You can enter up to 255 characters in this field.
#3 Phone number	Phone number of the customer. **Note:** Either the phone number or an email address is mandatory.
#3 Intl Code	International code of the third phone number. You can enter up to 10 numeric values in this field.
#3 Area Code	Area code of the third phone number. You can enter up to 10 numeric values in this field.
#3 CRM ID	The ID of the customer from the third alternative CRM system. You can enter up to 255 characters in this field.
#4 Phone number	Phone number of the customer. **Note:** Either the phone number or an email address is mandatory.
#4 Intl Code	International code of the fourth phone number. You can enter up to 10 numeric values in this field.

Table continues…

Fields	Description
#4 Area Code	Area code of the fourth phone number. You can enter up to 10 numeric values in this field.
#4 CRM ID	The ID of the customer from the fourth alternative CRM system. You can enter up to 255 characters in this field.
#5 Phone number	Phone number of the customer. **Note:** Either the phone number or an email address is mandatory.
#5 Intl Code	International code of the fifth phone number. You can enter up to 10 numeric values in this field.
#5 Area Code	Area code of the fifth phone number. You can enter up to 10 numeric values in this field.
#5 CRM ID	The ID of the customer from the fifth alternative CRM system. You can enter up to 255 characters in this field.
#1 Social Platform	Social platform such as Facebook or Twitter account's are mapped to customer email address or phone number.
#1 Social Handle	Social handle for a customer matching based on social details.
#2 Social Platform	Social platform such as Facebook or Twitter account's are mapped to customer email address or phone number.
#2 Social Handle	Social handle for a customer matching based on social details.
#3 Social Platform	Social platform such as Facebook or Twitter account's are mapped to customer email address or phone number.
#3 Social Handle	Social handle for a customer matching based on social details.
Email Address	Email id of the customer. The format is abc@xyz.com. You can enter up to 255 characters in this field. **Note:** Either the phone number or an email address is mandatory.
Last Name	Last name or surname of the customer. You can enter up to 50 characters in this field.
First Name	First name of the customer. You can enter up to 50 characters in this field.
Title	Title of the customer. For example, Dr, Mr, Ms. You can enter up to 20 characters in this field.
Address Line #1	Address of the customer. You can enter up to 255 characters in this field.
Address Line #2	Address of the customer. You can enter up to 255 characters in this field.
Address Line #3	Address of the customer. You can enter up to 255 characters in this field.

Table continues…

Fields	Description
Address Line #4	Address of the customer. You can enter up to 255 characters in this field.
Address Line #5	Address of the customer. You can enter up to 255 characters in this field.
Country	Country where the customer resides. You can enter up to 255 characters in this field.
Postal Code	Postal code where the customer resides. You can enter up to 255 characters in this field.
Display name	The name of the account type of the customer. Account type is the type of account associated with the customer for an interaction. For example, social security number, booking reference, support ticket, or subscription number.
Account identifier	Account type of a customer. Customers can add their site specific identifiers to Avaya Oceana®.
Async account identifier handle	Async account identifier is an identifier assigned to the customer when routing messaging contacts. It is unknown for new customers. However, if you want to update existing customers, you can find the identifier on customer search in Avaya Workspaces. You can then use this while updating other customers details using Oceana Customer Management Tool.

Oceana Customer Management Tool

Oceana Customer Management Tool (OCMT) is an application using which you can manually add customer data. You can also use it to import customer data from an external source into Avaya Oceana®.

You can gain access to the components of OCMT from the toolbar on the left of the OCMT window.

Icon	Name	Description
	**Import customer data**	Import customer data from a text file, ODBC, or manually. You can add customer data manually, import data from an external source, edit the data, and export the data.
	**General Settings**	View the log files to track problems in OCMT.
	**Help**	Get information about using OCMT.

Considerations

In a single import, OCMT limits you to import 20000 customers in Avaya Oceana®. However, you can import new sets of customers by repeatedly using OCMT.

There is also a limit on the overall number of customers that the database can store. If there are any contacts that are currently being processed or in queue to agents, OCMT permits only one customer at a time to be imported in Avaya Oceana®. These measures are taken to ensure that OCMT does not impact the normal operation of Avaya Oceana® Contact Center.

In your environment, OCMT is not supported if Round Trip Time (RTT) between the following servers is more than 500 ms:

- The server where OCMT is running
- The Omnichannel Provider server

It is highly recommended to run OCMT in environments where RTT is less than 200 ms.

Account Types

Customer accounts management

Avaya Oceana® provides customer support entered account data to enhance the management of customer accounts. A customer account consists of the following components:

- Account type: The account associated with the customer for an interaction. For example, social security number, booking reference, support ticket, or subscription number. You must specify the account type in Omnichannel Database through Oceana Customer Management Tool (OCMT) before a customer contact forwards the account to Avaya Oceana®.
- Account value: The value that the end customer supplies during the customer's interaction with the Avaya Oceana® contact center.

Avaya Oceana® supports accounts for voice and generic channels only.

- In the voice channel, two methods of orchestrating front-end IVR are Avaya Experience Portal and Avaya Aura® Call Center Elite.

  Note:

  The sample Experience Portal IVR application collects the account value from voice callers. This sample IVR application and the Call Center Elite workflow are available on DevConnect.

  The account is used to retrieve the internal customer ID value associated with the account from the Omnistore database through the CustomerManagementService and OCPDataServices snap-ins. The customer ID value is then used to track the customer interactions using Avaya Context Store Snap-in and the customer journey feature in Avaya Oceana®. The account of the current customer interaction is stored, retrieved, and updated in Avaya Context Store Snap-in through the OceanaCoreDataService, Oceana Pluggable Data Connector, and the Engagement Designer tasks. The information is then retrieved and

updated through the sample Engagement Designer workflows. This enables the customer journey feature to display the account of current customer interaction with the customer's previous interactions in Avaya Oceana®.

- In generic channel support, for each generic contact entered in Avaya Oceana®, an account is specified with the contact, which is then stored in the Oceana Omnistore database. All generic contacts that contain an account are tracked and used by customer journey in the same way as voice interactions.

Warning:

Avaya Oceana® does not validate any customer entered account value or CRM identifier value against data stored in the Omnichannel database. For more details on validation caveats, see *Avaya Oceana® Release Notes*.

Capturing custom data from Avaya Oceana® voice calls

Avaya Context Store Snap-in provides a centralized solution to store contextual information about PSTN voice callers and their contacts. Avaya Context Store Snap-in can store context entries containing several data elements. The following are the key data elements:

- ContextID: A text field containing a unique context identification. You can specify the contextID when adding the context entry in Context Store. Context Store generates a unique id if you do not specify a contextID when creating a context.
- Data: The data field in a context entry is an abstract map with multiple key-value pairs. Keys in the data field must be unique. Multiple identical keys in the same request results in the values being overwritten with the last key.

For more information about other Avaya Context Store Snap-in data elements, see *Avaya Context Store Snap-in Reference*.

Avaya Context Store Snap-in maps the front-end customer’s data model into the Context Store data model. You must consider the type of data and the size of data that you want to store in Context Store. There are several methods to add or update data in Context Store.

If your solution includes Avaya Experience Portal (AAEP), Avaya Oceana® provides a Pluggable Data Connector (PDC) to integrate with AAEP. AAEP uses call flows created in Orchestration Designer (OD) to handle incoming PSTN calls and capture customer data. When you install the Avaya Oceana® PDC in OD, a Context Store Connector node is available in OD. You can use the Context Store Connector node to integrate Avaya Context Store Snap-in into your call flows. You can also configure the Context Store Connector node to perform actions such as creating, getting, updating, or deleting context information using the contextID.

The External Data Mart (EDM) database and Journey PU are the other components of an Avaya Context Store Snap-in deployment. Avaya Context Store Snap-in uses the Journey PU to persist Context Store data to the External Data Mart. Components such as Customer Journey can retrieve the data from the External Data Mart when required and present it to Avaya Oceana® users. Context Store data expires after the predefined Lease Time parameter expires. The Lease Time parameter is configurable, and Context Store preserves a context entry until the lease time expires. Any Avaya Context Store Snap-in client can renew this lease or time-to-live anytime. The default value for lease time is 7200 seconds; you can configure the lease time to be any value between 1 second and 86400 seconds. Clients can also define the lease time when creating a context and specify different lease time values for different scenarios. If a context is accessed after its lease time has expired, it is resurrected into the data grid from the External Data Mart, using the default lease time.

The following rules apply to adding, updating, and deleting Avaya Context Store Snap-in data in an Avaya Oceana® deployment:

- Context Store stores the default standard schema detail. Schema contains caller attributes and Work Assignment related data against a unique contextID.
- You can pass custom data into Context Store using the Data element. For example, a customer's ticket number, location, or interest. Using a customized version of the default Avaya Oceana® AAEP application, you can capture the caller's custom data. You can then insert it into an existing Work Request ID using the Data field of that existing Work Request. In Avaya Oceana®, the Context ID and the Work Request ID are set to the same value. This process assumes that an existing Work Request ID is available to the AAEP application if deployed. In an Avaya Oceana® and AAEP deployment, Context Store can generate the Work Request ID. If you use Elite IVR, the UCID value is used. If you use Elite IVR, AAEP is not required.
- Avaya Oceana® supports data privacy. Custom data is not stored in the EDM database to comply with privacy laws. An administrator can change the default setting if there is a requirement to store custom data.
- You must use a maximum value of 600 Bytes for the custom data field size. To use a larger data field size, contact Avaya Support.

For other Avaya Context Store Snap-in deployments where there is a requirement to add custom data, see *Avaya Context Store Snap-in Developer Guide* and *Avaya Context Store Snap-in Reference*, available on the Avaya Support website at https://support.avaya.com.

Adding new account types to Avaya Oceana®

About this task

Use this procedure to create a display name that is associated with a new account type in Avaya Oceana®. After the account type is created, it gets displayed in the list of available input fields that customers can import or manually enter data.

Note:

- The Avaya Oceana® Omnistore database comes pre-populated with four default account types: Account identifier, Credit card number, Social Security number, and Subscription Identifier.
- You can add up to 16 new custom account types, apart from the four default account types.
- You cannot delete account types that are not associated with a customer.

Procedure

1. On the Oceana Customer Management Tool interface, click **Import customer data**.
2. On the Customer Settings page, click the **Account Types** > **Add**.
3. On the OCMT Insert Account Type window, enter the name and the display name for the account and click **Insert**.

Customer data import

Importing customer data from a text file

About this task

Use this procedure to import customer data from a text file into Oceana Customer Management Tool to save time and prevent data entry errors. If you cannot import customer data through a text file or an ODBC connection, you can manually add the data to Oceana Customer Management Tool.

Procedure

1. On the Oceana Customer Management Tool interface, click **Import customer data**.
2. On the Customer Settings page, click the **Customer Data Import** tab.
3. Click **Import Customer Data To Tool**.

   If the Customer Data table already contains data, Oceana Customer Management Tool displays the OCMT Import Customer Data dialog box.
4. In the OCMT Import Customer Data dialog box, do one of the following:
   - To add data to the existing table, click **Append to Data Table**.
   - To create a new table, click **Clear Data Table**.
5. In the Select Import Type window, select **Import from Text File** .
6. Click **Next**.
7. Click **Browse** to navigate to the appropriate directory.
8. Select the file and click **Open**.
9. Click **Next**.
10. To select how the fields are separated in your source file, click one of the following:
    - **Tab**
    - **Character**

    The default character is a comma.
11. To import a selection of records only from the source file, select the **Enable Record Selection** check box, and then select the beginning and end of the range of records to be imported.
12. If the first row of the source file contains column headers, select the **First row shall contain column headers** check box.
13. Click **Next**.
14. In the Map Data dialog box, do the following:
    a. Drag the first row from the **File Source Fields** area to the appropriate **Mapping** column in the **OCMT Target Fields** area.

b. Check and complete the mapping for the other rows in the **File Source Fields** area.

c. **(Optional)** In the source database table, if the area code or international code or both are in the same field as the telephone number, map that field to **Phone Number** in the **OCMT Target Fields** area.

   You can use the Customer Settings page to split the number into international code, area code, and phone number.

15. Review the **Mapping Results** table.
16. To remove the mapping, select the mapping column in the **OCMT Fields** table and click **Clear Mapping**.
17. Click **Finish**.

Importing customer data from an ODBC database

About this task

Use this procedure to import customer data from an ODBC database into Oceana Customer Management Tool to save time and prevent data entry errors. If you cannot import customer data through a text file or an ODBC connection, you can manually add the data to Oceana Customer Management Tool.

Procedure

1. On the Oceana Customer Management Tool interface, click **Import customer data**.
2. On the Customer Settings page, click the **Customer Data Import** tab.
3. Click **Import Customer Data To Tool**.

   If the Customer Data table already contains data, Oceana Customer Management Tool displays the OCMT Import Customer Data dialog box.
4. In the OCMT Import Customer Data dialog box, do one of the following:
   - To add data to the existing table, click **Append to Data Table**.
   - To create a new table, click **Clear Data Table**.
5. In the Select Import Type dialog box, select **Import from ODBC**.
6. Click **Next**.
7. In the Select DSN dialog box, do one of the following:
   - To select a system or user DSN, select a DSN from the list.
   - To select a file DSN, click the **File DSN** tab and browse to the DSN file.
8. **(Optional)** If the ODBC source requires a login ID, in the **Login Information** section, type the user name and password.
9. Click **Next**.
10. Click the table name or view name from which you want to import customer data and then click **Next**.

11. In the Map Data dialog box, do the following:
    a. Drag the first row from the **Data Source Fields** area to the appropriate **Mapping** column in the **OCMT Target Fields** area.
    b. In the **Data Source Fields** area, check and complete the mapping for the other rows .
    c. **(Optional)** In the source database table, if the area code or international code or both are in the same field as the telephone number, map that field to **Phone Number** in the **OCMT Target Fields** area.

       You can use the Customer Settings page to split the number into international code, area code, and phone number.
12. To remove the mapping, click the **Mapping** column in the **OCMT Target Fields** area and click **Clear Mapping.**
13. To import only a selection of the records from the source file, select the **Select Range** check box, and then select the beginning and end of the range of records to import.

    If the start record is the same as the end record, the data in that record is imported.
14. Click **Finish**.

Adding customer data manually

About this task

Use this procedure to manually add customer data if data is not available in ODBC or text file format.

Procedure

1. On the Oceana Customer Management Tool interface, click **Import customer data**.
2. In **Customer Data Table**, click the first empty row .
3. Type the customer information in the appropriate fields.

Adding custom fields

About this task

Use this procedure to add custom fields to the import data options available in Oceana Customer Management Tool.

Procedure

1. On the Oceana Customer Management Tool interface, click **Import customer data**.
2. On the Customer Settings page, click the **Custom Fields** tab.
3. Click **Add**.
4. In the OCMT Insert Custom Field dialog box, do the following:
    a. In the **Custom Field Name** field, type the name of the custom field.

b. Click **Insert** to insert the custom field to the Customer Data table.

5. **(Optional)** To delete a custom field, do the following:
   a. In the **Custom Field Name** list, select the custom field that you want to delete.
   b. Click **Delete**.
   c. In the OCMT Custom Fields message box, click **Yes**.

Customer data cleanup

Validating customer data

Before you begin

- Add customer data manually or by using an importing method .

Procedure

1. On the Oceana Customer Management Tool interface, click **Import customer data**.
2. Click **Customer Data Cleanup**.
3. On the **Customer Data Cleanup** page, click **Validate Customer Data**.

   The Customer Validation window displays the number of records that failed validation and provides the option to delete or review the records.
4. To review and correct the data, click **Review**.

   The invalid records are highlighted in the table.
5. To delete all invalid records, click **Delete**.

Inserting text

About this task

Use this procedure to insert text into the customer data to replace or change customer details. You can overwrite, prepend, or append the existing text.

Before you begin

Ensure that you have data in the Customer Data table.

Procedure

1. On the Oceana Customer Management Tool interface, click **Import customer data**.
2. Click **Customer Data Cleanup.**
3. Click the **Insert Text** tab.

4. Select one of the text change options:
   - **Overwrite**
   - **Prepend**
   - **Append**
5. In the **Text to Add** box, type the text that you want to append, prepend, or replace in a field.
6. In the **Select Field** field, click a column to change or replace the text.
7. To search for and replace text, do any one the following:
   - To search for and replace text in all rows of the table, click **All Customers**.
   - To search for and replace text in only selected rows of the table, click **Selected Customers**.
8. Click **Insert Text**.
9. Click **Continue** to confirm you want to add the selected text.
10. Click **OK**.

Procedure job aid

Value	Variable
Overwrite	Replace the current contents of the field.
Prepend	Add the text to the beginning of the current text in the field.
Append	Add the text to the end of the current text in the field.
Text to add	Type the text you want to appear.

Removing text

About this task

Use this procedure to remove text that is no longer valid from the Customer Data table .

Before you begin

Ensure that you have data in the Customer Data table.

Procedure

1. On the Oceana Customer Management Tool interface, click **Import customer data**.
2. On the Customer Settings page, click **Customer Data Cleanup**.
3. Click the **Remove Text** tab and do the following:
   - In the **Text to remove** field, type the text that you want to search and remove.
   - To remove all text from the selected column, click **Remove All Text**.
4. In the **Select Field** list, click the column from which to search and remove the text.

5. In the **Occurrence** list, click the option that describes what you want to remove.
6. Do one of the following:
   - To search for and remove text in all rows of the table, click **All Customers**.
   - To search for and remove text in only selected rows of the table, click **Selected Customers**.
7. Click **Remove Text**.
8. Click **Continue** to confirm that you want to delete the selected text.
9. Click **OK**.

Replacing text

About this task

Use this procedure to replace text in your Customer Data table with corrected information in one location or more.

Before you begin

Ensure that you have data in the Customer Data table.

Procedure

1. On the Oceana Customer Management Tool interface, click **Import customer data**.
2. On the Customer Settings page, click **Customer Data Cleanup**.
3. Click the **Replace Text** tab.
4. In the **Text to replace** box, type the existing text that you want to search and replace.
5. In the **Text to replace with** field, type the new text .
6. In the **Select Field** list, click the column from which to search and replace the text.
7. Do one of the following:
   - To search for and replace text in all rows of the table, click **All Customers**.
   - To search for and replace text in only selected rows of the table, click **Selected Customers**.
8. Click **Replace Text**.
9. Click **Continue** to confirm that you want to replace the selected text.
10. Click **OK**.

Splitting a phone number

About this task

Use this procedure to split a phone number in your Customer Data table if the international code or area code is combined with the telephone number in the imported data. You must ensure that the phone number in the Customer Data table is valid by removing a specified number of digits

from the beginning of the Phone Number and adding those digits to the selected Intl or Area Code column.

Before you begin

Ensure that you have data in the Customer Data table.

Procedure

1. On the Oceana Customer Management Tool interface, click **Import customer data**.
2. Click **Customer Data Cleanup**.
3. Click the **Split Phone Number** tab.
4. In the **Split Field into** field, click one of the following:
   - **Intl Code**
   - **Area Code**
5. In **Number of digits to split**, enter the number of digits to remove from the **Phone Number** and add to the selected **Code** column.
6. Do one of the following:
   - To split the phone number in all rows of the table, click **All Customers**.
   - To split the phone number in only selected rows of the table, select the specific rows, and then click **Selected Customers**.
7. Click **Split Phone Number**.
8. Click **Continue** .
9. Click **OK**.

Checking for duplicate customer data

About this task

Use this procedure to check for duplicate records in a field or in fields that you select.

Before you begin

Ensure that you have data in the Customer Data table.

Procedure

1. On the Oceana Customer Management Tool interface, click **Import customer data**.
2. On the Customer Settings page, click **Customer Data Cleanup**.
3. Click **Duplicate Customers**.
4. In the **Select fields** list, select the field or fields where you want to search for duplicate information.
5. Click **Select Duplicate Customers**.

Important:

Duplicates are only found on records that you selected in the Duplicate Field Search. If you do not select all fields, unique records do not appear.

6. Click **Review** to review the duplicate customer records.

   The duplicate customer records are displayed at the top of the table and the second and third or more of each group of duplicate records is highlighted.

7. To allow duplicate customer records to remain, select the duplicate records and click **Allow Selected Duplicates**.

   The **Duplicate Status** column displays **Duplicate Allowed** for the selected duplicate records.

8. To delete the duplicate records, click **Delete**.

   Oceana retains a single copy of each record and deletes the duplicate records.

Customer data search

Checking the length of fields

About this task

Use this procedure to check the length of fields in the Customer Data table to determine the validity of a field in a customer record. For example, you can see which records contain the incorrect number of digits for the telephone number. When the table displays the search results , you can either correct the content of the field or delete the record.

Before you begin

Ensure that you have data in the Customer Data table.

Procedure

1. On the Oceana Customer Management Tool interface, click **Import customer data**.
2. On the Customer Settings tab, click **Customer Data Search**.
3. Click the **Length Search** tab.
4. In the **Select Field** field, click the column on which to search the length.
5. In the **Operation** box, click the mathematical operation that applies to your search:
   - Greater than
   - Equal to
   - Less than
6. In the **Number of digits** box, enter the number of digits that each entry in the column must contain.

7. If you want the length check to ignore spaces, select the **Ignore Spaces** check box.
8. To check the length on specific rows of the table, select the rows, and then click **Selected Customers**.
9. Click **Search**.

   Customer data that matches your criteria is highlighted and moved to the top of the Customer Data table.
10. Do one of the following:
    - Change the data.
    - Delete the rows by clicking **Delete Checked Customers**.

Checking for a value

About this task

Use this procedure to check for fields that contain a specific value in your Customer Data table to ensure that the records are all valid. For example, you can search for records where the telephone numbers are not in your local area.

Before you begin

Ensure that you have data in the Customer Data table.

Procedure

1. On the Oceana Customer Management Tool interface, click **Import customer data**.
2. On the Customer Settings page, click **Customer Data Search**.
3. Click the **Value Search** tab.
4. In the **Select Field** list, click the column on which to do the value search.
5. In the **Operation** field, click the mathematical operation that applies to your value search:
   - Equal to
   - Not equal to
   - Contains
   - Does not contain
6. In the **Select Value** field, type the information that corresponds to the operation and selected field.
7. To check the value on specific rows of the table, select the rows, and then click **Selected Customers**.
8. Click **Search**.

   The Customer Data table displays the customer data that match your on the top.

9. Do one of the following:
   - Change the data.
   - Delete the rows by clicking **Delete Checked Customers**.

Checking for alphabetic characters

About this task

Use this procedure to check the fields for particular alphabetic characters or symbols to correct the data or delete the entire record from the Customer Data table.

Before you begin

Ensure that you have data in the Customer Data table.

Procedure

1. On the Oceana Customer Management Tool interface, click **Import customer data**.
2. On the Customer Settings page, click **Customer Data Search**.
3. Click the **Numeric Search** tab.
4. In the **Select Field** list, click the column on which to check for alphabetic characters.
5. To check the alphabetic character on specific rows of the table, select the rows, and then click **Selected Customers**.
6. Click **Search**.

   Rows that include non-numeric characters in the selected column are highlighted and moved to the top of the table.
7. Do one of the following:
   - Change the data.
   - Delete the rows by clicking **Delete Checked Customers**.

Customer match

The customer match feature indicates a close match to existing customer data in the database. The Administrator can determine whether the information in the customer data table is a new customer, for which you must create a new record, or an existing customer.

For example, if Mike Smith 091 12345 is present in the database, and Michael Smith 091 12345 is in the customer data table, when you run a customer match, the similarities are displayed to the Administrator.

If Enable Partial Match is selected, similarities between the customer data table and the database are shown based on partial matches of the telephone number. For example, if the customer table contains Michael Smith 12345, and the database contains Mike Smith 091 12345, the partial

match highlights the similarities. If Partial Match is not enabled, the entry in the customer data table is considered new.

Important:

It is recommended that you manually resolve any existing customer conflicts.

Checking customer matches

About this task

Use this procedure to determine whether records in the Customer Data table match a customer record.

Before you begin

Ensure that you have data in the Customer Data table.

Procedure

1. On the Oceana Customer Management Tool interface, click **Import customer data**.
2. On the **Customer Settings** tab, click the **Customer Match** tab.
3. To compare information based on a partial phone match, select the **Enable Partial Match** check box.
4. Click **Check Customer Association**.

   The customer data table highlights all records with matching phone numbers. A check box is displayed in the Customer Status column of each row.
5. If there is conflicting information, click the check box in the **Customer Status** column.
6. In the Customer Matching window, compare the Customer Details with the Existing Customer Details.
7. Select to add the record as a new customer, or use the existing customer information.
8. Click **OK**.
9. Review all conflicting customer data.
10. Click **OK**.

Import to Avaya Oceana®

Importing customer data into Avaya Oceana®

About this task

Use this procedure to import customer data into Avaya Oceana®.

Before you begin

- Import customer data to Oceana Customer Management Tool from a text file or ODBC database.
- Perform a customer match check to determine whether the records in the Customer Data table match a customer record.

Procedure

1. On the Oceana Customer Management Tool interface, click **Import customer data**.
2. On the Customer Settings page, click the **Import to Oceana** tab.
3. To replace the customer information in the database, do one of the following:
   - To overwrite the information of all customers in the Customer Data table, select the **Overwrite existing customer data with new customer data** check box.
   - To overwrite the information of specific customers, select the check boxes for the customers in the **Overwrite** data column.
4. Click **Import Customer Data to Oceana**.

   The Import customer data window displays a message summarizing the import status.
5. Click **OK**.

Export customer data

Exporting customer data

About this task

Use this procedure to export all the customer data from Oceana Customer Management Tool to an external file.

Procedure

1. On the Oceana Customer Management Tool interface, click **Import customer data**.
2. On the Customer Settings page, do the following:
   - To export customer data for a particular row, select the row.
   - To export customer data for all rows, click **Check All**.
3. Click **Export Checked Customers**.

   Oceana Customer Management Tool displays the Select Call Details dialog box.
4. In the **Call Details Fields** field, click the check boxes for the fields that you want to export.
5. To select all fields, click **Check All**.
6. To clear all fields, click **Uncheck All**.

7. To change the order of fields, click on the field name to highlight the row, and then click the up or down arrow.
8. To define how the fields are separated in the exported file, click one of the following:
   - **Tab**
   - **Character**

     The default character is a comma. To change this character, type the desired character in the text box.
9. If you want the first row of the exported file to contain the column headers, select the **First row shall contain column headers** check box.
10. Click **Next**.
11. In the Preview Data dialog box, click **Next**.
12. In the Select File dialog box, do the following:
    a. Click **Browse** to navigate to the directory where you want to save the exported file.
    b. Type the name of the file and click **Save**.
    c. Click **Finish**.

General settings

Viewing log files

About this task

Use this procedure to open the Oceana Customer Management Tool log file to view action, warning, and error log messages.

Procedure

1. On the Oceana Customer Management Tool interface, click **General Settings**.
2. Click the **OCMT Client Logging** tab.

   The OCMT Logging Configuration section displays the following fields which are read-only:
   - **Log file name**
   - **Log Level**
   - **Maximum log file size**
   - **Number of backup log files**
3. Click **View** to open the log file and view the log messages.

Selecting the language configuration

About this task

Oceana Customer Management Tool supports the following language configurations:

- Left to Right: This configuration is applicable to the languages that use left to right scripts. For example, English, German, French, and Italian.
- Right to Left: This configuration is applicable to the languages that use right to left scripts. For example, Arabic.

Based on your preferred language, you must select the appropriate language configuration to correctly view the elements on the user interface.

Procedure

1. On the Oceana Customer Management Tool interface, click **General Settings**.
2. Click the **OCMT Language** tab.
3. In the OCMT Language Configuration area, select one of the following options based on your preferred language:
   - **Left to Right Language**
   - **Right to Left Language**

Configuring the maximum number of days to retain active generic contacts

About this task

Configure the maximum number of days that Engagement Designer (ED) and Work Assignment can retain active generic contacts.

The default ED timeout value is 3 days. The default Work Assignment timeout value is 604800000 milliseconds, equivalent to 7 days. You can configure both of these values to retain active generic contacts for a longer period. Avaya recommends configuring these timeout values to the same number of days. The maximum value for both is 24 days.

Snap-in	Attribute	Default value	Maximum value	Comment
EngagementDesigner	Number of days the user want to retain active instances	3	24	Default value
WorkAssignmentManagerService	IMPU WorkItem Queued state for Generic Channel timeout in milliseconds	604800000 (7 days)	2073600000 (24 days)	2073600000 = (24 days) = (24 * 24 * 60 * 60 * 1000 * 1 ms)

Note:

The maximum number of queued generic contacts supported by Avaya Oceana® is a fixed limit. If you extend the maximum number of days that ED and Work Assignment can retain active generic contacts, the maximum number of queued generic limit can be reached before the increased retention time expires. For more information about the supported maximum number of queued generic contacts, see Capacity specifications on page 46.

Procedure

1. Log on to the System Manager web console.
2. Click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
3. On the Service Clusters tab, from the **Cluster** list, select Avaya Oceana® Cluster 1.
4. From the **Service** list, select **EngagementDesigner**.
5. From the list of DEFAULT_GROUP attributes, navigate to the to the **Number of days the user want to retain active instances** attribute.
6. Select **Override Default**.
7. Type the maximum number of days to retain active ED workflow instances. The maximum time is 24 days.
8. Click **Commit**.
9. On the Service Clusters tab, from the **Cluster** list, select Avaya Oceana® Cluster 1.
10. From the **Service** list, select **WorkAssignmentManagerService**.
11. From the list of IMPU Configuration attributes, navigate to the to the **IMPU WorkItem Queued state for Generic Channel timeout in milliseconds** attribute.
12. Select **Override Default**.
13. Type the maximum number of milliseconds to retain active generic contacts. The maximum time is 2073600000 ms (24 days).

    For more information, see WorkAssignmentManagerService attributes on page 711.
14. Click **Commit**.
15. Reboot Avaya Oceana® Cluster 1.

Capacity specifications

The following table shows the capacity specifications for Avaya Oceana® when deployed on-premise:

Parameter: Maximum supported number of …	On-Premise only: Agents			
	4500	**2000**	**1000**	**100**
Active Avaya Workspaces agents (including supervisors logged in as active agents)	4500 Of this, 2000 can be digital agents.	2000	1000	100
Configured channels per Agent	4 (1 voice + 3 digital)			
Active Avaya Workspaces users including supervisors and agents (Supervisors not logged in as active agents)	4950	2200	1100	110
Configured users (agents and supervisors)	14850	6600	3300	330
Configured agents	13500	6000	3000	300
Configured supervisors	1350	600	300	30
Active supervisors using Avaya Workspaces	450	200	100	10
Active voice agents	4500	2000	1000	100
Configured Social agents	300	300	300	100
Active Social agents	300	300	300	30
Configured Outbound agents	500	300	300	10
Active Outbound agents	500	300	300	10
Concurrent Avaya Workspaces instances per agent	1	1	1	1
Concurrent Avaya Workspaces instances per supervisor	1	1	1	1
Voice Busy Hour Call Completion (BHCC) - Self Service	45000	30000	30000	3000
Voice BHCC) - Assisted Service	45000	20000	10000	1000
BHCC - Outbound	10000	6000	6000	200
Chat/Email/SMS interactions per hour	15000	15000	6000	600
Chat interactions per hour Assumes no other multimedia channel is active.	15000	15000	6000	600
Messaging interactions per hour Assumes no other multimedia channel is active.	15000	15000	6000	600
Emails per hour Assumes no other multimedia channel is active.	15000	15000	6000	600

Table continues…

Parameter: Maximum supported number of …	On-Premise only: Agents			
	4500	**2000**	**1000**	**100**
SMS per hour Assumes no other multimedia channel is active.	15000	15000	6000	600
Social per hour Assumes no other multimedia channel is active.	15000	15000	6000	600
Generic Channel per hour Assumes no other multimedia channel is active.	15000	15000	6000	600
Concurrent Web Voice sessions***	1000	1000	1000	100
Concurrent Web Video sessions***	500	500	500	50
Ad-hoc Email per agent	1	1	1	1
Deferred Email interactions	10000	6000	3000	500
Deferred Emails per agent	20	20	20	20
Observe Chat per agent	3	3	3	3
Co-Browse sessions per node	200	200	200	20
Concurrent Chat sessions	2200	2200	1100	110
Concurrent Chat sessions per customer	10	10	10	10
Total Services supported	5000	5000	5000	1000
Services supported per agent	2000	2000	2000	1000
Attributes per Service	10 Channel + 9 attributes	10 Channel + 9 attributes	10 Channel + 9 attributes	10 Channel + 9 attributes
Attributes per agent*	500	500	500	500
Queued contacts across all channels	25000	25000	10000	1000
Queued Voice contacts	8000	8000	4000	400
Queued Chat contacts	2000	2000	1000	100
Queued Messaging contacts	4500	4500	2250	225
Queued Email contacts**	25000	25000	10000	1000
Queued Social contacts	5000	5000	2500	250
Queued SMS contacts	2200	2200	1100	110
Queued Generic Channel contacts	10000	10000	3000	200
Avaya WebRTC Connect agents	1000	1000	1000	100
Concurrent Chatbot sessions with two Chatbot servers	900	900	900	150

Table continues…

Parameter: Maximum supported number of …	On-Premise only: Agents			
	4500	**2000**	**1000**	**100**
Number of Communication Managers	One of the following: • 1 CM/CCElite Simplex • 1 CM/CCElite Duplex • 1 CM/CCElite Simplex or Duplex with associated ESS			
Transfer to Service operations	2000			
Engagement Designer Workflow Instances (WFIs) per cluster	25000	25000	10000	1000
Engagement Designer Workflow Definitions (WFDs) per cluster	200			
Contacts allowed on the OCP database	7 million			
Digital contacts per customer	700			
Public real-time views an administrator can create and view	60			
Private real-time views a supervisor can create and view	60			
Public dashboards an administrator can create	10			
Private dashboards a supervisor can create	10			

Notes:

* The total number of attributes is 50 times the maximum number of configured users. For example, in a 2000-agent deployment, the maximum number of configured users is 6600. Therefore, you can configure a total of 6600*50 attributes.

**Queued emails - Emails that arrive at the contact center but are not yet closed. These include active emails that agents are currently processing, emails in deferred state, and emails that are awaiting agent's availability.

*** To calculate the maximum supported sessions for a mixed Web Voice and Web Video environment, 1 Web Video session is equivalent to 2 Web Voice sessions.

For example, a large profile system can support one of the following:

- maximum 1000 Web Voice
- maximum 500 Web Video
- maximum 500 Web Voice and 250 Web Video

Ensure that your solution is engineered correctly to support the required WebRTC session counts.

WorkAssignmentManagerService attributes

Startup Configuration

Name	Description
Work Assignment Deployment Type	The deployment type that determines the memory size of processing units. • For an Avaya Oceana® deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® deployment that supports up to 100 active agents, select `OCEANA_SMALL`.
Lookup Locators for Common Spaces	The cluster that hosts Unified Collaboration Model (UCM) and Unified Collaboration Administrator (UCA) services. To set this attribute, select Avaya Oceana® Cluster 1.
Deploy the Metrics PU	The attribute that enables or disables the deployment of all the configured Work Assignment Grid components. To enable the deployment of Work Assignment Grid components, select `true`. If you set this attribute when WorkAssignmentManagerService is running, the changes of this attribute are automatically applied and the wa-metrics-agent-pu is deployed. You can verify the deployment of the wa-metrics-agent-pu through Oceana Monitor Service. The Metrics PU takes the metrics from Work Assignment and forwards them to Avaya Analytics™ through UCMService/UCMDataCollector. For IVR and Callback Assist, the Metrics PU also checks the system for estimated wait time (EWT) and staffed agents.

Advanced Configuration

Name	Description
Longest time since last contact center interaction	The attribute that enables or disables Aux Gaming Prevention. To enable Aux Gaming Prevention, select `true`. **Note:** You can modify this attribute at run-time even after creating the cluster.
Channel Overload Buffer Percentage	The percentage change required to trigger changing agents to the most overloaded channel. For example, if Voice is 50% over Reserve Level Threshold (RLT) and Chat is 40% over RLT, Voice is considered as the most overloaded channel if this attribute is set to 10. The default value of this attribute is 10.
Enable UCM Reporting Events	Enables or disables the Work Assignment interactions to be written into the UCM model. To enable the Work Assignment interactions to be written into the UCM model, select `true`.

IMPU Configuration

Name	Description
IMPU WorkItem Queued state for Chat timeout in milliseconds	The timeout of the Chat WorkItem Queued state in milliseconds. The value of this attribute must be a positive integer with a minimum value of 1 and a maximum value of 999999999. The default value of this attribute is 10800000.
IMPU WorkItem Queued state for Email timeout (value)	The timeout of the Email WorkItem Queued state in time units that are selected in the attribute IMPU WorkItem Queued state for Email timeout time unit (milliseconds or days). The value of this attribute must be a positive integer with a minimum value of 1 and a maximum value of 2073600000 (if in milliseconds) or 100 (if in days). The default value of this attribute is 604800000. You must set the value above the maximum number of days that you expect the emails to be in the queue. Include the holiday periods when email responses can be delayed.

Table continues…

Name	Description
IMPU WorkItem Queued state for Email timeout time unit	The time unit to set IMPU WorkItem Queued state for Email timeout. Select the time unit from the list. Supported time units are milliseconds and days. The default time unit is milliseconds.
IMPU WorkItem Queued state for Generic Channel timeout in milliseconds	The timeout of the Generic channel WorkItem Queued state in milliseconds. The default value of this attribute is 604800000.
IMPU WorkItem Queued state for SMS timeout in milliseconds	The timeout of the SMS WorkItem Queued state in milliseconds. The default value of this attribute is 43200000.
IMPU WorkItem Queued state for Social timeout in milliseconds	The timeout of the Social WorkItem Queued state in milliseconds. The default value of this attribute is 604800000.
IMPU WorkItem Queued state for Messaging timeout in milliseconds	The timeout of the Messaging WorkItem Queued state in milliseconds. The value of this attribute must be a positive integer with a minimum value of 1 and a maximum value of 999999999. The default value of this attribute is 604800000.
IMPU WorkItem Queued state timeout in milliseconds	The timeout of the WorkItem Queued state for all other channels that do not have a specific timeout. This value is in milliseconds. The default value of this attribute is 3600000.

Chapter 49: Configure Avaya CRMGateway snap-in

Avaya CRMGateway snap-in overview

The Avaya CRMGateway snap-in provides a normalized access layer between Avaya Oceana® and the Customer Relationship Management (CRM)s of the respective customers through an adapter. Customers can use Avaya CRMGateway SDK to develop adapters to fetch customer data from a customer CRM.

The Avaya CRMGateway snap-in is required in Avaya Oceana® to facilitate the customer use-case functionality, where the customer records are too large for importing to the Omnistore database. With Avaya CRMGateway, you can continue to manage the customer details primarily in the external CRM. You can then create the necessary linkage in the Omnistore database to enable the retrieval of customer history and customer journey data that is stored within Avaya Oceana® for the customer.

Using Avaya CRMGateway snap-in, you get a view of the customer details from the CRM directly, while doing a customer search on the CRM. The Avaya Customer Management snap-in fetches data from the CRM and stores this data or a part of this data in the Omnistore database.

The Avaya CRMGateway snap-in is installed in Avaya Breeze® using the System Manager web console. All Avaya CRMGateway alarms are displayed in System Manager.

The serviceability attributes of the Avaya CRMGateway snap-in are as follows:

- Runs in a secure cluster
- Uses Avaya Oceana® Serviceability API to send messages and heartbeats
- Registers on the Avaya Oceana® Monitor page

Using Avaya CRMGateway, you can also get the customer details that contain all the identifying values. Agents can access the customer-identifying information and the system can identify the customer from the channel on which the interaction originates.

Prerequisites

Before configuring the CRMGateway snap-in, ensure that you have the following:

- CRM adapter developed using CRMGateway SDK and its dependencies
- A valid mapper file
- Valid CRMGateway snap-In `.svar` file
- Avaya Oceana® Monitoring snap-in `.svar`

Configuring secure communication to customer CRM entity

About this task

Use this procedure to install trusted certificate while configuring a secured communication to any external customer CRM entity.

Procedure

1. In your web browser, open the following URL:

   `https://<connection url of CRM entity>`

2. From your web browser, download the relevant certificate.
3. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
4. On the Cluster Administration page, do the following:
   a. Select the check box for the cluster containing the Avaya CRMGateway.
   b. Click **Certificate Management** > **Install Trusted Certificate**.
5. On the Install Trusted Certificate page, do the following:
   a. Browse and locate the certificate.
   b. Click **Retrieve Certificate**.
   c. Click **Commit**.
6. Restart the Avaya Breeze® platform nodes that are added to the cluster containing the Avaya CRMGateway snap-in.

Verifying Avaya CRMGateway installation

About this task

Use this procedure to verify that the Avaya CRMGateway snap-in is installed correctly. After successful verification, you can configure the required attributes in the System Manager web console.

Procedure

Enter the following url in any web browser:

`https:// <Cluster IP>/ services/CRMGateway/v1/health/gateway`, where Cluster IP is the IP address of the cluster where the Avaya CRMGateway snap-in is installed.

The browser must display the following message: `{"description":"CRMGateway Snap-in is functional","status":"ACTIVE","statusCode":"200","timestamp":"11-03-2019 14:53:42"}`

If the snap-in is not installed correctly, the browser displays an error message.

Setting the Avaya CRMGateway snap-in attributes

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. Click the **Service Clusters** tab.
3. In the **Cluster** field, select the cluster that you created for the Avaya CRMGateway snap-in.
4. In the **Service** field, click **CRMGateway**.
5. Configure the required attributes.
6. Click **Commit**.

CRMGateway attributes

Default group

Name	Description
Custom CRMGateway Attributes	The custom attributes for the snap-in. Enter comma-separated values, such as maxrequestlength:1000000, maskfields:A|B|C.

Table continues…

Name	Description
Enable Tokenless Access	The attribute that enables the requests to access resource end-points without any authorization token. To enable tokenless access, retain the default value `true`.

CRM configuration

Name	Description
CRM Type	The type of CRM to connect for the configuration. The default value is SAP.
Connection URL	The FQDN or IP address of the CRM server. This is a mandatory attribute to establish a connection.
Server User-Name	The user name of the CRM server that has permission to access the CRM server database. This is a mandatory attribute to establish a connection.
Server Password	The password of the CRM server. This is an optional attribute for the connection establishment.
Custom CRM Initialization Attributes	The custom field to specify any non-sensitive information in a key:value format. For example, maxsize:1,datafile:/tmp/. This is an optional attribute.
Custom Authentication Field 1	The custom field that is used to specify sensitive information that is required by the adapter during run-time. For example, AWS secret keys, SSO information, or any token. This is an optional attribute.
Custom Authentication Field 2	The custom field that is used to specify sensitive information that is required by the adapter during run-time. For example, AWS secret keys, SSO information, or any token. This is an optional attribute.

Table continues…

Name	Description
Mapper file location	The secure location of the mapper file. For example, `https://server:port/adapter/Mapping_folder/mapper.json` or the CRMGateway Breeze node that include all the nodes in cluster where the snap-in is running. This is a mandatory attribute to establish a connection. Changing this attribute during runtime needs a service restart or cluster reboot.
Adapter Dependency Location	The base location of the plug-in JAR files. For example, `https://server:port/adaptter/JAR_FOLDER` or the Breeze node internal location such as . /tmp This is a mandatory attribute to establish a connection. Changing this attribute during runtime needs a service restart. For example, https://server:port/adapter/JAR_FOLDER or Breeze node internal location.
Adapter Dependency file Names	The JAR or properties file name that is specified by the attribute setting adapter dependency location. Enter comma (,) separated values. For example, `adapter.jar` or `helper1.jar`. This is a mandatory attribute to establish a connection. Changing this attribute during runtime requires a service restart.
Implementation Class Name	The canonical name of the class in the adapter that has implemented the SDK interface. This is a mandatory attribute to establish a connection. Changing this attribute during runtime requires a service restart.

Table continues…

Name	Description
Enable Adapter	The adapter connection state. To enable the connection, click True. The default option is False, which indicates that the connection is switched off. **Note:** You must enable this attribute only after configuring all the other attributes required for the configuration.
Input Validation	The option to ensure that the user enters valid input parameters. You must enable this attribute for enhanced security. By default, this check box is disabled. Changing this attribute during run-time requires a service restart.

Verifying CRM adapter configuration

About this task

Use this procedure to verify that the CRM adapter is installed correctly after you configure the required attributes in the System Manager web console.

Procedure

Enter the following url in any web browser:

`https:// <Cluster IP>//services/CRMGateway/v1/health/crmConnection`, where Cluster IP is the IP address of the cluster where the CRM adapter is configured.

The browser must display the following message:
`{"description":"","status":"ACTIVE","statusCode":"200","timestamp":"11-03-2019 14:53:12"}`

If the adapter is not installed correctly, the browser displays the following error message:

```
{
    "result": "Failure",
    "response": "",
    "errorMessage": "CRM Adapter is not found or is not active ",
    "errorCode": "2000",
    "statusCode": "422"
}
```

Restarting the Avaya CRMGateway snap-in service

About this task

Use this procedure to restart the Avaya CRMGateway snap-in service after editing the cluster attributes.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. On the Services page, click the **CRMGateway** check box.
3. Click **Stop**.

   The Services page displays a confirmation window listing all clusters on which the service is installed.
4. Select the check box for the clusters containing the CRMGateway service, and click **Stop**.

   On the Services page, the state of the CRMGateway service changes to `Stopping`.
5. To refresh the screen, click the  icon.

   The State column displays the status as `Stopped`.
6. Click **Services** and click the **CRMGateway** check box.
7. Click **Start**.

   The Services page displays a confirmation window listing all the clusters on which the service is installed.
8. Select the clusters on which you want to start the service, and click **Start**.

   On the Services page, in the State column, the service state changes to `Starting`.
9. Click the  icon.

   The state column displays the status as `Installed`.

Uninstalling the Avaya CRMGateway snap-in service

About this task

When you uninstall the Avaya CRMGateway snap-in, the service attributes from the Avaya Breeze® platform server remain on the web console.

Before you begin

Ensure that the Avaya CRMGateway service displays the status as `Installed` in System Manager at `Avaya Breeze® > Service Management > Services`.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. On the Services page, select the **CRMGateway** check box.
3. Click **Uninstall**.

   The service state changes to `Uninstalling`.
4. In the Confirm uninstall service dialog box, do the following:
   a. Select the cluster containing the CRMGateway service.
   b. **(Optional)** Click the **Do you want to force the uninstall?** check box.
   c. Click **Commit**.

Verifying Avaya CRMGateway snap-in uninstallation

About this task

Use this procedure to verify that the Avaya CRMGateway snap-in does not exist on the Cluster Administration page after it is uninstalled.

Before you begin

Ensure that you follow the steps for uninstalling the Avaya CRMGateway snap-in.

Procedure

1. On the Services page, verify that the **State** field displays `Loaded`.
2. On the navigation pane, click **Cluster Administration**.
3. On the Cluster Administration page, verify that the Service Status page does not display the uninstalled Avaya CRMGateway snap-in.

Deleting the Avaya CRMGateway snap-in

Before you begin

Ensure that the Avaya CRMGateway snap-in is uninstalled.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.

2. On the Services page, do the following:
    a. Verify that the status of the service displays as `Loaded`.
    b. Click **CRMGateway** > **Delete**.

       The **Services** page displays the Delete Service Confirmation window.
    c. Click **Delete**.

Next steps

Verify that the Services page does not display the deleted service.

Chapter 50: Configure secure connections from Avaya Oceana® Cluster 1 to External Data Mart

Overview

Avaya Context Store Snap-in uses the Avaya Breeze® platform to provide security configurations for access to its services. The Avaya Breeze® platform provides configuration for HTTPS, Mutual Transport Layer Security (TLS) through Client Certificate Challenge, Cross-Origin Resource Sharing (CORS), Whitelists, and Trust Certificates. For administering certificates and authorities, Avaya Aura® System Manager provides a flexible platform for the Context Store services.

Context Store supports TLS encryption for connection to the External Data Mart (EDM) database. For more information on TLS encryption, see the TLS encryption checklist section in this document.

You require additional security steps, such as certificates and licenses for the following:

- Geo Redundancy
- Context Store Pluggable Data Connector for Orchestration Designer
- ContextStoreScreenPop secured client
- Context Store SDK
- ContextStoreNotify

Though you can use any option available to configure certificates in System Manager, use the procedure provided as a worked example in the *Appendix section of Avaya Context Store Snap-in Developer Guide* for reference.

For more information on security configuration, see *Avaya Breeze® platform Overview and Specification* and *Avaya Aura® System Manager Overview and Specification*.

Secure space

With Context Store secure space, you can secure the data grid with a unique password. The unique password prevents unauthorized access to the grid. The secure user for the grid is

`dcmuser`. After security is enabled, Context Store secure space applies the username `dcmuser` and the password set in the Cluster Attributes page to the data grid.

You can configure space security when you create or edit the cluster configuration after creating the cluster.

Warning:

When you enable security after creating the cluster, System Manager deletes the existing unsecured data grid with the data. The data grid gets redeployed in a secure mode.

Configuring space security

About this task

Use this procedure to secure an existing Context Store cluster.

For configuring security in a new cluster, you must first create the cluster and perform the steps in this procedure. To configure a new cluster, see the *Avaya Context Store Snap-in Reference* document.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze** > **Cluster Administration**.
2. Select the check box of the cluster that you want to secure.
3. In **Cluster State**, click **Deny New Service**.
4. On the Warning: Deny New Service page, click **Continue**.

   System Manager changes the state of the cluster to `Denying`.
5. Select the check box of the cluster that you want to secure again and click **Edit**.

   System Manager displays the Cluster Editor page.
6. Scroll down to the Cluster Attributes section, in the **Grid password** field, enter the unique password.
7. Select the **Use secure grid?** check box.
8. Click **Commit**.

   System Manager prompts you to ensure all Avaya Breeze® platform server restarts are complete before placing the cluster into the **Accept New Service** state.
9. Click **OK**.
10. In the left navigation pane, click **Cluster Administration**.
11. Select the check box of the new or the modified cluster.
12. In **Cluster State**, select **Accept New Service**.

13. In the Accept New Service window, click **Continue**.

    System Manager displays the status as `Accepting` in the **Servers State** column.

Cross Origin Resource Sharing

Cross Origin Resource Sharing (CORS) provides access to Context Store requests that originate from other domains. The configuration option is available on the HTTP security page through the Avaya Breeze® platform.

Note:

When you enable the client certificate challenge, web clients cannot authenticate through Javascript Ajax calls. You cannot send the client certificate because the browser and the Javascript layer are disconnected.

Transport Layer Security encryption checklist

Avaya Context Store Snap-in supports Transport Layer Security (TLS) encryption for connection to the External Data Mart (EDM) database.

To enable TLS encryption in Context Store, you must perform the following tasks:

S.No.	Tasks	Descriptions	Notes
1	Configure the prerequisites for certificate management	Configuring the prerequisites for certificate management and usage on page 726	For configuring certificate management and encrypted connections, you must: • Ensure that you use a compatible JDBC driver. • Based on your requirement, configure the user configuration options in the Local Group Policy Editor of your server.

Table continues…

S.No.	Tasks	Descriptions	Notes
2	• Create Transport Layer Security (TLS) certificate in System Manager • Download TLS certificate from System Manager • Import TLS certificate from System Manager • Export TLS certificate from MS SQL server	Creating Transport Layer Security certificate in System Manager on page 727 Downloading Transport Layer Security certificate from System Manager on page 160 Importing Transport Layer Security certificate from System Manager on page 729 Exporting Transport Layer Security certificate from MS SQL server on page 730	For using secure TLS connections between MS SQL Server and System Manager, configure a valid security certificate. You can create this certificate from the root certificate in System Manager, or obtain the certificate from a third-party certificate authority. If you create a TLS certificate that is not from System Manager, you must import the certificate to the System Manager truststore.
3	Configure MS SQL Server to listen on a static port	Configuring the MS SQL server to listen on a static port on page 733	For the MS SQL server to listen on a static port, configure the settings by using the SQL Server Configuration Manager.
4	Configure MS SQL Server for forced encryption	Configuring MS SQL Server for forced encryption on page 732	For enabling forced encryption, configure the MS SQL server protocols for the required MS SQL server instance.

Configuring the prerequisites for certificate management and usage

About this task

Use this procedure to change the policy on the Windows Server running MS SQL Server. You must use the supported JDBC driver and configure the user configuration options available in the Local Group Policy Editor of your server.

Procedure

1. Ensure that you are using the supported JDBC driver for System Manager.

   The minimum supported driver is: `mssql-jdbc-7.4.1.jre8.jar`

See Loading JDBC driver to System Manager on page 162.

2. To open Local Group Policy Editor on your Windows Server running MS SQL Server, press +R, and type `gpedit.msc`.

   You can also search in Windows Server using `gpedit.msc`.

3. Click **User Configuration** > **Administrative Templates** > **Windows Components** > **Microsoft Management Console**.
4. On the right panel, right-click **Restrict the user from entering author mode** > **Edit**.
5. Select **Disabled** and click **OK**.
6. To choose the restricted or permitted snap-ins, click the **Restricted/Permitted snap-ins** folder.
7. On the right panel, right-click **Certification Authority** > **Edit**.
8. Select **Enabled**, and click **OK**.
9. On the right panel, right-click **Certificates** > **Edit**.
10. Select **Enabled**, and click **OK**.
11. On the right panel, right-click **Computer Management** > **Edit**.
12. Select **Enabled** and click **OK**.

Creating Transport Layer Security certificate in System Manager

About this task

Use this procedure to secure the connection between Context Store and Microsoft SQL Server. If you are using a third-party certificate, skip this procedure.

Note:

For creating TLS certificates in System Manager for the connection between Context Store and a group of EDMs hosted on two SQL Servers in an Availability Group see *Generating certificates to enable SSL connections from Context Store to a a cluster of two SQL Servers hosting EDMs configured in an AlwaysOn High Availability group* section.

Procedure

1. Log in to System Manager.
2. Click **Services** > **Security** > **Certificates** > **Authority**.
3. On the left navigation pane, click **Add End Entity**.
4. On the Add End Entity page, enter the details in the following fields:

Entering the following values is the minimum requirement. Depending on your requirements, enter the appropriate values in the other fields.

a. In the **End Entity Profile** field, select **INBOUND_OUTBOUND_TLS**.
b. Enter a username and password of your choice.

   Use this information to identify the certificate when you download it from System Manager.
c. In the **CN, Common name** field, enter the FQDN details of the MS SQL server.
d. In the **FQDN Name** field, enter the DNS name.
e. Leave the **IP Address** field blank.
f. In the **Token** field, select **P12 file**.
g. Click **Add**.

Downloading Transport Layer Security certificate from System Manager

About this task

To import a Transport Layer Security (TLS) certificate from System Manager to your server, download the certificate to your local machine.

Before you begin

Create a TLS certificate in System Manager.

Procedure

1. Log in to System Manager.
2. Click **Services** > **Security** > **Certificates** > **Authority**.
3. On the left navigation pane, click **Public Web**.

   System Manager displays the public EJBCA pages.
4. On the left navigation pane, click **Create Browser Certificate**.

   System Manager displays the Certificate Enrollment page.
5. To generate your token, do the following:
   a. In the **Username** field, enter the user name that you enter while creating an end entity.
   b. In the **Enrollment code** field, enter the password that you enter while creating an end entity.
   c. Click **OK**.

   System Manager displays the EJBCA Token Certificate Enrollment page.

6. In the **Key length** field, select **4096 bits**, and click **Enroll**.

   System Manager downloads the `p12` certificate to your downloads folder.

Importing Transport Layer Security certificate from System Manager

About this task

After creating the certificate, you must import the Transport Layer Security (TLS) certificate from System Manager and save it in the personal folder on your MS SQL server.

Before you begin

- Create a TLS certificate in System Manager.
- Download the TLS certificate from System Manager to your local machine and save it in a folder on your MS SQL server.

Procedure

1. Navigate to the folder where you saved your `p12` file.
2. To open the Certificate Import Wizard page, do one of the following:
   - Double-click the `p12` file.
   - Open `certlm.msc` from the Windows Search window: On the Certificates-Local Computer page, right-click **Personal**, and click **All Tasks** > **Import**.
3. On the Certificate Import Wizard page, select **Local Machine**, and click **Next**.
4. Click **Browse**, specify the certificate file to import, and click **Next**.
5. To maintain the private key security, enter the password you entered when creating an end-entity in System Manager, select the **Include all extended properties** check box, and click **Next**.
6. To select and import the certificate, do the following:
   a. Select **Place all certificates in the following store**.
   b. Click **Browse**.
   c. In the Select Certificate Store window, select **Personal** and click **OK**.
   d. On the Certificate Import Wizard, click **Next**.
   e. To import the certificate, click **Finish**.
7. Press +`R`, and type `certlm.msc`.
8. Click **OK**.

   In the navigation pane, expand the **Personal** > **Certificates** folders.

9. Double-click the required certificate.
10. Click the **Details** tab.
11. Click **Edit Properties**, in the **Friendly Name** field, enter a name of your choice for the certificate.

    Tip:

    To choose this certificate instantly when enforcing the TLS connection, you must save only one certificate in the personal folder of your MS SQL server.
12. Click **OK**.

Exporting Transport Layer Security certificate from MS SQL server

About this task

Use this procedure to import the Transport Layer Security (TLS) certificate to System Manager.

Note:

Perform these steps only if MS SQL Server already uses a third-party certificate that System Manager did not create.

Procedure

1. Log in to MMC and go to **File** > **Add/Remove Snap-ins.**
2. Add the **Certificates** snap-in and click **Ok**.
3. Navigate to your personal folder under **Certificates** > **Personal** > **Certificates**, and right-click the required certificate.
4. Click **All Tasks** > **Export**.
5. Click **Next**.

   The Certificate Wizard displays the Export Private key options.
6. Select **No, do not export the private key**, and click **Next**.
7. To select the required file format, select the **DER encoded binary X.509 (.CER)**, and click **Next**.
8. In **File name**, click **Browse** to select the file to export, and click **Save**.

   The file extension is `X.509(.CER)`, which you selected in the previous step.
9. In System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.

   System Manager displays the Cluster Administration page.

10. In the Cluster Administration page, do the following:
    a. Select the check box of the row for the Context Store cluster.
    b. In the **Certificate Management** tab, click **Install Trust Certificate (All Avaya Breeze® Instances)**.
11. In the Install Trusted Certificate page, do the following:
    a. In **Select Store Type to install trusted certificate**, click **WEBSPHERE**.
    b. In **Please select a file**, click **Browse** to select the certificate from the MS SQL server that you exported earlier.
    c. Click **Open**.
    d. To review the certificate details before you continue, click **Retrieve Certificate**.
    e. Click **Commit**.

Configuring Avaya Context Store Snap-in for secure connections

About this task

To enable secure connections from Avaya Context Store Snap-in to External Data Mart (EDM), you must set the appropriate values on System Manager.

Before you begin

If you are using a third-party certificate, do the following:

- Export the TLS certificate from the MS SQL server.
- Import the certificate to the truststore of each Avaya Breeze® node from the MS SQL server.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. In the Attributes Configuration page, click the **Service Clusters** tab and do the following:
    a. In **Cluster**, select the name of the **Provisioning Cluster**.
    b. In **Service**, select **OceanaConfiguration**.
    c. In the External Data Mart Configuration section, ensure that the value of **Secure Connections to EDM** is set to **true**.
    d. In **External Data Mart FQDN**, type the FQDN of the EDM database host for the TLS connection.

If connecting to an availability group of EDMs, type the FQDN of the AlwaysOn Availability Group Listener. Do the following to find the FQDN of the AlwaysOn Availability Group Listener:

a. Log on to the primary or secondary SQL Server as the domain user configured for use with the SQL Server Service.

b. Open SQL Server Management Studio.

c. Login to the SQL instance as the domain user configured for use with the SQL Server Service.

d. To find the name of the Availability Group Listener, click **Always On High Availability** > **Availability Groups** > **<The name of the EDM Availability Group>** > **Availability Group Listeners**.

The FQDN is the name of the Listener and the name of the domain to which the SQL Server cluster belongs to. For example, `myListener.exampleDomain.com`.

Important:

You must enter the FQDN of the host for secure connections. Do not enter the IP address.

3. Click **Commit**.

Configuring MS SQL Server for forced encryption

About this task

Use this procedure to do the following:

- Configure the server to accept encrypted connections and use the correct certificate for the Transport Layer Security (TLS) connection.
- Enable the forced encryption option in MS SQL Server Configuration Manager.

Before you begin

Ensure that you have configured a certificate on your server from System Manager or the third-party CA.

Procedure

1. Click and locate and open **Microsoft SQL Server *N*** > **SQL Server Configuration Manager** where *N* is the installed version of MS SQL.

   - Alternatively: Press +R and enter `compmgmt.msc` to start **Computer Management**. Expand **Services and Applications** and locate **SQL Server Configuration Manager**.

2. Expand **SQL Server Network Configuration**

3. Right-click **Protocols for MSSQLSERVER**, and select **Properties**.
4. In the Properties window:
    a. On the **Flags** tab: In the **Force Encryption** field, click **Yes** and then click **OK**.
    b. On the **Certificate** tab: In the **Certificate** field, click the required certificate and then click **OK**.
5. To apply the changes:, right-click the required MS SQL server and restart the MS SQL Server service.
    a. Click **SQL Server Services**.
    b. Right-click on the **SQL Server** and click **Restart**.

Configuring the MS SQL server to listen on a static port

About this task

Use this procedure to configure the MS SQL Server Database Engine to listen on a specific port by using SQL Server Configuration Manager.

Procedure

1. Click and locate and open **Microsoft SQL Server *N*** > **SQL Server Configuration Manager** where *N* is the installed version of MS SQL.
    - Alternatively: Press +R and enter `compmgmt.msc` to start **Computer Management**. Expand **Services and Applications** and locate **SQL Server Configuration Manager**.
2. Select **SQL Server Network Configuration** > **Protocols for MSSQLSERVER**.
3. Right-click **TCP/IP**, and click **Enable**.
4. Right-click **TCP/IP**, and click **Properties**.
5. On the TCP/IP Properties page, click the **IP Addresses** tab.
6. Scroll down to the **IPALL** section.
7. In the **IPALL** section, remove **TCP Dynamic Ports**, and in the **TCP Port** field, enter `1433`.

Breeze Authorization Service Integration

The Breeze Authorization Service Integration feature integrates the Avaya Breeze®Authorization service with Avaya Context Store Snap-in to grant access to applications using bearer tokens generated from the Context Store services.

Using this feature, you can configure any combinations of four values to grant access. You can also add or remove grants from the Authorization service in System Manager. This feature has the following user privileges:

- Privileged: Used for privileged users
- Standard: Used for standard users

  For information on adding grants to the Breeze Authorization configuration, see “Assigning permissions to an authorization client” section in *Avaya Context Store Snap-in Reference*.

The values and function applicable to these feature types are:

Value	Function
create	Applies to all ContextStore REST POST methods
delete	Applies to all ContextStore REST DELETE methods
read	Applies to all ContextStore REST GET methods
update	Applies to all ContextStore REST PUT methods

Integration with Context Store REST API

From Context Store Release 3.2 onwards, the Breeze Authorization Service Integration feature adds authorization to all the ContextStore REST API methods by adding a new header attribute to each REST request. The ContextStore REST API checks the authorization header only when the attribute is enabled in System Manager. You must start the value with a bearer followed by the token created.

Additional API Methods

Four REST methods are available for generating bearer tokens. These APIs are available only if you set the **Enable Breeze Authorization Service** attribute on ContextStoreREST to `True`.

Any user can use the **Get token** and **Get token by scope** APIs to generate tokens. However, the APIs are accessible only if you set the **Require user for Breeze Authorization Service** attribute on ContextStoreREST to `False`. If you set the attribute to `True`, then you can use only the more secure versions of the generate-token APIs, for which you require valid login credentials.

You can generate tokens using four new REST methods available in the ContextStore REST API as follows:

Name	REST Method	URL	Headers	Notes
Get Token	GET	/services/CSRest/cs/contexts/token/		You can disable this method in System Manager attributes

Table continues…

Name	REST Method	URL	Headers	Notes
Get Token by Scope	GET	/services/CSRest/cs/contexts/token/scope/	scope	• You can disable this method in System Manager attributes • <*SCOPE*> can be privileged or standard
Get Token for User	GET	/services/CSRest/cs/contexts/token/username/	• username • password	Set HTTP headers user name and password
Get Token for User by Scope	GET	/services/CSRest/cs/contexts/token/username/scope/	• scope • username • password	• Set HTTP headers user name and password • <*SCOPE*> can be privileged or standard

ContextStore Rest attributes

As a part of the Breeze Authorization Service Integration feature, the ContextStore Rest snap-in provides the following three attributes:

Name	Values	Details
Address of Authorization Service	The fully qualified domain name (FQDN) or IP address of the cluster where the Authorization Service is installed.	Enter the FQDN or IP address of the UAC cluster with the Authorization service installed. This setting is used by the Oceana Configuration service, where you must enter the Authorization service address.
Enable Breeze Authorization Service	• true • false	Set the value to true. This setting does the following: • It makes all of the ContextStoreRest APIs require tokens to use. Attempting to use one without a token gives an unauthorised error. • It enables the token-generation APIs mentioned in the table above.

Table continues…

Name	Values	Details
Require user for Breeze Authorization Service	• true • false	Set the value to true to use only the more secure versions of the generate-token APIs, for which you require valid login credentials. If you set this attribute on ContextStoreREST to false, all the APIs are accessible. **Note:** Setting the value to true disables the Get Token and the Get Token by Scope API methods. This means that the user is no longer able to generate a token without providing valid user credentials.

Port utilization

For Context Store and Avaya Breeze® platform port information, see the applicable Avaya Breeze® platform and Context Store Port Matrix documents available on the Avaya Support website at https://support.avaya.com.

Chapter 51: Centralized logging

Centralized Logging overview

Centralized Logging is a feature that you can use to view the logs for all services of Avaya Oceana® clusters through a centralized interface.

Checklist for centralized logging

The following table lists the tasks that you need to perform to set up centralized logging:

No.	Task	Notes	✔
1	Configure Certificate for Secure TLS connection between Breeze and CSP ElasticSearch. **Note:** Only Secure Connection is supported from Breeze Logstash to CSP ElasticSearch Connection between Breeze Logstash and CSP Elasticsearch can only be through Mutual TLS (MTLS) and it cannot be unsecured. It is necessary to perform the following procedures before updating cluster attributes and setting Centralized Logging destination to CSP Elasticsearch option on SMGR. You need to perform the following tasks: 1. Adding Breeze CA certificate to the Elasticsearch truststore on CCM on page 738 2. Adding Breeze node Common Name (CN) to CSP on page 740		

Table continues…

No.	Task	Notes	✔
2	Configure the cluster attribute for Centralized Logging. You need to perform the following tasks: 1. Changing the targeted Breeze cluster in Deny New Service state on page 741 2. Configuring Centralized Logging on the cluster editor on page 742 3. Changing the Avaya Breeze cluster state to accept new service on page 742		
3	Install Metricbeat and Packetbeat Snap-in on the Breeze cluster for metrics and traffic data related information. You need to perform the following task: • Download the latest Metricbeat and Packbeat SVAR from the Avaya Support website at https://support.avaya.com. • Installing the Metricbeat and Packbeat Snap-in on the Breeze cluster on page 743		
4	View Logs on CSP OpenSearch UI. You need to perform the following tasks: 1. Logging in to OpenSearch UI on page 743 2. Creating custom index patterns on page 744 3. Creating index policies for the custom index patterns on page 744 4. Discovering data using new index patterns on page 747 5. Recovery steps if the elasticsearch disk size is full on page 747		

Adding Breeze CA certificate to the Elasticsearch truststore on CCM

About this task

To add Breeze CA certificate to the Elasticsearch truststore on CCM, perform the following procedures:

Procedure

1. Loading the Breeze CA certificate into the Elasticsearch truststore on page 739.

2. Restarting the Elasticsearch cluster on page 739.

Loading the Breeze CA certificate into the Elasticsearch truststore

Procedure

1. Log in to the SMGR.
2. Go to **Service** > **Inventory** > **Manage Elements** and select the Breeze node.
3. From **More Actions** menu, select **Manage Trusted Certificate**.
4. Select a value from the **Store Description** column with **WEBSPHERE** as **Store Type** and click **Export**.

   The `trust-cert.pem` file is generated.
5. To transfer the `trust-cert.pem` file to the CSP CCM, run the following commands on CCM Command Line Interface (CLI):

   - `ccmcertmgr -ls trust | grep logelasticsearch`
   - `ccmcertmgr --add-trustcert logelasticsearch-certificate-default-logelasticsearch-mtls-trustedcert trust-cert.pem`

   The trust-cert.pem is the CA certificate of Breeze.

   Example of an expected output:

```
{
"status": "CREATED",
"statusCode": 201,
"timestamp": "12-03-2025 08:49:05",
"message": "logelasticsearch-certificate-default-logelasticsearch-mtls-
trustedcert : Certificate added to trusted store successfully"
}
```

Restarting the Elasticsearch cluster

About this task

This procedure does not impact the service of Analytics operations.

Procedure

1. Run the following commands as root user to restart the Elasticsearch cluster to pull in the Breeze CA certificate:

   ```
   kubectl scale statefulsets/logelasticsearch --replicas=0
   ```
2. Monitor pod state by running the following command:

   ```
   kubectl get pods | grep logelasticsearch
   ```
3. After all the logelasticsearch* pods are terminated, run the following command to bring them up:

   ```
   kubectl scale statefulsets/logelasticsearch --replicas=3
   ```

Adding Breeze node Common Name (CN) to CSP

About this task

To add Breeze node to CN to CSP, perform the following procedures:

Procedure

1. Retrieving the Breeze node CN on page 740.
2. Adding Breeze CN to CCM through CLI on page 740
3. Adding CSP CA to Avaya Breeze truststore on page 741

Retrieving the Breeze node CN

Procedure

1. Log in to the SMGR.
2. Go to **Service** > **Inventory** > **Manage Elements** and select the breeze node.
3. From **More Actions** menu, select **Manage Trusted Certificate**.
4. Check the **Subject Name** field value with **Store Type** as **WEBSPHERE** to see the CN value.

   An example of a CN value: C=US, O=Avaya, CN= <fqdn_of_the_breeze_node> where <fqdn_of_the_breeze_node> is CN for the breeze node.

Adding Breeze CN to CCM through CLI

Procedure

1. On the CCM lab, log in as a root user.
2. Obtain the `addCNMappingExt.tar.gz` file from the Avaya Support website at support.avaya.com. Place the file in the CCM lab folder `/var/avaya/artifactCache` folder of the CCM lab.
3. Run the following to change directory to `/var/avaya/artifactCache`:

   ```
   cd /var/avaya/artifactCache
   ```

4. Untar the compressed file in the CCM using the following command:

   ```
   tar -xvzf addCNMappingExt.tar.gz -C /var/avaya/artifactCache
   ```

5. Run the following to change directory to `/var/avaya/artifactCache/addCNMappingExt`:

   ```
   cd /var/avaya/artifactCache/addCNMappingExt
   ```

6. If the script file is copied from the Windows machine, convert it to Unix format using the following command:

   ```
   dos2unix addCNMappingExt.sh
   ```

7. Set the execution permissions on the script using the following command:

   ```
   chmod 755 addCNMappingExt.sh
   ```

8. The CN needs to be added using the following command for each node at a time:

   ```
   ./addCNMappingExt.sh -cn <fqdn of the breeze node>
   ```

   Repeat for each Breeze node in the Customer Engagement Breeze cluster.

   Example of an expected output: `The CN -` <fqdn of the breeze node> added successfully with READ-WRITE permissions.

Adding CSP CA to Avaya Breeze truststore

Procedure

1. On the CCM lab, log in as a root user.
2. Run the following command to get the CSP CA:

   ```
   kubectl get secrets --namespace default fluentd-ca-crt -o go-
   template='{{index .data "root-cert.pem"}}' | base64 -d > root-cert.pem
   ```

3. Transfer the `root-cert.pem` file created to your local machine using a utility tool such as, WinSCP or FileZilla.
4. Log in to SMGR and go to **Elements** > **Avaya Breeze** > **Cluster Administration** and then select the Breeze customer engagement cluster and select **Certificate Management** > **Install Trust Certificate**.
5. In the **Install Trusted Certificate** form select WEBSPHERE under **Select Store Type** to install the trusted certificate.
6. Click **Browse** to select the CSP `root-cert.pem` file on your local server and click **retrieve**.

   The CA details is displayed.

7. Click **commit** to add CA to the WEBSPHERE trust store.

Changing the targeted Breeze cluster in Deny New Service state

About this task

Change the Customer Engagement Breeze cluster status to **Deny New Service** in the SMGR.

Procedure

1. Log in to the SMGR.
2. Go to **Elements** > **Avaya Breeze** > **Cluster Administration**

3. Select the customer engagement Breeze cluster and click **Cluster state** > **Deny New Service** and then click **Continue**.

Configuring Centralized Logging on the cluster editor

About this task

Use this procedure to configure centralized logging on the cluster editor.

Procedure

1. Log in to SMGR.
2. Go to **Elements** > **Avaya Breeze** > **Cluster Administration** and select the Breeze Cluster and click **Edit** from menu.
3. In the **Cluster Attributes** section, from **Centralized logging destination** drop down menu select **CSP Elasticsearch**.

   Note:

   The check box **Use secure connection for centralized logging?** is selected by default when using CSP for the centralized logging solution. Insecure connections are not supported.
4. Provide the CSP/Analytics Cluster FQDN or IP Address in the text box **CSP Elasticsearch as destination**. For example, xyz190.abc.com:30004 (<CSP_Cluster_FQDN>:PORT)
5. Click **Commit** to save the changes.

Changing the Avaya Breeze cluster state to accept new service

About this task

Change the Breeze cluster status to **Accept New Service**.

Procedure

1. Log in to the SMGR.
2. Go to **Elements** > **Avaya Breeze** > **Cluster Administration**
3. Select the customer engagement Breeze cluster and click **Cluster state** > **Accept New Service** and then click **Continue**.

Installing the Metricbeat and Packbeat Snap-in on the Breeze cluster

About this task

Install Metricbeat and Packetbeat Snap-in on the Breeze cluster for metrics and traffic data related information.

Before you begin

Obtain the latest Metricbeat and Packbeat SVARs from the Avaya Support website at support.avaya.com.

Procedure

1. Log in to the SMGR.
2. Go to **Elements** > **Avaya Breeze** > **Service Management** > **Services** and click **Load** and then select the relevant file and accept the End User License Agreement (EULA).

   This step takes a few minutes due to the EULA load time.
3. Select the loaded service and click **Install**.
4. Select the targeted Breeze cluster and click **Install**.

Logging in to OpenSearch UI

About this task

Log in to OpenSearch UI using the following URL: `https://<csp__cluster_fqdn>/logging/`.

The following script is provided on CSP which creates a READ-WRITE user on Keycloak:

`createKibanaUser`

Procedure

1. On the CCM lab, log in as a root user.
2. Run the following command:

   ```
   ccm release common-services createKibanaUser -u adminuser -r READ-WRITE
   ```

   For example, the following message is displayed:

   ```
   User created successfully on Keycloak!
   User role assigned successfully on Keycloak!
   UserName = adminuser
    Password = Passwd@0987654321
   ```
3. Login to `https://<CSP Cluster FQDN>/logging/` using the credentials created.

Note:

When you access for the first time, you are prompted to change the password.

Creating custom index patterns

About this task

After you configure the Centralized Logging on the Breeze cluster and install the svars, indices are available in the following format: filebeat-<version>-<date> , metricbeat-<version>-metricbeat, packetbeat-<version>-<date>. For example, filebeat-8.5.3-2023.02.21.

You can create filebeat-* , metricbeat-* and packetbeat-* index patterns one by one.

Procedure

1. On the OpenSearch UI, click ☰ to display the navigation pane.
2. On the navigation pane, click **Management** > **Stack Management** > **Index Patterns** > **Create Index Pattern** and type the **Index pattern name**.
3. Click **Next step** and from the **Time field** menu select **@Timestamp**.
4. Click **Show Advanced Setting** and type the **Custom index pattern ID** same as index-pattern and click **Create Index Pattern**.

Creating index policies for the custom index patterns

About this task

Set up storage policies for the created indices. The retention values need to be adjusted according to the solution requirements and the storage size.

The fields, "min_index_age" and "min_size" under transition conditions for “read_only” and “delete” need to be configured.

Procedure

1. On the OpenSearch UI, click ☰ to display the navigation pane.
2. On the navigation pane, go to **OpenSearch Plugins** > **Index Management** and click **Create policy** and then select **JSON editor**.
3. In **Policy ID**, enter a name for the policy, for example: "breeze-default-policy-filebeat."
4. Replace the contents in **Define Policy** with the relevant files for each index pattern.

Example of a sample for "filebeat" JSON policy set for 100 agents lab with PVC Size: 80GB as below:

```
{
    "policy": {
        "description": "Adding log retention policy for Breeze logs coming from
filebeat.",
        "error_notification": null,
        "default_state": "read_write",
        "states": [
            {
                "name": "read_write",
                "actions": [
                    {
                        "retry": {
                            "count": 3,
                            "backoff": "exponential",
                            "delay": "1m"
                        },
                        "read_write": {}
                    }
                ],
                "transitions": [
                    {
                        "state_name": "read_only",
                        "conditions": {
                            "min_index_age": "2d"
                        }
                    },
                    {
                        "state_name": "read_only",
                        "conditions": {
                            "min_size": "1gb"
                        }
                    }
                ]
            },
            {
                "name": "read_only",
                "actions": [
                    {
                        "retry": {
                            "count": 3,
                            "backoff": "exponential",
                            "delay": "1m"
                        },
                        "read_only": {}
                    }
                ],
                "transitions": [
                    {
                        "state_name": "delete",
                        "conditions": {
                            "min_index_age": "7d"
                        }
                    }
                ]
            },
            {
                "name": "delete",
                "actions": [
                    {
                        "retry": {
                            "count": 3,
```

```
                            "backoff": "exponential",
                            "delay": "1m"
                        },
                        "delete": {}
                    }
                ],
                "transitions": []
            }
        ],
        "ism_template": [
            {
                "index_patterns": [
                    "filebeat-*"
                ],
                "priority": 0
            }
        ]
    }
}
```

For policy recommendations for different deployment sizes, see Policy recommendations for different deployment sizes on page 746.

Policy recommendations for different deployment sizes

The following table lists the policy recommendations for different deployment sizes:

	100 agents **PVC Size: 80GB**	**500 agents** **PVC Size: 120GB**	**1000 agents** **PVC Size: 150GB**	**2000 agents** **PVC Size: 200GB**	**4500 agents** **PVC Size: 300GB**
Filebeat policy	ready_only min_index_age: 2d ready_only min_index_size : 1GB delete min_index_age: 7d	ready_only min_index_age: 2d ready_only min_index_size : 2GB delete min_index_age: 7d	ready_only min_index_age: 2d ready_only min_index_size : 5GB delete min_index_age: 7d	ready_only min_index_age: 2d ready_only min_index_size : 5GB delete min_index_age: 7d	ready_only min_index_age: 2d ready_only min_index_size : 10GB delete min_index_age: 7d
Packetbeat policy	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d

Table continues…

	100 agents PVC Size: 80GB	500 agents PVC Size: 120GB	1000 agents PVC Size: 150GB	2000 agents PVC Size: 200GB	4500 agents PVC Size: 300GB
Metricbeat policy	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d	ready_only min_index_age: 2d ready_only min_index_size : 3GB delete min_index_age: 2d

Note:

The min index age in the read only transition should be less than or equal to the min index age in the delete transition.

If the Index size needs to be increased, ensure that the PVC size supports them.

Discovering data using new index patterns

Procedure

1. On the OpenSearch UI, click ☰ to display the navigation pane.
2. On the navigation pane, go to **Opensearch Dashboards** > **Discover**.
3. Use the **Add filter** and **Filter by type** options to filter the data displayed.
4. You can customize and save dashboards.

Recovery steps if the elasticsearch disk size is full

About this task

Delete the indices if the elasticsearch disk size if full.

Procedure

1. On the OpenSearch UI, click ☰ to display the navigation pane.
2. On the navigation pane, go to **Management** > **Dev Tools**.
3. Run the following command to get indices with size:

```
GET /_cat/indices?v&h=index,pri,rep,store.size
```

4. Run the following command to delete the indices of bigger sizes:

   ```
   DELETE /<index_name>
   ```

Chapter 52: Resources

Documentation

Title	Use this document to:	Audience
Overview		
Avaya Oceana® Solution Description	Use this guide to know about the tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Implementing		
Deploying Avaya Oceana®	Use this guide to know how to deploy Avaya Oceana® Solution on the customer environment.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Avaya Oceana® and Avaya Analytics™ Disaster Recovery	Use this guide to know how to restore Avaya Oceana®, solution when there is a complete outage at the primary data center.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Migrating Avaya Oceana®	Use this guide to know how to migrate Avaya Oceana® solution from the existing version.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Deploying Avaya Analytics™	Deploy Avaya Analytics™.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Administering		

Table continues…

Title	Use this document to:	Audience
Administering Avaya Oceana®	Administer Avaya Oceana®.	• System administrators • Supervisors
Using		
Using Avaya Workspaces for Avaya Oceana®	Use Avaya Workspaces for Avaya Oceana®.	• Agents • Supervisors
Using Avaya Analytics™	Use the features and capabilities of Avaya Analytics™.	• Supervisors • Administrators • Report designers
Avaya Analytics™ Data Dictionary	Use historical and real-time measures in custom reports.	• Administrators • Report designer
Maintaining and Troubleshooting		
Maintaining and Troubleshooting Avaya Oceana®	Perform maintenance and troubleshooting procedures for routine maintenance and troubleshooting of Avaya Oceana®.	• Support personnel • Implementation engineers • Administrators
Maintaining and Troubleshooting Avaya Analytics™	Perform common maintenance functions of Avaya Analytics™ and use tools and utilities for troubleshooting of Avaya Analytics™.	• Support personnel • Implementation engineers • Administrators
Avaya Oceana® Alarms	View details about Avaya Oceana® alarms.	• Support personnel • Administrators

Finding documents on the Avaya Support website

Procedure

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

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

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

8. Click to display the search results.

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** ( ) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

You can do the following:

- Create, rename, and delete a collection.
- Set a collection as the default or favorite collection.
- Save a PDF of the selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collections that others have shared with you.

- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.
- Send feedback for a topic.

Training

The following courses are available for the Avaya Oceana® program.

Table 1: Sales Credentials

Course code	Course title	Course duration in hours	Delivery type
APSS – 1202 Avaya OneCloud™ CCaaS Sales			
41511W	Selling Avaya OneCloud™ CCaaS Solutions	0.75	Web-based Training
41551T	Avaya OneCloud™ CCaaS Sales Specialized Test	1.0	Web-based Training
ALCC –2005 Avaya Multiexperience Solutions Sales (ALCC-2005)			
41710W	The Avaya OneCloud™ Contact Center Automated Story	0.50	Web-based Training
41411W	Selling Avaya Oceana®	0.75	Web-based Training
41401W	Selling Avaya Analytics™	0.50	Web-based Training
41481W	Avaya Oceana® ROI for Sales	0.50	Web-based Training
41770W	Avaya Experience Portal and Proactive Outreach Manager (POM) for Sales	0.25	Web-based Training

Table 2: Pre-Sales Design

Course code	Course title	Course duration in hours	Delivery type
ACDS – 3480 Avaya Oceana® Solution Design			
34211W	Avaya Oceana® Overview for Design	0.75	Web-based Training
34811W	Designing the Avaya Oceana Solution Part 1 of 3	1.0	Web-based Training
34821W	Designing the Avaya Oceana Solution Part 2 of 3	1.0	Web-based Training
34831W	Designing the Avaya Oceana Solution Part 3 of 3	1.0	Web-based Training
34801X	Avaya Oceana® Solution Design Exam	1.50	Exam
ALRI-7001 Avaya Oceana® Product Release Information Collection			
39001W	Avaya Oceana® R3.8 with Breeze Snap-ins Details for Pre-Sales	1.0	Portable Document Format (PDF)
39020W	Avaya Breeze® Snap-ins for Avaya Oceana Details for Pre-Sales	1.0	PDF

Table 3: Technical Services Partner Credentials

Course code	Course title	Course duration in hours	Delivery type
ACIS – 7495 Avaya Oceana® Solution Implement			
74150V	Integrating Avaya Oceana® Core and Workspaces	40.0	Virtual Instructor-Led Training
74950X	Avaya Oceana® Solution Integration Exam	1.50	Exam
ACSS-7497 Avaya Oceana®			
74550V	Supporting Avaya Oceana®	24	Virtual Instructor-Led Training
7497X	Avaya Oceana® Support Exam	1.75	Exam
74360W	Installing Avaya Analytics™ for Oceana®	1.5	Web-based Training

Table 4: Pre-requisite Courseware

Course code	Course title	Course duration in hours	Delivery type
77900W	Avaya Control Manager Training Bundle (5 courses 21900W, 77910W, 77920W, 77930W, 77940W)	5.50	Web-based Training
70160W	Avaya Breeze® Implementation and Support	30.0	Web-based Training

Table 5: End User, Programmer, Administration

Avaya Learning Center				
Course code	**Course title**	**Course duration in hours**	**Delivery type**	**Vanity Link for Attachment**
ALEU-5002 Avaya Oceana® End-User Training				
24020W	Using Avaya Workspaces for Avaya Oceana® - Agent	1.0	Web-based Training	https://www.avaya.com/oceana-agent
24040W	Using Avaya Workspaces for Avaya Oceana® - Supervisor	1.0	Web-based Training	https://www.avaya.com/oceana-supervisor
ALUC-4001 Avaya Breeze® Client SDK				
2410W	Customer Communications and Apps with Oceana® for Developers	3.0	Web-based Training	
ASDC-0010 Avaya Workspaces® Framework				
24150W	Customizing the Avaya Workspaces® Framework	3.0	Web-based Training	
24150T	Avaya Workspaces® Framework R3 Test	1.0	Online Test	
ASAC-0005 Avaya Oceana® Administration				
21160W	Avaya Oceana® Fundamentals	0.5	Web-based Training	
24300V	Administering Avaya Oceana® R3 Omnichannel	40.0	Virtual Instructor-Led Training	Attached with the sale
2430T	Administering Avaya Oceana® R3 Online Test	1.0	Online Test	
24320W	Administering Avaya Oceana® - Basic	2.5	Web-based Training	https://www.avaya.com/Oceana-admin

Table continues…

Avaya Learning Center				
Course code	**Course title**	**Course duration in hours**	**Delivery type**	**Vanity Link for Attachment**
ASAC-0031 Avaya Analytics™ R4 for Oceana® Administrator				
24380T	Administering Avaya Analytics1M R4 for Oceana8 Specialized Test	1.0	Online Test	

Table 6: Other Miscellaneous Courseware

Course code	Course title	Course duration in hours	Delivery type	Vanity Link for Attachment
ALCC-0001 Avaya Workforce Optimization Select Integration with Avaya Oceana® Workspaces				
7014W	Integrating Avaya Workforce Optimization Select with Avaya Oceana® Workspaces	3.0	Web-based Training	
7014A	Avaya Workforce Optimization Select with Avaya Oceana® Workspaces Integration Assessment	1.0	Assessment	
71610W	Integrating POM with Avaya Oceana®	1.0	Web-based Training	

Support

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

Appendix A: Service attributes

Service attributes overview

This section describes how to set the attributes of a service and explains the attributes of the services that you install on Avaya Oceana® clusters.

Setting service attributes

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In the **Cluster** field, select the cluster that hosts the service.
   b. In the **Service** field, select the service.
3. Configure the attributes of the service.
4. Click **Commit**.

CallServerConnector attributes

Startup Configuration

Name	Description
Solution type	The type of solution in which the CallServerConnector service is used. For Avaya Oceana®, select `Oceana`.
Number of Communication Managers	The number of Communication Managers that your solution supports. For Avaya Oceana®, select `1`.

Table continues…

Name	Description
Deployment type	The deployment type that determines the memory size of processing units. • For an Avaya Oceana® deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® deployment that supports up to 100 active agents, select `OCEANA_SMALL`.
Deploy CSC	The attribute that enables or disables the deployment of GigaSpaces Processing Unit. To enable the deployment of GigaSpaces Processing Unit, select `true`.

Startup Configuration - Communication Manager 1

Name	Description
Voice Provider Id	The name of the Voice provider (Type:CM) that you plan to configure in Avaya Control Manager.
Application Enablement Services' IP addresses	The IP address of the Application Enablement Services server that you plan to connect to Communication Manager through a TSAPI link. If two instances of Application Enablement Services are used for HA, click the plus sign (**+**) and add the second instance of Application Enablement Services.
Application Enablement Services Port	The port number of the DMCC server on Application Enablement Services for encrypted connections.
Application Enablement Services User	The user name of the Application Enablement Services account. If two instances of Application Enablement Services are used for HA, the same user name must be configured for both instances.
Application Enablement Services User Password	The password of the Application Enablement Services account. If two instances of Application Enablement Services are used for HA, the same password must be configured for both instances.

Table continues…

Name	Description
Communication Manager Connection Name on Application Enablement Services	The name of the Communication Manager switch connection configured on Application Enablement Services. If two instances of Application Enablement Services are used for HA, the same name must be configured for both instances.

Advanced

Name	Description
Manual memory capacity (MB)	The memory used in the MANUAL deployment type.

ContactCenterService attributes

Startup Configuration

Name	Description
Deployment type	The deployment type that determines the memory size of processing units. • For an Avaya Oceana® deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® deployment that supports up to 100 active agents, select `OCEANA_SMALL`.
Manual memory params for CCService PU	The custom memory parameters for specifying the deployment size of ContactCenterService Processing Unit. These parameters are applicable only for the MANUAL deployment type.
Manual memory params for Affinity Adapter PU	The custom memory parameters for specifying the deployment size of Affinity Adaptor Processing Unit. These parameters are applicable only for the MANUAL deployment type.

Table continues…

Name	Description
Deploy PU Now	The attribute that enables or disables the deployment of ContactCenterService Processing Unit. To enable the deployment of ContactCenterService Processing Unit, select `true`.
Common Components Cluster	The cluster that hosts Unified Collaboration Model (UCM) and Unified Collaboration Administrator (UCA) services. To set this attribute, select Avaya Oceana® Cluster 1.
Work Assignment Cluster	The cluster that hosts the Work Assignment snap-in. To set this attribute, select Avaya Oceana® Cluster 1.
Enable Secure Communications	The attribute that enables or disables the secure communications with the other services or snap-ins. To make all inter-component calls over HTTPS, select `true`. Salesforce.com accepts and authorizes applications connections through HTTPS. Therefore, you must configure Avaya Oceana® for HTTPS and start Avaya Workspaces through HTTPS. If you do not use HTTPS, agents cannot log in to Salesforce.com and Avaya Workspaces to automatically retrieve and view Customer details from Salesforce.com on Voice interactions. **Important:** Ensure that you configure the certificates correctly.
Engagement Designer Cluster	The cluster that hosts the Engagement Designer service. To set this attribute, select Avaya Oceana® Cluster 1.
Timeout values for HTTP Connections to Engagement Designer	The Engagement Designer HTTP connection timeout in milliseconds.

Table continues…

Name	Description
Mapped channels	The values for the channels in the following format: `ChannelA,CHANNEL_A;ChannelB,CHANNEL_B;` The terms `ChannelA` and `ChannelB` specify the UCM channel name, and the terms `CHANNEL_A` and `CHANNEL_B` specify the corresponding Engagement Designer Event Catalog channel postfix for ROUTE_COMMAND events.
Oceana Core Data Service Cluster	The cluster that hosts OceanaCoreDataService. To set this attribute, select Avaya Oceana® Cluster 1.

Advanced Configuration

Name	Description
Engagement Designer URI	The URI endpoint for Engagement Designer.

ContextStoreManager attributes

License Features

Name	Description
FEAT_CS_EXPIRATION	Context Store expiration feature.
VALUE_CS_AEP_CONNECTOR	Context Store AEP connector.
VALUE_CS_API	Context Store API.
VALUE_CS_GEO_REDUNDANT_1	Context Store Geo Redundancy.
VALUE_CS_SERVER	Context Store server.
VALUE_CS_USERS	Context Store users.

Startup Configuration

Name	Description
ContextStore DataGrid type	The type of Context Store DataGrid. For Avaya Oceana®, select `STANDARD`.
ContextStore ManagerSpace DataGrid Settings	The comma-separated values of memoryCapacityPerContainer, maximumMemoryCapacity for ContextStore ManagerSpace DataGrid. For example, `128m,256m`. The system interprets the numeric-only values as Mb. To specify the values in Gb, you must add the letter “g” after the number. For example, `1g`.

Table continues…

Name	Description
ContextStoreSpace DataGrid Settings	The comma-separated values of memoryCapacityPerContainer, maximumMemoryCapacity for ContextStoreSpace DataGrid. For example, `512m,10240m`. The system interprets the numeric-only values as Mb. To specify the values in Gb, you must add the letter “g” after the number. For example, `2g`.
Solution Type	The type of deployment. The options are: • Standalone • Oceana • Elite

External Data Mart Configuration

Name	Description
Secure Connections to EDM	Specifies if communications between the Context Store and the EDM must use a secure connection. The default value is true. **Note:** For unsecured connections from Avaya Oceana® to EDM, you must set the value to false. Unsecured EDM connections are for laboratory use only. They are not intended for Avaya Oceana® instances that confirm to security policies.
EDM: Disable persistence of personally identifiable data	The attribute to ensure that any potentially personally identifiable, such as, the data field and the collected digits within Avaya Oceana®, are not replicated to External Data Mart. You must enable this attribute if any Personally Identifying Information is written into the data field, or entered into the collected digits, to comply with Data Privacy Laws. For Avaya Oceana®, the default value is `true`.

Table continues…

Name	Description
EDM: Keep closed contacts for	Specifies the period of time for which closed contacts are retained in the EDM. The value range is 0-3650. Setting this attribute to 0 keeps the closed contacts permanently. However, it is not recommended because of performance implications. The default value is 30.
EDM: Run maintenance at hour	The hour of the day at which EDM maintenance runs. The value range is 0-23. The default value is 2 (02:00).
EDM: Mirror Service redo log size	The amount of context data to store for retry if disconnected from External Data Mart (EDM). The system discards the oldest data when this size limit is reached.
EDM: Enable Persistence to database	The attribute that enables or disables the persistence of Context data to EDM. For Avaya Oceana®, select `true`.
EDM: Persistence type	Specifies how the Context Store data is stored in the EDM. For Avaya Oceana®, select **Journey**.
EDM: Database type	The type of the EDM database. For Avaya Oceana®, select **Microsoft SQL Server**.
EDM: Enable Provisioning from database	The attribute that enables or disables the provisioning of Context data to EDM. For Avaya Oceana®, keep the default value `false`.
EDM: TLS version	The TLS version for the connection to the EDM database.
EDM: Database host	The host name of the EDM database.
EDM: Database port	The port number of the EDM database.
EDM: Database name	The name of the EDM database.
EDM: Database username	The user name of the EDM database.
EDM: Database password	The password of the EDM database.
EDM: Mirror Service container size	The memory required to deploy EDM Mirror Service. For example, 1. The system interprets the numeric-only value as GB. To specify the value in MB, you must add the letter “m” after the number. For example, `128m`.

Important:

In an Avaya Oceana® deployment, EDM is a mandatory requirement. For detailed information about EDM, see *Avaya Context Store Snap-in Reference*.

Run-time Service Configuration

Name	Description
Cluster Deny Service on two node outage	The attribute that determines whether to deny or accept a service when two nodes in a cluster are unavailable. If this attribute is disabled, the last remaining node continues to attempt service requests. The permissible values are: • `true`: If two nodes in a cluster are unavailable, the third node also denies service. • `false`: Even if two nodes in a cluster are unavailable, the third node attempts to serve incoming requests. The default value for this attribute is *`false`*. **Note:** This attribute is not applicable for one or two-node deployments.
CS Audit: Event limit	The limit of event entries in the audit trail of context objects. For Avaya Oceana®, enter the value as `1`.
CS Default Lease Time	The default lease time, in seconds, for which context data remains in the in-memory data cache. Context Store automatically removes a context if the context remains in Context Store for the lease period without any change. The default value for this attribute is 7200. You can specify any value between 1 to 86400 to configure this attribute. For values specific to your deployment type, see *Avaya Context Store Snap-in Release Notes*. **Note:** This time is not applicable to the contexts in the CS_PROVISION table, because the contexts in the CS_PROVISION table remain in the data grid permanently until they are deleted manually.

Table continues…

Name	Description
CS Maximum Lease Time	The maximum lease time, in seconds, for the context data. The system logs warnings for leases longer than this value. If the average lease time for the cluster exceeds this value, Context Store raises an error event. If a context is created or updated with a lease time that exceeds this value, Context Store logs only a warning. The default value for this attribute is 14400. You can specify any value between 1 to 86400 to configure this attribute. You can update this attribute dynamically.
CS Threshold: Instance High Requests per Second	High threshold on Context Store instance requests per second. This value must be greater than the related Minima. For a Context Store instance, if the number of requests per second exceeds this value, the instance rejects the further requests and raises an event. The default value for this attribute is 65. You can specify any value between 1 to 650 to configure this attribute. You can update this attribute dynamically. For values specific to your deployment type, see *Avaya Context Store Snap-in Release Notes*. Avaya Oceana® supports a maximum of 10000 active emails when you set the value of this field to `350`. If you upgrade the ContextStoreManager SVAR, you must note down this value before the upgrade and set the same value after the upgrade. **Note:** To support a maximum of 10000 active emails, you must also configure the **Max active Emails** field using the Omnichannel Administration Utility. For more information, see Configuring email settings on page 568.

Table continues…

Name	Description
CS Threshold: Instance Low Requests per Second	Low threshold on Context Store instance requests per second. This value must be lesser than the related Maxima. For a Context Store instance, if the number of requests per second exceeds this value, the instance raises an event, without rejecting any further requests. The default value for this attribute is 55. You can specify any value between 1 to 650 to configure this attribute. You can update this attribute dynamically. For values specific to your deployment type, see *Avaya Context Store Snap-in Release Notes*. Avaya Oceana® supports a maximum of 10000 active emails when you set the value of this field to `330`. If you upgrade the ContextStoreManager SVAR, you must note down this value before the upgrade and set the same value after the upgrade. **Note:** To support a maximum of 10000 active emails, you must also configure the **Max active Emails** field using the Omnichannel Administration Utility. For more information, see Configuring email settings on page 568.
CS Threshold: Max Error Rate	Threshold for maximum tolerated Context Store request error rate in percentage. The default value for this attribute is 20. You can specify any value between 1 to 100 to configure this attribute. You can update this attribute dynamically.
CS Threshold: Max Latency	Threshold for maximum tolerated Context Store request latency in milliseconds. When the average latency exceeds the specified value, Context Store raises an event. The default value for this attribute is 250. You can specify any value between 1 to 5000 to configure this attribute. You can update this attribute dynamically. **Note:** The average latency of a request in an hour is less than 250 milliseconds with a maximum latency of two seconds.

Table continues…

Name	Description
CS Threshold: Service High Requests per Second	High threshold on Context Store service requests per second. This value must be greater than the related Minima. For a Context Store cluster, if the number of service requests per second exceeds this value, Context Store rejects the further service requests and raises an event. The default value for this attribute is 105. You can specify any value between 1 to 1240 to configure this attribute. You can update this attribute dynamically. For values specific to your deployment type, see *Avaya Context Store Snap-in Release Notes*. Avaya Oceana® supports a maximum of 10000 active emails when you set the value of this field to `1240`. If you upgrade the ContextStoreManager SVAR, you must note down this value before the upgrade and set the same value after the upgrade. **Note:** To support a maximum of 10000 active emails, you must also configure the **Max active Emails** field using the Omnichannel Administration Utility. For more information, see Configuring email settings on page 568.

Table continues…

Name	Description
CS Threshold: Service Low Requests per Second	Low threshold on Context Store service requests per second. This value must be lesser than the related Maxima. For a Context Store cluster, if the number of service requests per second exceeds this value, Context Store raises and alarm, without rejecting the further service requests. The default value for this attribute is 85. You can specify any value between 1 to 1240 to configure this attribute. You can update this attribute dynamically. For values specific to your deployment type, see *Avaya Context Store Snap-in Release Notes*. Avaya Oceana® supports a maximum of 10000 active emails when you set the value of this field to `1200`. If you upgrade the ContextStoreManager SVAR, you must note down this value before the upgrade and set the same value after the upgrade. **Note:** To support a maximum of 10000 active emails, you must also configure the **Max active Emails** field using the Omnichannel Administration Utility. For more information, see Configuring email settings on page 568.

Geo Redundancy Configuration

Name	Description
GEO: Enable session preservation	Context Store expiration feature.
GEO: Gateway Service container size	Memory required for Geo-Redundancy Gateway Service deployment. The system interprets a numeric value only as gigabytes. You can specify megabytes with an `m` or `mb` after the number. For example, `2m`. For values specific to your deployment type, see the *Certified Deployments section in Avaya Context Store Snap-in Release Notes*. The default value is *1*.
GEO: Keystore file name	Certificate name of the geo redundancy keystore.
GEO: Keystore password	Password of the geo redundancy keystore.
GEO: Target cluster Id	Name of the target cluster on the geo redundant site

Streams Configuration

Name	Description
Event Stream: Enable Event Streaming	Setting this to 'true' enables clients to subscribe for personalized events from Context Store.

Supplier

Name	Description
Supplier Id	The supplier Id that Avaya provides. The default value is *10000000*.

Advanced Configuration

Name	Description
Enable Centralized Logging	This value indicates that centralized logging is needed by the snap-in. Enables centralized logging after the snap-in is installed.

ContextStoreQuery attributes

Using the ContextStoreQuery service, you can retrieve customer data stored in an External Data Mart (EDM) database. For detailed information about EDM, see *Avaya Context Store Snap-in Reference*.

License Features

Name	Description
FEAT_CS_EXPIRATION	Context Store expiration feature.
VALUE_CS_AEP_CONNECTOR	Context Store AEP connector.
VALUE_CS_API	Context Store API
VALUE_CS_GEO_REDUNDANT_1	Context Store Geo Redundancy
VALUE_CS_SERVER	Context Store server
VALUE_CS_USERS	Context Store users

External Data Mart Configuration

Name	Description
Secure Connections to EDM	Specifies if communications between the Context Store and the EDM must use a secure connection. The default value is true. **Note:** For unsecured connections from Avaya Oceana® to EDM, you must set the value to false. Unsecured EDM connections are for laboratory use only. They are not intended for Avaya Oceana® instances that confirm to security policies.
EDM: Database type	The type of the EDM database. For Avaya Oceana®, select **Microsoft SQL Server**.
EDM: TLS version	The TLS version for the connection to the EDM database.
EDM: Database host	The host name of the EDM database.
EDM: Database port	The port number of the EDM database.
EDM: Database name	The name of the EDM database.
EDM: Database username	The user name of the EDM database.
EDM: Database password	The password of the EDM database.
EDM: Maximum Database Query Results	The maximum number of results that a ContextStoreQuery REST APIs return. If a query returns more than this maximum, then only the newest results is returned. The valid range is 50 - 5000. The default limit is set to 1000.

GDPR Redact Configuration

Name	Description
Thread pool size for tasks to delete contexts	The maximum number of threads per cluster node to handle submitted tasks. The range is between 1 and 8. The default value is 4. A snap-in restart is not required to take effect.

Supplier

Name	Description
Supplier Id	The supplier ID that Avaya provides.

Advanced Configuration

Name	Description
Enable Centralized Logging	This value indicates that centralized logging is needed by the snap-in. Enables centralized logging after the snap-in is installed.

ContextStoreRest attributes

License Features

Name	Description
FEAT_CS_EXPIRATION	Context Store expiration feature.
VALUE_CS_AEP_CONNECTOR	Context Store AEP connector.
VALUE_CS_API	Context Store API.
VALUE_CS_GEO_REDUNDANT_1	Context Store Geo Redundancy.
VALUE_CS_SERVER	Context Store server.
VALUE_CS_USERS	Context Store users.

Advanced Configuration

Name	Description
Address of Authorization Service	The FQDN or IP address of the cluster that hosts AuthorizationService.
Enable Breeze Authorization Service	The attribute that enables or disables the requirement for authentication, for Breeze authorization service. • To disable authentication, keep the default value `false`. • To enable authentication, select `true`.

Table continues…

Name	Description
Require user for Breeze Authorization Service	Setting this to `true` enforces user access only for the Breeze Authorization Service. If you enable this attribute, the system disables the Get Token and Get Token by Scope API methods. If you disable this attribute, you can no longer generate a token without providing valid user credentials. The accepted values are: • `true` • `false` The default value is `false`. • To disable user authentication, keep the default value `false`. • To enable user authentication, select `true`.
Enable Centralized Logging	This value indicates that centralized logging is needed by the snap-in. Enables centralized logging after the snap-in is installed.

External Data Mart Configuration

Name	Description
Enable Retrieval From Database	The attribute that enables or disables retrieval of Context data from External Data Mart when expired in Context Store Space. • To disable centralized logging, select `false`. • To enable centralized logging, keep the default value `true`.

Supplier

Name	Description
SupplierId	The supplier Id that Avaya provides.

Support for CustomerJourneyService attributes

When an agent accepts an interaction within in Avaya Workspaces, the Customer Journey widget is populated using the Customer Journey Service APIs. You must configure CustomerJourneyService attribute to connect to the External Data Mart for the optimized database schema provided for customer journey data with Avaya Oceana® Release 3.8.

License Features

Name	Description
FEAT_CS_EXPIRATION	Context Store expiration feature.
VALUE_CS_AEP_CONNECTOR	Context Store AEP connector.
VALUE_CS_API	Context Store API.
VALUE_CS_GEO_REDUNDANT_1	Context Store Geo Redundancy.
VALUE_CS_SERVER	Context Store server.
VALUE_CS_USERS	Context Store users.

Startup Configuration

Name	Description
Context Store Cluster Address	The cluster that hosts Context Store services. To set this attribute, select Avaya Oceana® Cluster 1.
OmniChannelProvider Cluster Address	The name of the Omnichannel Provider Breeze cluster. IP address or a Fully Qualified Domain Name is retrieved using this name.
Omnichannel Provider Data Services Cluster	The cluster containing the Omnichannel Provider Data Services service.

Supplier

Name	Description
Supplier Id	The supplier Id that Avaya provides. The default value is *10000000*.

Run-time Service Configuration

Name	Description
Enable Secure Communications	The attribute that enables or disables the secure communications with the other services or snap-ins. To make all inter-component calls over HTTPS, select `true`. Salesforce.com accepts and authorizes application connections through HTTPS. Therefore, you must configure Avaya Oceana® for HTTPS and start Avaya Workspaces through HTTPS. If you do not use HTTPS, agents cannot log in to Salesforce.com.Avaya Workspaces to automatically retrieves and view Customer details from Salesforce.com on Voice interactions. **Important:** Ensure that you configure the certificates correctly.
Authorization Required to contact the Customer Journey Service	The attribute that enables or disables user authentication for contacting CustomerJourneyService. • To disable authentication, keep the default value `false`. • To enable authentication, select `true`.
Oceana Authorization cluster IP	The FQDN or IP address of the cluster that hosts AuthorizationService. • For an Avaya Oceana® deployment that supports up to 100 active agents, enter the FQDN or IP address of Avaya Oceana® Cluster 1. • For an Avaya Oceana® deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, enter the FQDN or IP address of Avaya Oceana® Cluster 2. **Important:** Authorization is always enabled to access OceanaMonitor. If authorization is not configured, use EASG authorization.
OmniChannelProvider services public address	Externally available address of the OCP cluster. Must be an IP address or an FQDN.
Context Store services public address	Externally available address of the Context Store cluster. Must be an IP address or an FQDN.

External Data Mart Configuration

Name	Description
Secure Connections to EDM	Specifies if communications between the Context Store and the EDM must use a secure connection. The default value is true. **Note:** For unsecured connections from Avaya Oceana® to EDM, you must set the value to false. Unsecured EDM connections are for laboratory use only. They are not intended for Avaya Oceana® instances that confirm to security policies.
EDM: Database type	The type of the EDM database. For Avaya Oceana®, select **Microsoft SQL Server**.
EDM: TLS version	The TLS version for the connection to the EDM database.
EDM: Database host	The host name of the EDM database.
EDM: Database port	The port number of the EDM database.
EDM: Database name	The name of the EDM database.
EDM: Database username	The user name of the EDM database.
EDM: Database password	The password of the EDM database.
EDM: Maximum Database Query Results	The maximum number of results that ContextStoreQuery REST APIs. The valid range is 50-5000.

Customer Journey Admin Configuration

Name	Description
AutoFilter Customer Journey By:	The attribute that enables auto filter by current Account ID in the Customer Journey Widget. To set this attribute, select **Account Id**.
Agent Note Enabled:	The attribute that enables updating Agent Note in the Customer Journey Widget. To set this attribute, select `true`.
Hide Transcripts Button:	The attribute enables to Customer Journey transcripts. It affects all agents. To set this attribute, select `true`.
Manual assignment of Account ID for work requests	The attribute that allows the agent to assign Account Id for the current interaction in the CustomerJourney widget.

Table continues…

Name	Description
Display button more data	The **More data** button is not displayed by default from the 3.8.0.0 release. This attribute allows to show the **More data** button in the CustomerJourney widget. To set this attribute, select `true`.
Hide transcripts button	The attribute that allows to restrict access to Customer Journey transcripts. It affects all agents. To set this attribute, select `true`.

CustomerManagement attributes

License Features

Name	Description
FEAT_AOC_BASE	AOC Base
VALUE_AOC_ADMIN_USER	Number of AOC Admin Users.
VALUE_AOC_AGENT_DESKTOP_USER	Number of AOC Agent Desktop Users.
VALUE_AOC_ANAYLTICS_USER	Number of AOC Analytics Users.
VALUE_AOC_CHAT_USER	Number of AOC Chat Users.
VALUE_AOC_COBROWSE_USER	Number of AOC Co-Browse Users.
VALUE_AOC_CORE_COMPONENTS	AOC Core Components.
VALUE_AOC_DIGITAL_AUDIO_USER	Number of AOC Digital Audio Users.
VALUE_AOC_EMAIL_USER	Number of AOC Email Users.
VALUE_AOC_INTERACTIONS_USER	Number of AOC Customer Interactions.
VALUE_AOC_PHONE_USER	Number of AOC Phone Users.
VALUE_AOC_SM_USER	Number of AOC Social Media Users.
VALUE_AOC_SMS_USER	Number of AOC SMS Users.
VALUE_AOC_SUPERVISOR_USER	Number of AOC Supervisor Users.
VALUE_AOC_VIDEO_USER	Number of AOC Video Users.
VALUE_AOC_WORKSPACES_SDK_USER	Number of AOC SDK Workspace Users.
VALUE_AOC_WORKSPACES_USER	Number of AOC Workspaces Users.

Startup Configuration

Name	Description
Omnichannel Provider Data Services Cluster	The cluster containing the Omnichannel Provider Data Services service.

Table continues…

Name	Description
OmniChannelProvider Cluster Address	The cluster that hosts Omnichannel Provider services. To set this attribute, select Avaya Oceana® Cluster 3.
Monitor OmniChannelProvider Connection	The attribute that enables or disables status check on the Omnichannel Provider connection every 60 seconds. • To enable status check, keep the default value `true`. • To disable status check, select `false`.
Context Store Cluster Address	The cluster that hosts Context Store services. To set this attribute, select Avaya Oceana® Cluster 1.
Monitor Context Store Connection	The attribute that enables or disables status check on the Context Store connection every 60 seconds. • To enable status check, keep the default value `true`. • To disable status check, select `false`.

Advanced Configuration

Name	Description
Enable Secure Communications	The attribute that enables or disables the secure communications with the other services or snap-ins. To make all inter-component calls over HTTPS, select `true`. Salesforce.com accepts and authorizes applications connections through HTTPS. Therefore, you must configure Avaya Oceana® for HTTPS and start Avaya Workspaces through HTTPS. If you do not use HTTPS, agents cannot log in to Salesforce.com and Avaya Workspaces to automatically retrieve and view Customer details from Salesforce.com on Voice interactions. **Important:** Ensure that you configure the certificates correctly.
Retrieve customer information from CRM	The attribute that enables or disables merging of CRM data into the Oceana customer database.

Table continues…

Name	Description
CRM Connector Cluster Address	The address of the CRMGateway Breeze cluster. You can enter only an IP address or a Fully Qualified Domain Name. For example, w.x.y.z or abc.avaya.com.
CRM Settings	The various CRM settings in json format. For CRMGateway, Avaya Oceana® supports selective fields. Using the selective fields feature, you can request for specific CRM details instead of a full record. For example, customerEmails, customerAccounts, and lastUpdatedTimeStamp.
Monitor CRM Connection	The attribute that enables or disables status check on the CRM connection every 60 seconds. • To enable status check, keep the default value `true`. • To disable status check, select `false`.
Timeout for the rest services (in milliseconds)	The attribute that defines the timeout for all calls to external rest-services.
Enable Centralized Logging	This value indicates that the Centralized Logging is needed by the snap-in. Enables Centralized Logging once snap-in is installed.

Supplier

Name	Description
Supplier Id	The supplier ID that Avaya provides.

EngagementDesigner attributes

DEFAULT_GROUP

Name	Description
Treat error handled instances like successfully completed instance	The attribute that determines whether the error handled instances are treated like successfully completed instances for delete operation. To set this attribute, select `true`.
ChatBot Cluster(s)	The cluster that hosts the BotConnector service. • For an Avaya Oceana® deployment that supports up to 100 active agents, select Avaya Oceana® Cluster 1. • For an Avaya Oceana® deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, select Avaya Oceana® Cluster 2.

Table continues…

Name	Description
Completed instance to be deleted or not	The attribute that enables or disables the deletion of completed instances. If you set this attribute to `true`, the completed instances are deleted immediately after completion. If you set this attribute to `false`, the completed instances are deleted periodically based on the **Number of days the data user want to retain** property.
Context Store Cluster(s)	The cluster that hosts Context Store services. To set this attribute, select Avaya Oceana® Cluster 1.
Customer Management Cluster(s)	The cluster that hosts the CustomerManagement service. To set this attribute, select Avaya Oceana® Cluster 1.
Debugger Service Profile	The attribute that specifies the service profile for WebRTC debugger.
Deployment type	The attribute that specifies the type of deployment. Select **Oceana deployment** or **Breeze only deployment**.
Engagement Call Control server FQDN/IP address	The attribute that specifies the FQDN/IP of Engagement Call Control server.
Error rate threshold percentage	Error rate threshold percentage is 50%.
Experience Portal Manager (Primary)	Host address of the Primary Experience Portal Manager.
Experience Portal Manager (Secondary)	Host address of the Secondary Experience Portal Manager.
Experience Portal Manager User Name	Experience Portal Manager username.
Experience Portal Manager User Password	Experience Portal Manager user password.
Locale	The prompt language that Avaya Aura® Media Server supports. To set this attribute, enter the value `en_us`. **Note:** Set this attribute only if you deploy Avaya Aura® Media Server.

Table continues…

Name	Description
Maximum limit for the number of error instances to be retained	The value sets the limit for the number of errors or error handled instances to be retained in the system for the duration set by 'Number of days the user wants to retain error instances'. The default value is 2000. Increasing this value has impact on the disk usage and performance.
Maximum number of matching WFI's to be shown on instance tab	The number of latest WFI's to be shown on the **Instance** tab. To set this attribute, enter the value `200`. **Note:** Set this attribute only if you deploy Avaya Aura® Media Server.
Maximum Retry Time in seconds to get DB connection after call reconstruction	The retry time in seconds to get database connection after call reconstruction. To set this attribute, enter the value `20`. **Note:** Set this attribute only if you deploy Avaya Aura® Media Server.
Media Server Inclusion	The attribute that enables or disables the inclusion of Avaya Aura® Media Server. To configure Avaya Oceana® for Web Voice/Video, set the value to `true`. **Note:** Set this attribute only if you deploy Avaya Aura® Media Server.
Number of days the data user want to retain	The attribute to cleanup completed instances, 0 - means user wants to cleanup completed instances which are 15 minutes old, 1 - means user wants to cleanup completed instances which are 1 day old.
Number of days the user want to retain active instances	The attribute that controls the number of days the ED flows remain active. This attribute is significant for contact types such as email and generic channel where it is not necessary to route immediately to agents. For example, if an agent is unavailable to service emails on a particular day, then the next day, the flows are removed from ED and the contact cannot reach the agent.

Table continues…

Name	Description
Number of days the user want to retain archival run summary	The attribute to clear the cleanup runs, 0 - means user wants to cleanup the runs which are 15 minutes old, 30 - means user wants to cleanup the runs which are 30 days old.
Number of days the user want to retain error instances	The attribute to cleanup error instances, 0 - means user wants to cleanup error instances which are 15 minutes old, 7 - means user wants to cleanup error instances which are 7 days old.
Number of days the user wants to retain the last agent records for contacts	0 - means user want to cleanup last agent records which are 15 minutes old, 30 - means the user wants to retain the last agent records for contacts for 30 days. When the same customer calls back in 30 days or less, the customer can be routed to the same agent if required. This data is removed after 30 days.
Number of instances for calculating error rate	Error rate is calculated for instances more than 25.
Number of threads available for executing asynchronous tasks within Engagement Designer	Increase or decrease as appropriate based on load. Minimum is 10 and maximum is 50.
Site ID(s)	The Site ID of the BotConnector service followed by `:FriendlyName`. For example, `iasljety4so7:FriendlyName`.
UCA Cluster(s)	The cluster that hosts Unified Collaboration Administrator (UCA) services. To set this attribute, select Avaya Oceana® Cluster 1.
UCM Cluster(s)	The cluster that hosts Unified Collaboration Model (UCM) services. To set this attribute, select Avaya Oceana® Cluster 1.
Work Assignment Attributes	The attributes that you must set while configuring Voice Self Service through Call Center Elite.
Work Assignment Cluster(s)	The cluster that hosts the Work Assignment snap-in. To set this attribute, select Avaya Oceana® Cluster 1.

Client Attributes

Name	Description
Authorization Service Address	The IP address or FQDN of the cluster that hosts AuthorizationService.

License Features

Name	Description
VALUE_CD_BASE	Maximum Collaboration Designer Base.
VALUE_CD_DEVELOPER	Maximum Collaboration Designer Developers.
VALUE_CD_IVR_TASK	IVR task feature.

Salesforce CRM Login Information

Name	Description
Salesforce Login URL	URL used to login Salesforce Account.
Salesforce Login UserName	User Name used to login Salesforce Account.
Salesforce Login User Password	User Password used to login Salesforce Account.
Salesforce Login User Password Security Token	User Password SecurityToken used to login Salesforce Account.
Salesforce Login ClientId	The Client ID for login Salesforce Account.
Salesforce Login Client Secret	The Client Secret for login Salesforce Account.

Advanced

Name	Description
Enable Centralized Logging	This value indicates that centralized logging is needed by the snap-in. Enables centralized logging after the snap-in is installed.

OceanaCoreDataService attributes

Advanced

Name	Description
Enable Centralized Logging	The attribute that enables Centralized Logging after snap-in is installed. To set this attribute, select `true`.

External Data Mart Configuration

Name	Description
Enable Retrieval From Database	The attribute that enables or disables retrieval of Context data from External Data Mart when the data is unavailable in Context Store Space.

Oceana Core Data Service API Configuration

Name	Description
Timeout for Oceana Core Data Service Requests	The attribute that sets the timeout requests that are serviced by Oceana Core Data Request in milliseconds. The default value is 20000.

Run-time Service Configuration

Name	Description
Authorization Required to contact the OceanaCoreDataService	The attribute that enables or disables user authentication for contacting OceanaCoreDataService. • To disable authentication, keep the default value `false`. • To enable authentication, select `true`.
Oceana Authorization cluster IP	The FQDN or IP address of the cluster that hosts AuthorizationService. • For an Avaya Oceana® deployment that supports up to 100 active agents, enter the FQDN or IP address of Avaya Oceana® Cluster 1. • For an Avaya Oceana® deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, enter the FQDN or IP address of Avaya Oceana® Cluster 2. **Important:** Set this attribute only if you enable user authentication for contacting OceanaCoreDataService.

Supplier

Name	Description
Supplier Id	The supplier Id that Avaya provides. The default value is 10000000.

OceanaMonitorService attributes

Deployment

Name	Description
Deployment Type	The type that determines the deployment size for the installation. • For an Avaya Oceana® deployment that supports up to 4500 active agents, select `3X Large`. • For an Avaya Oceana® deployment that supports up to 2000 active agents, select `Extra Large`. • For an Avaya Oceana® deployment that supports up to 1000, 500, or 250 active agents, select `Large`. • For an Avaya Oceana® deployment that supports up to 100 active agents, select `Small`.
Locale	The locale or language for the installation.
Secure Communications	The attribute that enables or disables the secure communications across the clusters in the installation. For Https-only and wss-only connections across the clusters, select `Enabled`.
Allow Tokenless Access	The attribute that allows the requests to access resource end-points without any authorization token. To allow tokenless access, retain the default value `false`.

Advanced

Name	Description
Client Redirection path	Oceana Monitor uses the path, `/services/OceanaMonitorService/manager.html?affinity=attribute` to redirect the browser to.

Startup Configuration

Name	Description
Common Cluster	To set this attribute, select the common cluster for the installation.
Context Store Cluster	To set this attribute, select the cluster where Context Store is located for the installation.

Table continues…

Name	Description
Co-Browse Cluster	To set this attribute, select the cluster where Co-Browse is located for the installation.
OCP Cluster	To set this attribute, select the cluster where the multimedia snap-ins are located for the installation.
Customer Management Cluster	To set this attribute, select the cluster where Customer Management is located for the installation.
Chatbot Cluster	To set this attribute, select the cluster where Chatbot is located for the installation.
Unified Agent Cluster	To set this attribute, select the cluster where Unified Agents snap-ins are located for the installation.
Cluster 1	To set this attribute, select Avaya Oceana® Cluster 1.
Cluster 2	• For an Avaya Oceana® deployment that supports up to 100 active agents, select Avaya Oceana® Cluster 1. • For an Avaya Oceana® deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, select Avaya Oceana® Cluster 2.
Cluster 3	To set this attribute, select Avaya Oceana® Cluster 3.
Cluster 4	To set this attribute, select Avaya Oceana® Cluster 4.
Cluster 5	To set this attribute, select Avaya Oceana® Cluster 5.
Secure Connection	The attribute that enables or disables the secure connection of OceanaMonitorService with the other services. To enable the secure connection, select `true`.

Feature configuration

Name	Description
Voice Channel	If the Avaya Oceana® deployment has the Voice Channel feature, select `true`.
Video Channel	If the Avaya Oceana® deployment has the Video Channel feature, select `true`.
Chat Channel	If the Avaya Oceana® deployment has the Chat Channel feature, select `true`.
Email Channel	If the Avaya Oceana® deployment has the Email Channel feature, select `true`.

Table continues…

Name	Description
SMS Channel	If the Avaya Oceana® deployment has the SMS Channel feature, select `true`.
Social Channel	If the Avaya Oceana® deployment has the Social Channel feature, select `true`.
Generic Channel	If the Avaya Oceana® deployment has the Generic Channel feature, select `true`.
Asynchronous Messaging Channel	If the Avaya Oceana® deployment has the Asynchronous Messaging Channel feature, select `true`.
Customer Journey	If the Avaya Oceana® deployment has the Customer Journey feature, select `true`.
Outbound	If the Avaya Oceana® deployment has the Outbound Channel feature, select `true`.
Automation	If the Avaya Oceana® deployment has the Automation feature, select `true`.
Reporting	If the Avaya Oceana® deployment has the Reporting feature, select `true`.

Run-time Service Configuration

Name	Description
Oceana Authorization cluster IP	The FQDN or IP address of the cluster that hosts AuthorizationService. • For an Avaya Oceana® deployment that supports up to 100 active agents, enter the FQDN or IP address of Avaya Oceana® Cluster 1. • For an Avaya Oceana® deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, enter the FQDN or IP address of Avaya Oceana® Cluster 2. **Important:** Set this attribute only if you enable user authentication for viewing Oceana Monitor Service pages.
EASG authorization enabled in Oceana Monitor	The attribute that enables or disables EASG authorization for the Oceana Monitor. • To enable EASG authentication, keep the default value `true`. • To disable EASG authentication, select `false`. Restart the snap-in for the changes to reflect.

Advanced Configuration

Name	Description
Anti-CSRF token validity time	The attribute that specifies the duration of the anti-SCRF tokens generated by the server. If the server receives a POST, PUT, DELETE request with anti-SCRF tokens that are older than this value, the service do not accept the request for processing. The values ranges from 1 to 24. But, the default value is 2.
Support logging web session identity information in OceanaMonitor	The attribute that enables or disables logging web session identity. To set this attribute, select `true`.
Enable Centralized Logging	The attribute that enables Centralized Logging after snap-in is installed. To set this attribute, select `true`.

EASG authentication config

Name	Description
Number of retries to connect to CECommonSpace	The attribute that specifies the number of times the Oceana Monitor Service retries to connect to the CECommonSpace. The default value is 60.
Time delay between attempts to connect to CECommonSpace	The attribute that specifies the delay between Oceana Monitor Service attempts to connect to CECommonSpace in milliseconds. The default value is 30000.

Supplier

Name	Description
Supplier Id	The Avaya supplier ID.

OmniCenterProvisioningCollector attributes

Advanced

Name	Description
Message time to live	The time in minutes for which the messages produced by the collector remain available.

Table continues…

Name	Description
Number of Queues supported	The number of supported ActiveMQ queues. The minimum value for the supported ActiveMQ queues is 2 and the maximum value for the supported ActiveMQ queues is 20. If you enter a value lesser than the minimum value, the system ignores the entered value and uses the minimum value. Similarly, if you enter a value greater than the maximum value, the system ignores the entered value and uses the maximum value.
Number of Connection Recovery attempts	The number of retry attempts that must be made to reconnect before tearing down the connection. The default value of this attribute is 5 and the default period between retry attempts is 30 seconds. The system ignores the value which is lesser than the default value.

Note:

If you modify OmniCenterProvisioningCollector attributes separately at a later time, you must reinstall the OmniCenterProvisioningCollector SVAR on Avaya Oceana® Cluster 1.

UCAStoreService attributes

Startup Configuration

Name	Description
Deployment type	The deployment type that determines the memory size of processing units. • For an Avaya Oceana® deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® deployment that supports up to 100 active agents, select `OCEANA_SMALL`.
Persistence configuration	The attribute that ensures the persistence of the data to the local cluster database. For Avaya Oceana®, select `OCEANA_DATABASE`.

Table continues…

Name	Description
Disaster recovery role	For information about this attribute, see *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.
OCPDataServices Cluster	The cluster that hosts OCPDataServices. To set this attribute, select Avaya Oceana® Cluster 1.

Advanced

Name	Description
Enable Tokenless Access	The attribute that enables the requests to access resource end-points without the need of the Authorization token. To enable tokenless access, select `TRUE`.

UCMDataCollector attributes

Startup Configuration

Name	Description
Deployment type	The deployment type that determines the memory size of processing units. • For an Avaya Oceana® deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® deployment that supports up to 100 active agents, select `OCEANA_SMALL`.
Manual memory params UCM DC PU	The attribute that allows the passing in of custom memory parameters for specifying the deployment size of Unified Collaboration Model Data Collector Processing Unit. • For an Avaya Oceana® deployment that supports up to 1000, 500, or 250 active agents, enter the value `1024,6144,0,1`. • For an Avaya Oceana® deployment that supports up to 100 active agents, enter the value `256,1536,0,1`.

Table continues…

Name	Description
Command line params UCM DC PU	The attribute that allows the passing in of command line parameters to Unified Collaboration Model Data Collector Processing Unit.

UCMService attributes

Startup Configuration

Name	Description
Deployment type	The deployment type that determines the memory size of processing units. • For an Avaya Oceana® deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® deployment that supports up to 100 active agents, select `OCEANA_SMALL`.
Oceana Core Data Service Cluster	The cluster that hosts OceanaCoreDataService. To set this attribute, select Avaya Oceana® Cluster 1.

Data Collector Settings

Name	Description
DC ADAPTOR: Enable deployment	The attribute that enables or disables the notifications to be sent out from UCMService. To enable the notifications, select `true`. **Note:** You must set this attribute to `true` if you deploy Avaya Analytics™.

Advanced

Name	Description
Oceana Core Data Service URI	The URI for accessing the cluster that hosts OceanaCoreDataService.

WorkAssignmentManagerService attributes

Startup Configuration

Name	Description
Work Assignment Deployment Type	The deployment type that determines the memory size of processing units. • For an Avaya Oceana® deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® deployment that supports up to 100 active agents, select `OCEANA_SMALL`.
Lookup Locators for Common Spaces	The cluster that hosts Unified Collaboration Model (UCM) and Unified Collaboration Administrator (UCA) services. To set this attribute, select Avaya Oceana® Cluster 1.
Deploy the Metrics PU	The attribute that enables or disables the deployment of all the configured Work Assignment Grid components. To enable the deployment of Work Assignment Grid components, select `true`. If you set this attribute when WorkAssignmentManagerService is running, the changes of this attribute are automatically applied and the wa-metrics-agent-pu is deployed. You can verify the deployment of the wa-metrics-agent-pu through Oceana Monitor Service. The Metrics PU takes the metrics from Work Assignment and forwards them to Avaya Analytics™ through UCMService/UCMDataCollector. For IVR and Callback Assist, the Metrics PU also checks the system for estimated wait time (EWT) and staffed agents.

Advanced Configuration

Name	Description
Longest time since last contact center interaction	The attribute that enables or disables Aux Gaming Prevention. To enable Aux Gaming Prevention, select `true`. **Note:** You can modify this attribute at run-time even after creating the cluster.
Channel Overload Buffer Percentage	The percentage change required to trigger changing agents to the most overloaded channel. For example, if Voice is 50% over Reserve Level Threshold (RLT) and Chat is 40% over RLT, Voice is considered as the most overloaded channel if this attribute is set to 10. The default value of this attribute is 10.
Enable UCM Reporting Events	Enables or disables the Work Assignment interactions to be written into the UCM model. To enable the Work Assignment interactions to be written into the UCM model, select `true`.

IMPU Configuration

Name	Description
IMPU WorkItem Queued state for Chat timeout in milliseconds	The timeout of the Chat WorkItem Queued state in milliseconds. The value of this attribute must be a positive integer with a minimum value of 1 and a maximum value of 999999999. The default value of this attribute is 10800000.
IMPU WorkItem Queued state for Email timeout (value)	The timeout of the Email WorkItem Queued state in time units that are selected in the attribute IMPU WorkItem Queued state for Email timeout time unit (milliseconds or days). The value of this attribute must be a positive integer with a minimum value of 1 and a maximum value of 2073600000 (if in milliseconds) or 100 (if in days). The default value of this attribute is 604800000. You must set the value above the maximum number of days that you expect the emails to be in the queue. Include the holiday periods when email responses can be delayed.

Table continues…

Name	Description
IMPU WorkItem Queued state for Email timeout time unit	The time unit to set IMPU WorkItem Queued state for Email timeout. Select the time unit from the list. Supported time units are milliseconds and days. The default time unit is milliseconds.
IMPU WorkItem Queued state for Generic Channel timeout in milliseconds	The timeout of the Generic channel WorkItem Queued state in milliseconds. The default value of this attribute is 604800000.
IMPU WorkItem Queued state for SMS timeout in milliseconds	The timeout of the SMS WorkItem Queued state in milliseconds. The default value of this attribute is 43200000.
IMPU WorkItem Queued state for Social timeout in milliseconds	The timeout of the Social WorkItem Queued state in milliseconds. The default value of this attribute is 604800000.
IMPU WorkItem Queued state for Messaging timeout in milliseconds	The timeout of the Messaging WorkItem Queued state in milliseconds. The value of this attribute must be a positive integer with a minimum value of 1 and a maximum value of 999999999. The default value of this attribute is 604800000.
IMPU WorkItem Queued state timeout in milliseconds	The timeout of the WorkItem Queued state for all other channels that do not have a specific timeout. This value is in milliseconds. The default value of this attribute is 3600000.

AuthorizationService attributes

Authorization Attributes

Name	Description
Token validity time	The time in hours for which the authorization token remains valid. You can specify any value between 1 to 24 to configure this attribute.
Client JWT Validity Time	The time in seconds for which the JWT generated by the client application remains valid. You can specify any value between 60 to 300 to configure this attribute.
Authorization Grant Expiry	The time in seconds for which an authorization grant remains valid. The default value for this attribute is 15. You can specify any value between 10 to 40 to configure this attribute.

Table continues…

Name	Description
Browser Cookies	The attribute that enables of disables browser cookies to maintain an authenticated session.
Allow Public Clients	The attribute that enables public clients to request access token for valid users.

SAML Attributes

Name	Description
SAML Profile	The attribute to start or stop SAML on all nodes in a cluster. To set this attribute, select `Deploy`.

SAML Attributes

Name	Description
UCA Cluster	The cluster that hosts the Unified Collaboration Administrator (UCA) service. To set this attribute, select Avaya Oceana® Cluster 1.

AvayaMobileCommunications attributes

Startup Configuration

Name	Description
Default Web Voice SIP address	The number that you plan to configure in Engagement Designer Event Mapper to trigger the Web Voice workflow.
Default Web Video SIP address	The number that you plan to configure in Engagement Designer Event Mapper to trigger the Web Video workflow.
Common Cluster	The cluster that hosts Unified Collaboration Model (UCM) and Unified Collaboration Administrator (UCA) services. To set this attribute, select Avaya Oceana® Cluster 1.
Context Store Cluster	The cluster that hosts Context Store services. To set this attribute, select Avaya Oceana® Cluster 1.

Table continues…

Name	Description
Customer Management Cluster	The cluster that hosts the CustomerManagement service. To set this attribute, select Avaya Oceana® Cluster 1.
Common cluster data-grid password	The password to secure Avaya Oceana® Cluster 1 if a secure datagrid is enabled on Avaya Oceana® Cluster 1. **Note:** If this attribute is modified after installing the AvayaMobileCommunications service, you must reinstall the service or restart the Avaya Breeze® platform nodes containing the Avaya Mobile Communications snap-in.

Run-time Service Configuration

Name	Description
Secure mode	The attribute that enables or disables the secure communications with the other services or snap-ins. To make all inter-component calls over HTTPS, select `true`.
Default locale	The prompt language that Avaya Aura® Media Server supports. To set this attribute, enter the value `en_us`. **Note:** Set this attribute only if you deploy Avaya Aura® Media Server.
Resource Selection Strategy	Work Assignment Resource Selection Strategy. To set this attribute, enter one of the following values based on your Resource Selection Strategy: • `Most Idle` • `Least Occupied`

Advanced Configuration

Name	Description
Deployment Type	The deployment type that determines the memory size of processing units. • For an Avaya Oceana® deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® deployment that supports up to 100 active agents, select `OCEANA_SMALL`. **Important:** Restart the Avaya Breeze® platform nodes containing the Avaya Mobile Communications snap-in for the **Deployment type** changes to take effect.

BotConnector attributes

Advanced Configuration

Name	Description
Oceana Core Data Service (OCDS) Cluster	The cluster that hosts OceanaCoreDataService. To set this attribute, select Avaya Oceana® Cluster 1.
Enable Oceana Service Monitor Feature	The attribute that enables or disables this snap-in's heartbeat and lifecycle messages to be shown on System Manager Monitoring Service page.
Enable Tokenless Access	The attribute that enables the requests to access resource end-points without the need of the Authorization token. Ensure that you do not change the default value `FALSE`.

Session

Name	Description
Deployment type	The attribute that determines the Processing Units (PUs) to be deployed and the memory size of the PUs. Options are: • OCEANA_LAB • OCEANA_SMALL • OCEANA_MEDIUM • OCEANA_LARGE • OCEANA_XLARGE • OCEANA_3XLARGE • OCEANA_4XLARGE Changing this attribute requires **Stop** and **Start** of BotConnector Service.

UnifiedAgentContextService attributes

Startup Configuration

Name	Description
Deployment Type	The deployment type that determines the memory size of processing units. • For an Avaya Oceana® deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® deployment that supports up to 100 active agents, select `OCEANA_SMALL`.

Table continues…

Name	Description
Enable Secure Communications	The attribute that enables or disables the secure communications with the other services or snap-ins. To make all inter-component calls over HTTPS, select `true`. Salesforce.com accepts and authorizes applications connections through HTTPS. Therefore, you must configure Avaya Oceana® for HTTPS and start Avaya Workspaces through HTTPS. If you do not use HTTPS, agents cannot log in to Salesforce.com and Avaya Workspaces to automatically retrieve and view Customer details from Salesforce.com on Voice interactions. **Important:** Ensure that you configure the certificates correctly.
OCP Api Cluster	The cluster that hosts Omnichannel Provider services. To set this attribute, select Avaya Oceana® Cluster 3.

Advanced Configuration

Name	Description
OCP Channel Chat API URI	The URI for accessing the Omnichannel Chat API service.
OCP Channel Email API URI	The URI for accessing the Omnichannel Email API service.

UnifiedAgentController attributes

Startup Configuration

Name	Description
AADS FQDN	The FQDN of Avaya Aura® Device Services.
AAWG FQDN	The FQDN of Avaya Aura® Web Gateway. **Important:** Do not enter an IP address in this field.
Co-Browse Cluster	The cluster that hosts the CoBrowse service. To set this attribute, select Avaya Oceana® Cluster 4.

Table continues…

Name	Description
Customer Management Cluster	The cluster that hosts the CustomerManagement service. To set this attribute, select Avaya Oceana® Cluster 1.
Deployment Type	The deployment type that determines the memory size of processing units. • For an Avaya Oceana® deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® deployment that supports up to 100 active agents, select `OCEANA_SMALL`.
Enable Secure Communications	The attribute that enables or disables the secure communications with the other services or snap-ins. To make all inter-component calls over HTTPS, select `true`. Salesforce.com accepts and authorizes applications connections through HTTPS. Therefore, you must configure Avaya Oceana® for HTTPS and start Avaya Workspaces through HTTPS. If you do not use HTTPS, agents cannot log in to Salesforce.com and Avaya Workspaces to automatically retrieve and view Customer details from Salesforce.com on Voice interactions. **Important:** Ensure that you configure the certificates correctly.
OCP Api Cluster	The cluster that hosts Omnichannel Provider services. To set this attribute, select Avaya Oceana® Cluster 3.
OCDS Cluster	The cluster that hosts OceanaCoreDataService. To set this attribute, select Avaya Oceana® Cluster 1.

Table continues…

Name	Description
Public Customer Management	The public or external FQDN of the Customer Management cluster. Use this attribute to support a reverse proxy.
Public OCPDS	The public or external FQDN of the OCPDS cluster. Use this attribute to support a reverse proxy.
UCA Cluster	The cluster that hosts the Unified Collaboration Administrator (UCA) service. To set this attribute, select Avaya Oceana® Cluster 1.
UCM Cluster	The cluster that hosts Unified Collaboration Model (UCM) services. To set this attribute, select Avaya Oceana® Cluster 1.

Runtime Configuration

Name	Description
Unified Agent Client Log Upload Location	The location of the shared network folder that all Unified Agent clients can access to upload the logs when the agents select the Upload option.

Advanced Configuration

Name	Description
Customer Management Rest URI	The URI for accessing the cluster that hosts Customer Management Data Service.
Enable Client Logs Download	Set this value to **True** to enable downloading all user-related data from Avaya Workspaces log files. The default setting is **false**.
Enable Web Chat File Transfer	Set this value to **True** to enable web chat file transfer. The default setting is **false**.
OCDS URI	The URI for accessing the cluster that host OceanaCoreDataService.
Remove all Data from Client Logs	Set this value to **True** to remove all user-related data from Avaya Workspaces log files. The default setting is **false**.
User State Command Time Out	The timeout in seconds for which UnifiedAgentController waits before allowing the users to retry changing their User state. The range of values for this attribute is from 20 seconds to 300 seconds, and the default value is 30 seconds.

Table continues…

Name	Description
Enable Agents to clean up Stuck Contacts	Enable to disable the ability for an agent to remove stuck contacts. Set this value to **True** to allow agent to remove stuck interaction. The default setting is **True**.
End Contact Time Out	The timeout in seconds for which UnifiedAgentController waits before allowing the users to remove the stuck contacts. The range of values for this attribute is from 10 seconds to 300 seconds, and the default value is 20 seconds.

AgentControllerService attributes

DEFAULT_GROUP

Name	Description
Supplier Id	The supplier Id that Avaya provides. The default value is 10000000.

Startup

Name	Description
Omnichannel Database Address	The IP address or FQDN of Omnichannel Database.
OmniResourceConnector Cluster	The cluster that hosts ORCRestService. To set this attribute, select Avaya Oceana® Cluster 3.
UnifiedAgentContextService Cluster	The cluster that hosts UnifiedAgentContextService. • For an Avaya Oceana® deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, select Avaya Oceana® Cluster 2. • For an Avaya Oceana® deployment that supports up to 100 active agents, select Avaya Oceana® Cluster 1.

Advanced

Name	Description
Agents count	The number of licensed agents. The default values for the respective deployment types are as follows: • For `OCEANA_3XLARGE`: 2000 • For `OCEANA_XLARGE`: 2000 • For `OCEANA_LARGE`: 2000 • For `OCEANA_MEDIUM` : 1000 • For`OCEANA_SMALL`: 100 **Note:** The default values are dependent on the deployment type. Changing the value affects the number of attachments allowed at a given time. The larger the value, the greater is the number of attachment requests that are allowed.
Attachment Public IP Address	The IP address or FQDN for Avaya Workspaces for Avaya Oceana® agents to handle attachments, when the agents are located outside the customer intranet.
Authorization Service Address	The FQDN or the IP of the node or cluster where the authorization service is installed. **Note:** This is a required attribute for accessing UnifiedAgentController.
Available heap memory percentage threshold	The attribute that defines a minimal safe percentage of available heap memory to the total current heap size. Oceana Monitor runs events if the actual percentage becomes lower than this threshold. Acceptable values are integers from 1 to 99.
Deployment status of ChatMonitorPu	The value that sets the deployment process.
Maximum size of a downloaded attachment	The attribute that defines a maximum size of a downloaded attachment in MB. A warning is shown if the size is greater than the threshold. Acceptable values are whole numbers.
Outgoing REST request timeout	The amount of time (in seconds) that service waits when sending outgoing REST requests. The default value is 20 seconds.
Password for the Omnichannel Database	The password for Omnichannel Database.

Table continues…

Name	Description
Secure Connections to Omnichannel Database	The attribute that toggles a secure connection to Omnichannel Database. To set this attribute, select `true`.
Tasks In Queue Error Threshold	The number of times tasks in a queue for executor exceed a threshold before a warning event is raised in Oceana Monitor. **Note:** The next warning event is raised only after the timeout of this attribute.
Tasks In Queue Error Timeout	The amount of time (in minutes) since last raised warning event until raising of next warning event in OceanaMonitor for the same executor.
Tasks In Queue Threshold	The max number of tasks in queue for executor before starting of errors number calculation.
Thread pool size for the Omnichannel Database	The number of concurrent connections to the Omnichannel Database. You can select any number from 1 to 500.
Toggle Secure Mode	The attribute that toggles all secure connections, except the connection to Omnichannel Database. To set this attribute, select `true`.
Username for the Omnichannel Database	The user name for Omnichannel Database.
Enable Centralized Logging	The attribute that enables Centralized Logging after snap-in is installed. To set this attribute, select `true`.

AutomationController attributes

Startup

Name	Description
Omnichannel Database Address	The IP address or FQDN of Omnichannel Database.
OmniResourceConnector Cluster	The cluster that hosts ORCRestService. To set this attribute, select Avaya Oceana® Cluster 3.

Advanced

Name	Description
Password for the Omnichannel Database	The password for Omnichannel Database.

Table continues…

Name	Description
Secure Connections to Omnichannel Database	The attribute that toggles a secure connection to Omnichannel Database. To set this attribute, select `true`.
Toggle Secure Mode	The attribute that toggles all secure connections, except the connection to Omnichannel Database. To set this attribute, select `true`.
Username for the Omnichannel Database	The user name for Omnichannel Database.

CustomerControllerService attributes

Startup

Name	Description
Omnichannel Database Address	The IP address or FQDN of Omnichannel Database.
OmniResourceConnector Cluster	The cluster that hosts ORCRestService. To set this attribute, select Avaya Oceana® Cluster 3.
WorkAssignment Cluster	The cluster that hosts the Work Assignment snap-in. To set this attribute, select Avaya Oceana® Cluster 1.

Advanced

Name	Description
Agents count	The number of licensed agents. With this attribute, you can define the maximum contact rate for Chat, SMS, and Social Media contacts that match the supported capacity for the number of agents configured. The default value is 1000 agents supporting a maximum contact rate of 1000 contacts per channel. Based on your deployment type, set the value of this attribute as follows: • For the `OCEANA_3XLARGE` deployment type, set this attribute to `2000`. • For the `OCEANA_XLARGE` deployment type, set this attribute to `2000`. • For the `OCEANA_LARGE` deployment type, set this attribute to `2000`. • For the `OCEANA_MEDIUM` deployment type, set this attribute to `1000`. • For the `OCEANA_SMALL` deployment type, set this attribute to `100`.
Attachment Public IP Address	The IP address or FQDN for Avaya Workspaces agents to interact with attachments when situated outside the customer Intranet. You must restart the Avaya Breeze® platform nodes for the changes to the **Attachment Public IP Address** attribute to take effect.
Deployment Type	The deployment type that determines the memory size of processing units. • For an Avaya Oceana® deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® deployment that supports up to 100 active agents, select `OCEANA_SMALL`.

Table continues…

Name	Description
Filtering failure alarm threshold	The number of messaging transcript filtering requests that must fail in a 30-minute window before an alarm is raised. This value applies only if a messaging transcript filtering service is configured. The range of values for this attribute is from 5 to 10000. The following are the default values of this attribute: • For Small deployments, the default value is 5. • For Medium deployments, the default value is 20. • For Large deployments, the default value is 60. • For Extra Large deployments, the default value is 120. • For 3X Large deployments, the default value is 120.
Password for the Omnichannel Database	The password for Omnichannel Database.
Secure Connections to Omnichannel Database	The attribute that toggles a secure connection to Omnichannel Database. To set this attribute, select `true`.
Toggle Secure Mode	The attribute that toggles all secure connections, except the connection to Omnichannel Database. To set this attribute, select `true`.
Username for the Omnichannel Database	The user name for Omnichannel Database.

EmailService attributes

Startup

Name	Description
Omnichannel Database Address	The IP address or FQDN of Omnichannel Database.
OmniResourceConnector Cluster	The cluster that hosts ORCRestService. To set this attribute, select Avaya Oceana® Cluster 3.

Advanced

Name	Description
Filtering failure alarm threshold	The number of email transcript filtering requests that must fail in a 30-minute window before an alarm is raised. This value applies only if an email transcript filtering service is configured. The range of values for this attribute is from 5 to 10000. The following are the default values of this attribute: • For Small deployments, the default value is 5. • For Medium deployments, the default value is 20. • For Large deployments, the default value is 60. • For Extra Large deployments, the default value is 120. • For 3X Large deployments, the default value is 120.
Mailhandler thread's timeout value	The maximum time in seconds that an email handler thread must take to process a task before timing out and restarting. The task can be sending an email, reading an email, or reading mailboxes. The default value of this attribute is 120 seconds. You must restart the Avaya Breeze® platform nodes that contain EmailService for changes to the **Mailhandler thread's timeout value** attribute to take effect.
Password for the Omnichannel Database	The password for Omnichannel Database.
Secure Connections to Omnichannel Database	The attribute that toggles a secure connection to Omnichannel Database. To set this attribute, select `true`.
Toggle Secure Mode	The attribute that toggles all secure connections, except the connection to Omnichannel Database. To set this attribute, select `true`.

Table continues…

Name	Description
Use secure Ethernet interface	This attribute toggles EmailService to use the Avaya Breeze® platform Asset interface to communicate with the email server. By default, EmailService uses the Avaya Breeze® platform Management interface for communication with the email server. **Note:** The Avaya Breeze® platform Asset interface does not support TLS 1.2 or SMTPS Port 465. You must restart the Avaya Breeze® platform nodes that contain EmailService for changes to the **Use secure Ethernet interface** attribute to take effect.
Username for the Omnichannel Database	The user name for Omnichannel Database.

GenericChannelAPI attributes

DEFAULT_GROUP

Name	Description
Agents Count	The number of licensed Generic Channel agents.
ContextStoreService Cluster	The cluster that hosts Context Store services. To set this attribute, select Avaya Oceana® Cluster 1.
CoreDataService Cluster	The cluster that hosts OceanaCoreDataService. To set this attribute, select Avaya Oceana® Cluster 1.
CustomerManagement Cluster	The cluster that hosts the CustomerManagement service. To set this attribute, select Avaya Oceana® Cluster 1.
ORCRestService Cluster	The cluster that hosts ORCRestService. To set this attribute, select Avaya Oceana® Cluster 3.
Secure Connection to ORCRestService	The attribute that toggles a secure connection to ORCRestService. To set this attribute, select `true`.
Shutdown Mode	The attribute that you must set to reject new contacts but allow ongoing interactions to complete. To set this attribute, select `true`.

Table continues…

Name	Description
UCA Cluster	The cluster that hosts the Unified Collaboration Administrator (UCA) service. To set this attribute, select Avaya Oceana® Cluster 1.

OCP Database Configuration

Name	Description
Caché connection pool size	The number of connections to Omnichannel Database.
Caché Password	The password for Omnichannel Database.
Caché server FQDN	The IP address or FQDN of Omnichannel Database.
Caché User	The user name for Omnichannel Database.
Secure Caché Connection	The attribute that toggles all secure connections, except the connection to Omnichannel Database. To set this attribute, select `true`.

MessagingService attributes

DEFAULT_GROUP

Name	Description
Supplier Id	The Supplier ID that Avaya provides. The default value is 10000000.
Use message timestamp from Social provider	If set to true then value of message timestamp from Social provider will be sent to CustomerController as new message timestamp.

Startup

Name	Description
Authorization Service Address	The IP address or FQDN of that hosts AuthorizationService. • For an Avaya Oceana® deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, enter the IP address or FQDN of Avaya Oceana® Cluster 2. • For an Avaya Oceana® deployment that supports up to 100 active agents, enter the IP address or FQDN of Avaya Oceana® Cluster 1.

Table continues…

Name	Description
CustomerControllerService Cluster	The cluster that hosts CustomerControllerService. To set this attribute, select Avaya Oceana® Cluster 3.
Omnichannel Database Address	The IP address or FQDN of Omnichannel Database.

Database Configuration

Name	Description
Password for the Omnichannel Database	The password for Omnichannel Database.
Secure Connections to Omnichannel Database	The attribute that toggles a secure connection to Omnichannel Database. To set this attribute, select `true`.
Thread pool size for the Omnichannel Database	The number of concurrent connections to the Omnichannel Database, ranging between 1 and 500. The default value is 10. Requires a reboot or restart to take effect.
Username for the Omnichannel Database	The user name for Omnichannel Database.

Messaging Connector 1 Configuration

Name	Description
Messaging Snapin 1 Cluster	The cluster that hosts the first MessagingConnector snap-in service.
Messaging Snapin 1 Key	The database key for the first snap-in account, which is obtained after setting up data in Omnichannel Database. For example, if you set this attribute for SMS, you must enter the name of the snap-in that you create while configuring the SMS gateway.
Messaging Snapin Service 1 Name	The name of the first MessagingConnector snap-in service.

Messaging Connector 2 Configuration

Name	Description
Messaging Snapin 2 Cluster	The cluster that hosts the second MessagingConnector snap-in service.
Messaging Snapin 2 Key	The database key for the second snap-in account, which is obtained after setting up data in Omnichannel Database.

Table continues…

Name	Description
Messaging Snapin Service 2 Name	The name of the second MessagingConnector snap-in service.

Messaging Connector 3 Configuration

Name	Description
Messaging Snapin 3 Cluster	The cluster that hosts the third MessagingConnector snap-in service.
Messaging Snapin 3 Key	The database key for the third snap-in account, which is obtained after setting up data in Omnichannel Database.
Messaging Snapin Service 3 Name	The name of the third MessagingConnector snap-in service.

Language Analysis

Name	Description
SMS Analyze Language	The attribute that toggles whether or not to analyze the language of SMS messages. It appends the attribute returned from the SMS rest language analyzer. The default value is `false`.
SMS Rest Language Analyzer	The URL of the third-party service that analyzes the language of the SMS message. The URL must be in the following format: `http://<IP address/FQDN>` or `https://<IP address/FQDN>`
Social Analyze Language	The attribute that toggles whether or not to analyze the language of Social messages. It appends an attribute based on the language and the LanguageContextMap.xml. The default value is `false`.
Social language and attributes map	A map that determines what attributes get mapped to the language of the Social contact. For example, en,Language.English;es,Language.Spanish;fr,Language.French.

Advanced

Name	Description
Additional Messaging Snapin IPs/FQDNs	The FQDNs or IP addresses of the clusters that host any additional Messaging snap-ins.

Table continues…

Name	Description
Additional Messaging Snapin Keys	A comma-separated list of additional database keys for the snap-in accounts.
Additional Messaging Snapin Service Names	A comma-separated list of the names of any additional MessagingConnector snap-in services.
Deployment status of MessagingSpace	The attribute that triggers the deplyment. A reboot or restart to take effect is not required. To set this attribute, select `true`.
Deployment Type	The deployment type that determines the memory size of MessagingSpace to be deployed. • For an Avaya Oceana® deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® deployment that supports up to 100 active agents, select `OCEANA_SMALL`.
Messaging Connector Error Threshold	The number of messaging connector errors that must occur before an Oceana Monitor event is raised.
Send context from Social messages as custom data	The attribute that passes the value of "additionalData" field from Social message's context to CustomerController as custom data. To set this attribute, select `true`.
Shutdown mode	The attribute that rejects new contacts. However, allows ongoing interactions to complete. To set this attribute, select `true`.
Toggle Secure Mode	The attribute that toggles all secure connections, except the connection to Omnichannel Database. To set this attribute, select `true`.
Unsent agent social messages fails threshold	The number of fails to occur within 20 minutes monitoring period to rise Oceana Monitor event. Requires a reboot or restart to take effect.
Unsent agent's social resend attempts	The number of attempts that MessagingService tries to resend unsent agent's social messages. After the number of attempts, unsent messages are deleted.

Table continues…

Name	Description
Unsent agent's social resend interval	The amount of time, in minutes, that MessagingService uses between attempts to resend unsent agent's social messages.
Enable Centralized Logging	The attribute that enables Centralized Logging after snap-in is installed. To set this attribute, select `true`.

Authorization Service

Name	Description
Authorization Required for SMS API	The attribute that send requests to SMS API of MessagingService for JWT authorization token. A change to this attribute requires a restart of the system to take effect. To set this attribute, select `true`.
Authorization Required for SMS Vendor Snap-in	The attribute that enables or disables authentication for reading data from the SMS Vendor Snap-in. The default value is `false`, which specifies that the authentication for reading data from the SMS Vendor Snap-in is disabled.
Authorization Required for Social Media Snap-in	The attribute that enables or disables authentication for reading data from the SocialConnector Snap-in. The default value is `false`, which specifies that the authentication for reading data from the SocialConnector Snap-in is disabled.
Authorization Required for Socials API	The attribute that send requests to Socials API of MessagingService for JWT authorization token. A change to this attribute requires a restart of the system to take effect. To set this attribute, select `true`.
Context Length	Maximum length of the social message. The minimum default length is 8420.

OBCService attributes

Startup Configuration

Name	Description
Deployment type	Determines the memory size of processing units. The available deployment types are: • For an Avaya Oceana® deployment that supports up to <> active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® deployment that supports up to <> active agents, select `OCEANA_4XLARGE`. • For an Avaya Oceana® deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® deployment that supports up to 100 active agents, select `OCEANA_SMALL`.
POM Server	The IP address or FQDN of the POM server that the Outbound Connector services.
UAC Cluster	The cluster that hosts the Unified Agent Controller services. • For an Avaya Oceana® deployment that supports up to 100 active agents, select Avaya Oceana® Cluster 1. • For an Avaya Oceana® deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, select Avaya Oceana® Cluster 2.
UCA Cluster	The cluster that hosts the Unified Collaboration Administrator (UCA) service. To set this attribute, select Avaya Oceana® Cluster 1.
UCM Cluster	The cluster that hosts Unified Collaboration Model (UCM) services. To set this attribute, select Avaya Oceana® Cluster 1.

Advanced Configuration

Name	Description
Enable Authentication	If you set the JSON Web Tokens (JWT) authentication to true, the authentication server sends the token to the Unified Agent Controller (UAC) component through XML Paper Specification (XPS) API. If you set the authentication token to false, the authentication server does not send a JWT authentication token.
UAC URL	The service URL of the UnifiedAgentController service API. For example, `/services/UnifiedAgentContextService/XpsAPI`.

OCPDataServices attributes

Startup

Name	Description
AgentController Cluster	The cluster that hosts AgentControllerService. To set this attribute, select Avaya Oceana® Cluster 3.
Omnichannel Database Address	The IP address or FQDN of Omnichannel Database.

Advanced

Name	Description
Authorization Service Address	The FQDN or the IP of the node or cluster where the authorization service is installed.
Enable Tokenless Access	The attribute that enables the requests to access OCPDataServices without the need of the Authorization token. To enable tokenless access, select `TRUE`.
Password for the Omnichannel Database	The password for Omnichannel Database.
Secure Connections to Omnichannel Database	The attribute that toggles a secure connection to Omnichannel Database. To set this attribute, select `true`.
Toggle Secure Mode	The attribute that toggles all secure connections, except the connection to Omnichannel Database. To set this attribute, select `true`.
Username for the Omnichannel Database	The user name for Omnichannel Database.

Table continues…

Name	Description
Enable Centralized Logging	The value that enables centralized logging when a snap-in is installed.

ORCRestService attributes

Startup

Name	Description
Common Cluster	To set this attribute, select Avaya Oceana® Cluster 1.
AgentControllerService Cluster	The cluster that hosts AgentControllerService. To set this attribute, select Avaya Oceana® Cluster 3.
AutomationControllerService Cluster	The cluster that hosts AutomationControllerService. To set this attribute, select Avaya Oceana® Cluster 3.
Customer Management Service Cluster	The cluster that hosts the CustomerManagement service. To set this attribute, select Avaya Oceana® Cluster 1.
CustomerControllerService Cluster	The cluster that hosts CustomerControllerService. To set this attribute, select Avaya Oceana® Cluster 3.
Generic Provider Cluster	The cluster that hosts the GenericChannelAPI service. To set this attribute, select Avaya Oceana® Cluster 3.
OceanaCoreDataService Cluster	The cluster that hosts OceanaCoreDataService. To set this attribute, select Avaya Oceana® Cluster 1.
OCP Lookup Locators	The cluster that hosts Omnichannel Provider services. To set this attribute, select Avaya Oceana® Cluster 3.
Omnichannel Database Address	The IP address or FQDN of Omnichannel Database.
UCA Lookup Locators	The cluster that hosts the Unified Collaboration Administrator (UCA) service. To set this attribute, select Avaya Oceana® Cluster 1.

Table continues…

Name	Description
UCM Lookup Locators	The cluster that hosts Unified Collaboration Model (UCM) services. To set this attribute, select Avaya Oceana® Cluster 1.

Advanced

Name	Description
Deployment status of processing unit or-connector-uca-pu	The attribute to trigger the deployment of spaces and PUs. • If you want the application to trigger the deployment of spaces and PUs after the installation of SVAR, keep the default value `true`. • If you want the application to not trigger the deployment of the PU, select `false`.
Deployment type	The deployment type that determines the memory size of processing units. • For an Avaya Oceana® deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`. • For an Avaya Oceana® deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`. • For an Avaya Oceana® deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`. • For an Avaya Oceana® deployment that supports up to 100 active agents, select `OCEANA_SMALL`.
EngagementDesigner status check	The attiribute that enables or disables EngagementDesigner status consideration during Contacts Audit.
Password for the Omnichannel Database	The password for Omnichannel Database.
Secure Connections to Omnichannel Database	The attribute that toggles a secure connection to Omnichannel Database. To set this attribute, select `true`.
Send External-ID to Context Store	The attribute that enables sending Email Message-ID to Context Store as part of the contact record being created. To set this attribute, select `true`.

Table continues…

Name	Description
Toggle Secure Mode	The attribute that toggles all secure connections, except the connection to Omnichannel Database. To set this attribute, select `true`.
Username for the Omnichannel Database	The user name for Omnichannel Database.

OceanaDataViewer attributes

Startup

Name	Description
Authorization Service Address	The IP address or FQDN of the cluster that hosts AuthorizationService.
CustomerControllerService Cluster	The cluster that hosts the CustomerControllerService. This requires a snap-in restart to take effect.
Omnichannel Database Address	The IP address or FQDN of Omnichannel Database.
OmniResourceConnector Cluster	The cluster that hosts ORCRestService. To set this attribute, select Avaya Oceana® Cluster 3.
Password for the Omnichannel Database	The password for Omnichannel Database.

Advanced

Name	Description
Client Redirection Path	OceanaDataViewer uses this path attribute to redirect the browser to.
Customer high contact threshold	The number of contacts that a customer can have before they appear on the high contact count list on the dashboard. The default value is 700.
Enable RTL option	Toggle show RTL option. You have to restart the service to take effect.
Maximum concurrent user sessions	The maximum number of user sessions that can be active at a time. If a new user logs in, the oldest session is invalidated. You can set any value between 1 and 5. The default value is 1.
Maximum query time	The maximum time in seconds for a SQL query to the database. The default value is 15 seconds.

Table continues…

Name	Description
Secure Connections to Omnichannel Database	The attribute that toggles a secure connection to Omnichannel Database. To set this attribute, select `true`.
Toggle Secure Mode	The attribute that toggles all secure connections, except the connection to Omnichannel Database. To set this attribute, select `true`.
Username for the Omnichannel Database	The user name for Omnichannel Database.
Enable Centralized Logging	The attribute that enables Centralized Logging after snap-in is installed. To set this attribute, select true.

EASG authentication config

Name	Description
Enable EASG Authentication	The attribute that enables or disables EASG authorization for the Oceana Data Viewer. • To enable EASG authentication, keep the default value `true`. • To disable EASG authentication, select `false`.
Number of retries to connect to CECommonSpace	The attribute that specifies the number of times the Oceana Data Viewer retries to connect to the CECommonSpace. The default value is 60.
Time delay between attempts to connect to CECommonSpace	The attribute that specifies the delay between Oceana Data Viewer attempts to connect to CECommonSpace in milliseconds. The default value is 30000.

SocialConnector attributes

Startup Configuration

Name	Description
Oceana Messaging Snapin IP	The FQDN or the IP address of the cluster that hosts MessagingService.
Oceana Messaging Snapin key	The name of the snap-in that you create while configuring the Social Media gateway. The same name gets automatically configured for Social Media in the **Messaging Snapin Key** attribute of MessagingService or **Snap-in Key** attribute of the OceanaConfiguration service.

Run-time Service Configuration

Name	Description
Enable Oceana serviceability feature	The attribute to enable or disable the snap-in heartbeat and life cycle messages. The System Manager Monitoring Service page displays these messages.
Maintenance Mode	The attribute that determines whether to fetch or accept any request from Social Media Gateway. The values are: • `False`: To enable Social Media Snap-in to fetch or accept requests from Social Media Gateway. • `True`: To enableSocial Media Snap-in to not fetch or accept any requests from Social Media Gateway.
Max Request Length	The attribute that determines the maximum number of HTTP bytes requests that Social Connector accept. • The value can range between 100 to 524288000. The default value is `25000`.
Enable Tokenless Access	The attribute that enables the requests to access resource end-points without the need of the authorization token. The default value is `False`. **Important:** Do not change the default value.

Advanced Configuration

Name	Description
Oceana Messaging Snapin Name	The name of the MessagingService snap-in.
Oceana Messaging Snapin Version	The version number of the MessagingService snap-in. You can view this number from the Service Management page.
Authorization Service Address	The FQDN or the IP address of the node or cluster that hosts the authorization service.

CoBrowse attributes

Runtime service configuration

Name	Description
Inactive Timeout (Minutes)	The time in minutes after which the Co-Browsing session between the agent and customer closes because of inactivity. The default value for this attribute is 2. You can specify any value between 2 to 30 to configure this attribute.
Inactive Timeout Message	The message that must be displayed to the agent and customer after the inactive timeout. The length of the message must be between 10 to 80 characters.
Session Timeout (Minute)	The time in minutes after which the Co-Browsing session between the agent and customer closes. The default value for this attribute is 60. You can specify any value between 30 to 1440 to configure this attribute.
Enable Tokenless Access	The attribute that enables the requests to access resource end-points without the need of the Authorization token. Ensure that you do not change the default value `FALSE`.
Oceana Serviceability Feature Enable	The attribute that enables or disables this snap-in's heartbeat and lifecycle messages to be shown on System Manager Monitoring Service page.

Database Configuration

Name	Description
Enable JNDI	The attribute that enables or disables Java Naming and Directory Interface (JNDI). For Avaya Oceana®, select `false`.
Database JNDI Name	The JNDI name of the Co-Browse database.
Database Type	The type of the Co-Browse database. For Avaya Oceana®, select `intersystemcache`.
Database Dialect	The dialect of the Co-Browse database. To set this attribute, type the dialect as `org.hibernate.dialect.Cache71Dialect`.

Omnichannel Database Configuration

Name	Description
Database User Name	The user name for the Co-Browse database. To set this attribute, type the user name as `Cobrowse`.
Database Password	The password for the Co-Browse database. To set this attribute, type the password as `Oceana16`.
Database Driver Class	The driver class name of the Co-Browse database. To set this attribute, type the class name as `com.intersys.jdbc.CacheDriver`.
Database IP/FQDN	The IP address or FQDN of the Co-Browse database.
Database Port	The port number of the Co-Browse database. Ensure that you keep the default port number 1972.
Secure InterSystem Cache	The attribute that enables or disables the secure communication to the Co-Browse database.

CRMGateway attributes

Default group

Name	Description
Custom CRMGateway Attributes	The custom attributes for the snap-in. Enter comma-separated values, such as maxrequestlength:1000000, maskfields:A|B|C.
Enable Tokenless Access	The attribute that enables the requests to access resource end-points without any authorization token. To enable tokenless access, retain the default value `true`.

CRM configuration

Name	Description
CRM Type	The type of CRM to connect for the configuration. The default value is SAP.
Connection URL	The FQDN or IP address of the CRM server. This is a mandatory attribute to establish a connection.

Table continues…

Name	Description
Server User-Name	The user name of the CRM server that has permission to access the CRM server database. This is a mandatory attribute to establish a connection.
Server Password	The password of the CRM server. This is an optional attribute for the connection establishment.
Custom CRM Initialization Attributes	The custom field to specify any non-sensitive information in a key:value format. For example, maxsize:1,datafile:/tmp/. This is an optional attribute.
Custom Authentication Field 1	The custom field that is used to specify sensitive information that is required by the adapter during run-time. For example, AWS secret keys, SSO information, or any token. This is an optional attribute.
Custom Authentication Field 2	The custom field that is used to specify sensitive information that is required by the adapter during run-time. For example, AWS secret keys, SSO information, or any token. This is an optional attribute.
Mapper file location	The secure location of the mapper file. For example, `https://server:port/adapter/Mapping_folder/mapper.json` or the CRMGateway Breeze node that include all the nodes in cluster where the snap-in is running. This is a mandatory attribute to establish a connection. Changing this attribute during runtime needs a service restart or cluster reboot.
Adapter Dependency Location	The base location of the plug-in JAR files. For example, `https://server:port/adaptter/JAR_FOLDER` or the Breeze node internal location such as . /tmp This is a mandatory attribute to establish a connection. Changing this attribute during runtime needs a service restart. For example, https://server:port/adapter/JAR_FOLDER or Breeze node internal location.

Table continues…

Name	Description
Adapter Dependency file Names	The JAR or properties file name that is specified by the attribute setting adapter dependency location. Enter comma (,) separated values. For example, `adapter.jar` or `helper1.jar`. This is a mandatory attribute to establish a connection. Changing this attribute during runtime requires a service restart.
Implementation Class Name	The canonical name of the class in the adapter that has implemented the SDK interface. This is a mandatory attribute to establish a connection. Changing this attribute during runtime requires a service restart.
Enable Adapter	The adapter connection state. To enable the connection, click True. The default option is False, which indicates that the connection is switched off. **Note:** You must enable this attribute only after configuring all the other attributes required for the configuration.
Input Validation	The option to ensure that the user enters valid input parameters. You must enable this attribute for enhanced security. By default, this check box is disabled. Changing this attribute during run-time requires a service restart.

ZangSmsConnector attributes

You must configure the ZangSmsConnector snap-in attributes in System Manager and configure the Zang account gateway attributes through Omnichannel Administration Utility. The attributes are:

DEFAULT_GROUP

Name	Description
Maintenance Mode	The attribute to enable the maintenance mode. The supported values are true and false. The default value is false. This feature is available only in Avaya Oceana® mode.
Zang Polling Service Base URL	The base URI of the Zang SMS Poller service.
Zang URL	The base URI of the Zang SMS API.
Proxy Server Protocol	The proxy server configured in Avaya Breeze® platform for an Outbound connection. The supported values are http and https. The default value is http.
Enable Tokenless Access	The attribute that enables the requests to access resource end-points without the need of the Authorization token. The supported values are true and false. The default value is true. This feature is available only in Avaya Oceana® mode.
Authorization Service Address	The FQDN or IP of the node or cluster that hosts the Authorization Service. This attribute is required for authorization in Avaya Oceana® mode.

OCEANA

Name	Description
Oceana Mode	The attribute to enable Oceana support for ZangSmsConnector. The supported values are true and false. The default value is false.
Oceana Messaging Service key	The attribute used for polling the Oceana SMS snap-in for accounts information. This attribute is mandatory to support the Oceana mode.
Oceana Messaging Service IP	The Avaya Breeze® platform node IP address or the IP address of the cluster that hosts the Oceana Messaging snap-in. This option is mandatory to support the Oceana mode.

Table continues…

Name	Description
Oceana Messaging Service name	The name of the MessagingService snap-in. This option is mandatory to support the Oceana mode.
Enable Inbound MMS	The value that indicates whether the Inbound MMS feature is enabled. **Note:** This feature is available only in Avaya Oceana® mode.

Index

A

accept email messages 583
accept incoming calls 372
accept incoming Chat contacts 548
accept Outbound calls 655
accept SMS messages 603
accept Social Media messages 619
access to UnifiedAgentController 545, 579, 600, 616, 637
account type support 692
accounts 238
  account type 690
  account value 690
accounts support 690
activating
  encryption key 214
add
  attribute categories 238
  attributes 239, 368
  Avaya Oceana® Server 226
  Callback VDN 344
  Communication Manager to Avaya Control Manager 221
  Communication Manager to the location 222
  connectors to Provisioning Server 227
  custom attributes 533
  department 222
  Disposition Codes 650
  extensions 365
  No Media Treatment VDN 347
  provider 365
  SelfService VDN 324
  server to a domain 200
  site 222
  skills 365
  Survey VDN 358
  team 222
  VDN 365
add authorization client 231
add rule
  sample Chat workflow 539
  sample Voice workflow 298
adding
  account types 692
  Callback applications 339
  custom fields 695
  Experience Portal 310
  OceanaSurvey application 353
  self-service application 310
  server configuration 439, 440
  server flow 440, 441
  SIP entity for Session Border Controller 442
  STUN server configuration 501
  TURN/STUN service 434, 499
adding Breeze CA certificate to the Elasticsearch truststore on CCM 738
adding Breeze CN to CCM through CLI 740
adding Breeze node CN to CSP 740
Adding CSP CA to Avaya Breeze truststore 741
adding customer data manually 695
adding grants
  Control manager application 232
  Engagement Designer 233
  to Authorization Service 233
adding nodes
  Avaya Oceana® Cluster 1 127
  Avaya Oceana® Cluster 2 128
  Avaya Oceana® Cluster 3 129
  Avaya Oceana® Cluster 4 130
  Avaya Oceana® Cluster 5 131
administering
  implicit sequencing 451
AgentControllerService attributes 800
Alias field descriptions 561
alphabetic characters 702
android reference client 422
announcements 318
  adding 273
Apache HTTP server 531
architecture 24
assign
  location to Application Server 235
  location to Synchronizer Service Server 236
assigning
  location to UCA proxy server 235
attribute sets 237
attributes 153, 173, 237
authentication 723
Authorization Service address 545, 546, 579, 580, 600, 601, 616, 617, 637, 638
AuthorizationService attributes 792
authorized access to Oceana transcripts 546, 580, 601, 617, 638
automated installation 100, 133
AutomationController attributes 802
Avaya Aura Web Gateway 439, 440
Avaya Aura® Device Services 380
Avaya Aura® Media Server 386
Avaya Aura® Web Gateway 400
Avaya Contact Recorder 77
Avaya Control Manager HA 663
Avaya Oceana® overview 23
Avaya support website 755
AvayaMobileCommunications attributes 793

B

blacklist
email addresses and domains ... 570
BotConnector attributes ... 795
Breeze authorization service ... 733
Breeze identity certificate ... 40
breeze node identity certificates ... 34

C

cache mirroring ... 666, 668
CallServerConnector attributes ... 756
capacity ... 46, 707
categories ... 237
Centralized Logging overview ... 737
certificate authority ... 29
certificate for messaging HA ... 635
certificate installation on SMGR for SMS portal ... 590
certificate management prerequisites ... 726
Certificate Profiles ... 207
change
workflow type ... 534
change password ... 212
changing the Avaya Breeze cluster to accept new service 742
changing the targeted Breeze cluster in “Deny New Service” ... 741
chat limits ... 545
checking
replication status of nodes ... 135
checking customer matches ... 703
checklist
TLS encryption ... 725
checklist for centralized logging ... 737
client profile
AvayaMobileCommunications ... 432
TLS ... 504
Client Side TURN
enable ... 435, 500
CM configuration ... 251
CoBrowse attributes ... 820
collection
delete ... 751
edit ... 751
generating PDF ... 751
sharing content ... 751
commission
Avaya Control Manager ... 219
communication manager ... 260
Communication Manager logging on ... 253, 268
config.properties ... 308
configuration
external datamart ... 153, 173
configuration and deployment details ... 70
configure
ACW time ... 652
AES certificates ... 262
configure *(continued)*
Agent Login ID ... 258
Agent Phone-sets ... 259
an automatic suggestion response ... 558
Application Enablement Services ... 256, 260
automatic response ... 558
Avaya Aura® Experience Portal ... 304
Avaya Control Manager voice resources ... 361
BotConnector Snap-in licenses ... 537
Caché superserver ... 211
Caché to use TLS ... 210
Call Center Elite ... 251
Callback vector ... 342
Chat ... 537
Chat client ... 531
Chat provider ... 542
CM Hunt Group ... 361
Communication Manager ... 251
coverage vector ... 288
Direct Agent Calling ... 257
Elite IVR ... 315
email ... 552
Email provider ... 552
Email Route Point ... 553
email server and mailboxes ... 554
Email server certificates ... 553
email templates ... 569
fallback vector ... 275
Hunt Group ... 257
Inbound Mail server ... 556
Ingress vector ... 277
keyword groups ... 557
LDAP server integration ... 74
media files ... 272, 317, 387
Messaging client ... 642
Messaging provider ... 628
No Media vector ... 346
Oceana Customer Management Tool ... 676
Omnichannel Database address ... 671
Outbound ... 646
Outbound provider ... 649
Outbound SMTP server ... 556
POM server certificates ... 649
properties ... 241
provider ... 468
recipient address ... 559
RONA vector ... 285
Route Pattern ... 255
routing for the AvayaMobileCommunications SVAR ... 448
Routing vector ... 282
rule groups ... 564
screen pops ... 632
secure space ... 724
SelfService vector ... 321
server certificates ... 87
session manager routing ... 90
Signaling Group ... 254

configure *(continued)*
SMS ... 585
SMS Gateway ... 587
SMS provider ... 586
Social Media ... 605
Social Media provider ... 605
Survey vector ... 355
third-party gateways ... 605
TLS version ... 69
Transfer to Service Implicit User for Web Video ... 475, 477
Transfer to Service Implicit User for Web Voice ... 456, 458
Transfer to Service Route Point for Chat ... 544
Transfer to Service Route Point for Email ... 575
Transfer to Service Route Point for Messaging ... 631
Transfer to Service Route Point for SMS ... 599
Transfer to Service Route Point for Social Media ... 613
Transfer to Service vector ... 292
Transfer to Service workflow for Chat ... 541
Transfer to Service workflow for Email ... 573
Transfer to Service workflow for Messaging ... 627
Transfer to Service workflow for SMS ... 596
Transfer to Service workflow for Social Media ... 609
Transfer to User vector ... 293
treatment vector ... 279, 343
Trunk Group ... 254
URLs ... 532
VDNs ... 364
voice resources ... 361
Web Video Transfer vector ... 476
Web Voice Transfer vector ... 457
WebRTC Connect service profile ... 390
configure and exchange
certificate ... 646
configure automated SQL Server Agent jobs ... 189
configure for voice
media files ... 272, 317, 387
configuring
client profile ... 510
codecs ... 407, 470
Context Store for secure connections ... 731
CRMGateway ... 716
external media interface ... 436
Firefox ... 210
internal media interface ... 437
Java clients ... 212
load monitoring ... 514
LOB ... 337
media interface ... 512
Oceana token-based access ... 228
Office 365 ... 563
security ... 210
server flows ... 515
server profile for media tunneling ... 509
server profile for signaling interface ... 508
Session Border Controller network interfaces ... 511
Session Border Controller networks ... 425, 502
signaling interface ... 511
configuring *(continued)*
SQL Server Configuration Manager ... 732
system properties ... 242
token-based access ... 228
Voice workflow ... 348
Workspaces for Elite token-based access ... 228
configuring authorization service for outbound connector
provider cluste ... 359
configuring Centralized Logging on the cluster editor ... 742
configuring routing ... 443
configuring system rules ... 567
configuring,
MS SQL server to listen to static port ... 733
connection with CSC ... 265
connectivity details ... 487
contact priority ... 640
ContactCenterService attributes ... 758
content
publishing PDF output ... 751
searching ... 751
sharing ... 751
sort by last updated ... 751
watching for updates ... 751
Context Store for secure connections
configure ... 731
ContextStoreManager attributes ... 760
ContextStoreQuery attributes ... 768
ContextStoreRest attributes ... 770
control manager
certificate ... 231
exporting ... 231
Control Manager identity
configuration ... 234
CORS ... 725
create
Avaya Oceana® Cluster 1 ... 105
Avaya Oceana® Cluster 2 ... 108
Avaya Oceana® Cluster 3 ... 110
Avaya Oceana® Cluster 4 ... 113
Avaya Oceana® Cluster 5 ... 114
callback configuration ... 334
Callback VDN ... 341
certificate ... 209, 680
Certificate Signing Request ... 208, 679
Communication Manager user ... 219
Coverage VDN ... 287
Dial Patterns ... 94, 95
end entities ... 208, 678
entity link ... 93
fallback VDN ... 274
implicit user profile ... 447
Ingress VDN ... 276
keystore ... 210
location for Avaya Oceana ... 221
manager server for UCA ... 224
no media treatment VDN ... 345
Provisioning Cluster ... 116

create *(continued)*
RONA VDN 284
routing location 90
routing policy 93, 94, 505, 506
Routing VDN 281
SelfService VDN 321
SIP entity for Avaya Breeze® platform 92
SIP entity for Communication Manager 91
SIP entity for Experience Portal MPP 92
SIP entity for Session Manager 91
site definition 331
Survey VDN 354
topology hiding profile 504
Transfer Target service for Messaging 631
Transfer Target services for Chat 544
Transfer Target services for Email 576
Transfer Target services for SMS 600
Transfer Target services for Social Media 613
Transfer Target services for Voice 369
Transfer Target services for Web Video 478
Transfer Target services for Web Voice 459
Transfer VDN 290
treatment VDN 278
user to handle Chat contacts 542
user to handle email contacts 574
user to handle Messaging contacts 630
user to handle outbound contacts 651
user to handle SMS contacts 598
user to handle Social Media contacts 612
variables 362
virtual machine 197
create certificate 263
create for Web Video Transfer VDN 457, 476
create for Web Voice Transfer VDN 457, 476
create grants 580
create variables 269
creating
application 450
application rule 437
application sequence 450
client profile 429
client profile for signaling interface 438
encryption key 214
endpoint policy group 438
interworking profile 438
reverse proxy 426
reverse proxy policy 426
server profile 430
server profile for AMC 433
server profile for signaling interface 435
signaling interface 436
STUN TURN server 517
TLS certificate 727
TLS server profile 505
Web Service user 330
creating a new master key with a known password 186
creating custom index patterns 744
Creating index policies for the custom index patterns 744
creating the EDM database for the standalone deployment
existing customers 171
CRMGateway
configuration verification 719
installation verification 716
trusted certificate 715
CRMGateway attributes 716, 821
CRMGateway snap-in 714
serviceability attributes 714
Cross Origin Resource Sharing 725
CSC communication 264
Customer data import template 686
CustomerControllerService attributes 803
CustomerJourneyService attributes 771
CustomerManagement attributes 775
customizing
Elite IVR ED attributes 326
cylanceprotect 82

D

database
JDBC driver 162, 178
MS SQL 162, 178
database drivers
JDBC driver 162, 178
Database encryption 213
database tables 153, 173
Delete
Server Message Block 204
SMB 204
deleting
CRMGateway 721
deletion
completed instances 195
error handled instances 195
errored instances 195
deploy
Avaya Breeze® platform nodes 79
Chat workflow 538
clusters 97
Engagement Designer tasks 191
Messaging workflow 624
Omnichannel Windows Server 197
sample Email workflow 571
sample SelfService workflow 324
sample Transfer to Service workflow for Chat 540
sample Transfer to Service workflow for Email 572
sample Transfer to Service workflow for Messaging 625
sample Transfer to Service workflow for SMS 595
sample Transfer to Service workflow for Social Media 608
sample Transfer to Service workflow for Voice 301

deploy *(continued)*
sample Transfer to Service workflow for Web Video .. 473
sample Transfer to Service workflow for Web Voice .. 454
sample Voice workflow 295
sample Web Video workflow 464
sample Web Voice workflow 389
SMS workflow 593
Social Media workflow 607
deploying
OceanaCallback 339
OceanaSurvey 352
run-time support files 306
self-service application 307
support files 306
deployment checklist
Avaya Breeze® platform nodes 80
deployment process 42
disable
Network Adapters 201
disable Admin Approval Mode
Omnichannel Windows Server administrators 202
disabling cylance 84
discovering data using new index patterns 747
disk 51
Distribution group field descriptions 562
document changes 22
documentation center 751
finding content 751
navigation 751
documentation portal 751
download CA certificate 263
downloading
certificates for CPaaS SMS Portal 590
TLS certificate 160, 728
downloading logs 657
dropping the master key 186
duplicate customer data 699

E

EASG
authentication 31
ED admin console
error handled instances 194
EDM 68, 152, 153, 171, 173
EDM TDE 183, 187
email approval 576
email approval ratios 578
EmailService attributes 805
enable
CORS 133
Remote Desktop 201
enable port for remote access
Avaya Aura Web Gateway 405
enabling
SSL 683
enabling authentication flag in the OCP service cluster 359
enabling automation startup message overview 537
enabling TDE
cluster of SQL servers 183
single SQL server 187
encrypting
database 215, 216
encryptings
database 215, 216
end entity 36, 262
Engagement Designer Event Mapper 446, 455, 465, 474
Engagement Designer tasks 192
Engagement Designer workflow 192
EngagementDesigner attributes 777
Enhanced Access Security Gateway 31
error scenarios 218
ESXi
upgrade 67
export
intermediate certificate 86
LDAP certificate 86
Export multiple workflows 193
exporting
TLS certificate 730
Exporting
customer details from Salesforce 685
exporting customer data 704
exporting sample application 314
external data mart 68
external firewall 486, 521

F

finding content on documentation center 751
function and role of the internal firewall 487

G

general settings 568
generate
certificate 210
private key 210
GenericChannelAPI attributes 807

H

hardware 51

I

identity certificates 37–39
import CA certificate 263
Import multiple workflows 194
import sample application 312
import server certificate 264
importing
certificates 338

importing *(continued)*
customer data ... 703
TLS certificate ... 161, 729
importing data from a text file ... 693
importing data from an ODBC database ... 694
inbound web video
implicit user route point ... 466
inbound web voice
implicit user route point ... 451
Incoming messages limit ... 634
inserting text ... 696
install
Omnichannel server ... 203
POM ... 646
Session Border Controller ... 425
SMSVendorSnapin ... 589
Windows Server 2022 ... 198
ZangSmsConnector ... 589
installing ... 206, 536
application server ... 305
Arbiter service ... 665
Installing
trusted certificate for CRMGateway ... 715
installing certificate on system manager ... 590
instances by work request ID ... 194

L

language configuration ... 706
legal notices ...
length of fields ... 700
load
license files ... 99
SVARs ... 101
loading and installing the Metricbeat and Packbeat svars ... 743
loading the Breeze CA certificate into the Elasticsearch truststore ... 739
log files ... 705
log in to Avaya Control Manager ... 220
log on
Communication Manager ... 253, 268
logging configuration ... 658
logging in to OpenSearch UI ... 743
logs ... 657

M

mail approval ... 577
Mail Store field descriptions ... 559
managing
Avaya Oceana ... 226
synchronization ... 226
manual synchronization ... 226
maximum accounts ... 46, 707
maximum active users ... 46, 707
media servers for Web Video ... 469
memory ... 51
message connector ... 635
messaging
contact status ... 636
Oceana Data Viewer ... 636
messaging limits ... 634
MessagingService attributes ... 808
mobile applications ... 417
modify
sample Voice workflow ... 297
Monitor Service page ... 140

N

notices legal ...

O

OBCService attributes ... 813
Oceana customer management tool ... 695–703
customer match ... 702
Oceana Customer Management Tool ... 250, 684, 689, 693, 694, 704
Oceana Dashboard ... 141
Oceana manager
viewing ... 143
Oceana server URL ... 230
Oceana Services Overview page ... 141
OceanaConfiguration attributes ... 118
OceanaCoreDataService attributes ... 781
OceanaDataViewer attributes ... 817
OceanaMonitorService attributes ... 783
OCPDataServices attributes ... 814
OmniCenterProvisioningCollector attributes ... 786
Omnichannel administration utility ... 635
Omnichannel Administration Utility ... 246, 250, 685
Omnichannel Database HA ... 663
Omnichannel Windows Server installation
disable Admin Approval Mode ... 202
Omnistore database ... 692
ORCRestService attributes ... 815
Outbound Callback application name ... 332
outbound email ... 576
overview
Callback Assist ... 329
Messaging ... 622
Post Call Survey ... 350
Overview ... 141

P

personal certificates pools for breeze authorization ... 234
planning ... 45
planning tasks ... 69
policy recommendations for different deployment sizes ... 746
ports ... 736
preconfiguration ... 45

prerequisites
CRMGateway 715
ZangSmsConnector 585
prioritizing
codecs 408, 470
prompt timeout
CM 268
providers 238
publishing
COMM_ADDR_HANDLE values 385
purpose 22

R

recovery steps if the elasticsearch disk size is full 747
reference clients 417
rejection codes 577
related documentation 749
relay service 496
remote worker 479
remote worker solution architecture 481
remote worker solution process flow 484
remote workers capabilities 479
remote workers limitations 480
Remove
Server Message Block 204
SMB 204
Removing IIS default page, Remove IIS default page 205
removing text 697
replacing text 698
restart
CallServerConnector service 369
restarting
CRMGateway service 720
restarting the Elasticsearch cluster 739
retain email
maximum number of days 554
retain generic
maximum number of days 706
retain messaging
maximum number of days 628
retain SMS
maximum number of days 597
retain social media
maximum number of days 610
retrieving the Breeze node CN 740
reverse proxy 433, 486, 495
reviewing
existing trusted certificate 727
root certificate 206, 229, 535
installing 206, 536

S

SAL Policy Manager 27
sample voice workflow 299
scheduled system maintenance 203
searching for content 751
secure browser access 683
secure connections 41
Secure space
space security 723
security 26, 27, 33, 205, 723, 736
send as group 562
Server Message Block - remove 204
service attributes 756
CRMGateway attributes 716, 821
service packs 199
Session Manager 440, 441
setting
Cluster State to Accepting 133
Cluster State to Denying 135
OceanaConfiguration attributes 117
service attributes 756
SMSVendorSnapin attributes 591
Storage URL 333
System ANI 332
ZangSmsConnector attributes 591
sharing content 751
SMB - remove 204
SMGR root certificate 229
SMS limits 600
SMSVendorSnapin attributes 592
Social Media contact routing
verify 620
SocialConnector attributes 818
sort documents 751
space security
configure 724
specifications
hardware and software 49
splitting phone numbers 698
SQL Server
forced encryption 732
SSL management 733
Stuck Contact tool 143
viewing 143
support 755
switch connection 260
synchronization 223, 226
system delivery failure rule 568
System Manager 231

T

TDE 182
cluster of SQL servers 183
single SQL server 187
TDE troubleshooting 189
test
UCA REST connection 236
test Chat contact 549
test Chat contact using Co-Browse 550
thin provisioning

thin provisioning *(continued)*
VMware disk storage 67
TLS 212, 671
TLS certificate
create 727
review 727
TLS certificates 205
TLS Turn relay
server profile 434
token enforcement in UCA 234
training 752
Transparent Data Encryption 182
transport layer security 27
troubleshooting TDE issues 189
trusted node 315

U

UCAStoreService attributes 787
UCMDataCollector attributes 788
UCMService attributes 789
UnifiedAgentContextService attributes 796
UnifiedAgentController attributes 797
update
voicemail announcement 347
upgrade
ESXi 67
host 67
VMware 67
upgrade script parameters
Avaya Breeze 137
upgrading
self-service application 308
user configuration 367, 413
users 238
using CPaaS portal
CPaaS portal 585
using zang portal
zang portal 586, 590

V

validating customer data 696
value checking 701
vCPU 51
verify
Avaya Breeze platform deployment 81
Chat contacts 547
email contact routing 584
Email contacts 582
host name resolution 98
Messaging contact routing 645
Messaging contacts 643
Outbound contact routing 655
Outbound contacts 654
SMS contact routing 604
SMS contacts 602
verify *(continued)*
Social Media contacts 618
status of nodes 132
voice contact routing to agents 373
voice contacts 371
verify deployment
SMSVendorSnapin 592
verifying
CRMGateway configuration 719
CRMGateway installation 716
dial plan 341
Social Media contact routing 620
Verifying
CRMGateway unistallation 721
view
Oceana Dashboard 142
Oceana Monitor Service 140
viewing
log files 705
viewing Oceana manager 143
viewing Stuck Contact tool 143
Virtual resource allocation 56
virtualized deployment 68
VMware 197
upgrade 67
vmware configuration 63
voice resources 251
voice self service 303
voice treatments 267
vSphere 56

W

wait treatments 267
watchlist 751
web applications 417
WebRTC
configure TURN 434
WebRTC agents 460, 462
WebRTC configurations 375
WebRTC Connect agents 376
Windows Server
disable UAC 202
WorkAssignmentManagerService attributes 711, 790

Z

ZangSmsConnector
verify deployment 593
ZangSmsConnector attributes 823